Modèles

Recommandations AWS



Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Recommandations AWS: Modèles

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques commerciales et la présentation commerciale d’Amazon ne peuvent pas être utilisées en relation avec un produit ou un service extérieur à Amazon, d’une manière susceptible d’entraîner une confusion chez les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

AWS Modèles de directives prescriptives 1
Fondements du cloud 3
Automatisez la création de comptes à l'aide de l'accélérateur Landing Zone sur AWS 4
Récapitulatif 4
Conditions préalables et limitations 4
Architecture 5
Outils 6
Bonnes pratiques 9
Épopées 9
Ressources connexes 37
Informations supplémentaires 37
Inventaire automatique AWS des ressources 39
Récapitulatif 39
Conditions préalables et limitations 40
Architecture 41
Outils 42
Bonnes pratiques 43
Épopées 43
Résolution des problèmes 50
Ressources connexes 51
Configuration des journaux de flux VPC pour tous les comptes 52
Récapitulatif 52
Conditions préalables et limitations 52
Architecture 53
Outils 54
Bonnes pratiques 54
Épopées 56
Ressources connexes 58
Informations supplémentaires 58
Étiquetez automatiquement les pièces jointes de Transit Gateway 60
Récapitulatif 60
Conditions préalables et limitations 60
Architecture 60
Outils 62

Épopées 64
Ressources connexes 70
Plus de modèles 71
IA et apprentissage automatique 72
Agréger les données DynamoDB pour les prévisions du machine learning dans Athena 74
Récapitulatif 74
Conditions préalables et limitations 74
Architecture 74
Outils 75
Épopées 77
Ressources connexes 89
Associer un AWS CodeCommit référentiel à Amazon SageMaker AI Studio Classic sur plusieurs comptes 90
Récapitulatif 90
Conditions préalables et limitations 90
Architecture 91
Outils 91
Épopées 92
Informations supplémentaires 98
Extraire automatiquement le contenu des fichiers PDF 101
Récapitulatif 101
Conditions préalables et limitations 101
Architecture 102
Outils 103
Épopées 104
Ressources connexes 109
Pièces jointes 109
Créez un modèle de prévision de démarrage à froid à l'aide d' SageMaker AI DeePar 110
Récapitulatif 110
Conditions préalables et limitations 110
Architecture 111
Outils 112
Bonnes pratiques 113
Épopées 113
Ressources connexes 115
Créez un MLOps flux de travail à l'aide de l' SageMaker IA et d'Azure DevOps 117

Récapitulatif 117
Conditions préalables et limitations 117
Architecture 118
Outils 120
Bonnes pratiques 121
Épopées 122
Résolution des problèmes 132
Ressources connexes 133
Configurez la connexion dans Amazon Bedrock à l'aide de CloudFormation 135
Récapitulatif 135
Conditions préalables et limitations 135
Architecture 136
Outils 137
Épopées 138
Ressources connexes 141
Créez des conteneurs Docker SageMaker pour l'entraînement des modèles dans Step Functions 143
Récapitulatif 143
Conditions préalables et limitations 143
Architecture 144
Outils 144
Épopées 145
Ressources connexes 159
Créez des contrôles d'accès dans Amazon EKS avec les agents Amazon Bedrock 160
Récapitulatif 160
Conditions préalables et limitations 160
Architecture 161
Outils 162
Bonnes pratiques 163
Épopées 163
Résolution des problèmes 182
Ressources connexes 183
Déployez un cas d'utilisation de RAG sur AWS 184
Récapitulatif 184
Conditions préalables et limitations 184
Architecture 186

Outils 187
Bonnes pratiques 188
Épopées 189
Ressources connexes 192
Informations supplémentaires 193
Déployez plusieurs objets de modèle de pipeline sur un seul SageMaker point de terminaison 195
Récapitulatif 195
Conditions préalables et limitations 195
Architecture 196
Outils 196
Épopées 197
Ressources connexes 207
Développez des assistants basés sur le chat basé sur l'IA en utilisant RAG et des instructions ReAct 208
Récapitulatif 208
Conditions préalables et limitations 209
Architecture 210
Outils 211
Bonnes pratiques 213
Épopées 213
Résolution des problèmes 221
Ressources connexes 221
Informations supplémentaires 222
Développez un assistant basé sur le chat à l'aide d'Amazon Bedrock 223
Récapitulatif 223
Conditions préalables et limitations 224
Architecture 224
Outils 225
Bonnes pratiques 227
Épopées 228
Ressources connexes 232
Informations supplémentaires 233
Documenter les connaissances institutionnelles à partir de saisies vocales 235
Récapitulatif 235
Conditions préalables et limitations 235

Architecture 236
Outils 237
Bonnes pratiques 239
Épopées 239
Ressources connexes 245
Générez des recommandations personnalisées à l'aide d'Amazon Personalize 247
Récapitulatif 247
Conditions préalables et limitations 247
Architecture 247
Outils 249
Épopées 250
Ressources connexes 252
Informations supplémentaires 253
Simplifiez les flux de travail ML grâce à l' SageMaker IA et à Hydra 257
Récapitulatif 257
Conditions préalables et limitations 257
Architecture 258
Outils 259
Bonnes pratiques 260
Épopées 260
Résolution des problèmes 268
Ressources connexes 268
Informations supplémentaires 268
Entraînez et déployez un modèle de machine learning personnalisé supporté par GPU 270
Récapitulatif 270
Conditions préalables et limitations 270
Architecture 271
Outils 271
Épopées 272
Ressources connexes 289
Informations supplémentaires 289
..... 292
Récapitulatif 292
Conditions préalables et limitations 293
Architecture 296
Outils 298

Bonnes pratiques 299
Épopées 299
Ressources connexes 307
Informations supplémentaires 307
Utiliser Amazon Q Developer comme assistant de codage 313
Récapitulatif 313
Conditions préalables et limitations 314
Outils 314
Bonnes pratiques 314
Épopées 315
Résolution des problèmes 324
Ressources connexes 324
Utiliser SageMaker le traitement pour l'ingénierie des fonctionnalités distribuées d'ensembles de données ML à l'échelle du téraoctet 325
Récapitulatif 325
Conditions préalables et limitations 325
Architecture 326
Outils 329
Épopées 330
Ressources connexes 342
Pièces jointes 343
Visualisez les résultats du modèle AI/ML à l'aide de Flask et Elastic Beanstalk 344
Récapitulatif 344
Conditions préalables et limitations 344
Architecture 345
Outils 347
Épopées 348
Ressources connexes 358
Informations supplémentaires 359
Plus de modèles 363
Analyse 364
Analyser les données Amazon Redshift dans Microsoft SQL Server Analysis Services 366
Récapitulatif 366
Conditions préalables et limitations 366
Architecture 366
Outils 367

Épopées 367
Ressources connexes 369
..... 370
Récapitulatif 370
Conditions préalables et limitations 370
Architecture 371
Outils 371
Épopées 372
Ressources connexes 377
Automatisez l'ingestion de AWS Data Exchange données depuis Amazon S3 379
Récapitulatif 379
Conditions préalables et limitations 379
Architecture 379
Outils 380
Épopées 381
Ressources connexes 383
Pièces jointes 383
Automatisez l'application du chiffrement dans AWS Glue 384
Récapitulatif 384
Conditions préalables et limitations 384
Architecture 384
Outils 385
Bonnes pratiques 386
Épopées 386
Ressources connexes 389
Créez un pipeline de données pour traiter les données de Google Analytics à l'aide du kit AWS DataOps de développement 390
Récapitulatif 390
Conditions préalables et limitations 390
Architecture 391
Outils 391
Épopées 393
Résolution des problèmes 395
Ressources connexes 395
Informations supplémentaires 395
Créez un pipeline de traitement vidéo 398

Récapitulatif 398
Conditions préalables et limitations 398
Architecture 399
Outils 399
Épopées 400
Ressources connexes 407
Informations supplémentaires 408
Pièces jointes 408
Créez un pipeline ETL entre Amazon S3 et Amazon Redshift à l'aide d'AWS Glue 409
Récapitulatif 409
Conditions préalables et limitations 409
Architecture 410
Outils 410
Épopées 411
Ressources connexes 419
Informations supplémentaires 419
Créez un maillage de données d'entreprise avec Amazon DataZone 421
Récapitulatif 421
Conditions préalables et limitations 421
Architecture 423
Outils 424
Épopées 425
Ressources connexes 438
Informations supplémentaires 439
Calculez la valeur à risque (VaR) à l'aide des services AWS 441
Récapitulatif 441
Conditions préalables et limitations 441
Architecture 442
Outils 443
Bonnes pratiques 444
Épopées 445
Ressources connexes 448
Configurer l'accès entre comptes à un catalogue de données AWS Glue partagé à l'aide d'Athena 449
Récapitulatif 449
Conditions préalables et limitations 449

Architecture 449
Outils 451
Épopées 451
Ressources connexes 464
Informations supplémentaires 464
Convertir NORMALIZE en Amazon Redshift SQL 465
Récapitulatif 465
Conditions préalables et limitations 465
Architecture 465
Outils 466
Épopées 471
Ressources connexes 471
Convertir RESET WHEN en Amazon Redshift SQL 473
Récapitulatif 473
Conditions préalables et limitations 473
Architecture 473
Outils 474
Épopées 478
Ressources connexes 478
Déployez et gérez un lac de données sans serveur sur AWS 480
Récapitulatif 480
Conditions préalables et limitations 480
Architecture 481
Outils 482
Épopées 483
Ressources connexes 485
..... 487
Récapitulatif 487
Conditions préalables et limitations 487
Architecture 488
Outils 488
Épopées 489
Ressources connexes 493
Pièces jointes 493
Garantir la connexion d'Amazon EMR à Amazon S3 494
Récapitulatif 494

Conditions préalables et limitations 495
Architecture 495
Outils 496
Épopées 496
Ressources connexes 499
Pièces jointes 499
Génération de données de test à l'aide d'AWS Glue 500
Récapitulatif 500
Conditions préalables et limitations 500
Architecture 501
Outils 501
Bonnes pratiques 502
Épopées 502
Ressources connexes 513
Informations supplémentaires 514
Ingérez des données IoT directement dans Amazon S3 519
Récapitulatif 519
Conditions préalables et limitations 519
Architecture 520
Outils 521
Bonnes pratiques 521
Épopées 522
Résolution des problèmes 530
Ressources connexes 530
Informations supplémentaires 531
Lancer une tâche Spark dans Amazon EMR à l'aide d'une fonction Lambda 535
Récapitulatif 535
Conditions préalables et limitations 535
Architecture 536
Outils 536
Épopées 537
Ressources connexes 540
Informations supplémentaires 541
Pièces jointes 543
Migrer les charges de travail Apache Cassandra vers Amazon Keyspaces 544
Récapitulatif 544

Conditions préalables et limitations 544
Architecture 544
Outils 545
Bonnes pratiques 546
Épopées 546
Résolution des problèmes 560
Ressources connexes 560
Informations supplémentaires 561
Migrez les données Hadoop vers Amazon S3 à l'aide de Migrator WANdisco LiveData 563
Récapitulatif 563
Conditions préalables et limitations 563
Architecture 564
Épopées 565
Ressources connexes 571
Informations supplémentaires 571
Migrez Oracle Business Intelligence 12C vers le cloud AWS 572
Récapitulatif 572
Conditions préalables et limitations 572
Architecture 573
Outils 574
Épopées 575
Ressources connexes 589
Informations supplémentaires 590
Migrez un cluster Kafka vers Amazon MSK à l'aide de MirrorMaker 595
Récapitulatif 595
Conditions préalables et limitations 595
Architecture 596
Outils 596
Bonnes pratiques 597
Épopées 597
Ressources connexes 602
Informations supplémentaires 602
Migrer une pile ELK vers le cloud AWS 603
Récapitulatif 603
Conditions préalables et limitations 603
Architecture 605

Outils 607
Épopées 608
Ressources connexes 616
Informations supplémentaires 618
Migrer les données vers AWS Starburst 619
Récapitulatif 619
Conditions préalables et limitations 619
Architecture 619
Outils 621
Épopées 622
Ressources connexes 625
Optimisation de l'ingestion ETL de la taille du fichier d'entrée 626
Récapitulatif 626
Conditions préalables et limitations 626
Architecture 626
Outils 627
Épopées 627
Ressources connexes 630
Informations supplémentaires 631
Orchestrez un pipeline ETL avec AWS Step Functions 632
Récapitulatif 632
Conditions préalables et limitations 632
Architecture 633
Outils 634
Épopées 635
Résolution des problèmes 643
Ressources connexes 643
Informations supplémentaires 643
Effectuez des analyses ML à l'aide d'Amazon Redshift ML 644
Récapitulatif 644
Conditions préalables et limitations 644
Architecture 645
Outils 646
Épopées 647
Ressources connexes 651
Interrogez Amazon DynamoDB à l'aide d'Amazon Athena 653

Récapitulatif 653
Conditions préalables et limitations 653
Architecture 654
Outils 654
Épopées 655
Résolution des problèmes 658
Ressources connexes 659
Interrogez les tables DynamoDB à l'aide d'Athena 660
Récapitulatif 660
Conditions préalables et limitations 660
Architecture 661
Outils 661
Épopées 662
Ressources connexes 671
Informations supplémentaires 672
Configurez un espace de données minimum viable 673
Récapitulatif 673
Conditions préalables et limitations 674
Architecture 675
Outils 676
Bonnes pratiques 677
Épopées 678
Résolution des problèmes 732
Ressources connexes 732
Informations supplémentaires 732
Configurer un tri spécifique à la langue pour les résultats des requêtes Amazon Redshift 738
Récapitulatif 738
Conditions préalables et limitations 738
Architecture 739
Outils 739
Épopées 739
Ressources connexes 744
Informations supplémentaires 744
Abonnement d'une fonction Lambda aux notifications d'événements provenant de compartiments S3 interrégionaux 748
Récapitulatif 748

Conditions préalables et limitations 748
Architecture 749
Outils 749
Épopées 750
Ressources connexes 755
Trois types de tâches AWS Glue pour convertir des données 756
Récapitulatif 756
Conditions préalables et limitations 756
Architecture 756
Outils 757
Épopées 758
Ressources connexes 760
Informations supplémentaires 761
Pièces jointes 767
Visualisez les journaux d'audit Amazon Redshift à l'aide d'Athena et QuickSight 768
Récapitulatif 768
Conditions préalables et limitations 768
Architecture 768
Outils 769
Épopées 769
Ressources connexes 775
Pièces jointes 775
Visualisez les rapports d'identification IAM à l'aide d'Amazon QuickSight 776
Récapitulatif 776
Conditions préalables et limitations 777
Architecture 777
Outils 778
Épopées 779
Informations supplémentaires 786
Plus de modèles 788
Calcul 790
Conteneurs et microservices 791
Accédez à Amazon Neptune depuis Amazon EKS 793
Accédez aux applications de conteneur sur Amazon ECS 805
Accédez aux applications de conteneur sur Amazon ECS avec un type de lancement AWS Fargate 822

Accédez aux applications de conteneur en privé sur Amazon EKS 837
Activer les MTL dans App Mesh sur Amazon EKS 845
Automatisez les sauvegardes pour les instances de base de données Amazon RDS for PostgreSQL 853
Automatisez le déploiement du gestionnaire de terminaison de nœuds 867
Créez et déployez automatiquement une application Java sur Amazon EKS 882
Création d'une définition de tâche Amazon ECS sur des EC2 instances à l'aide d'Amazon EFS 908
Déployer des fonctions Lambda avec des images de conteneurs 915
Déployez des microservices Java sur Amazon ECS à l'aide d'AWS Fargate 924
Déployez des packages Kubernetes à l'aide d'Amazon EKS et Helm 931
Déployez un microservice Java sur Amazon EKS et exposez-le à l'aide d'un Application Load Balancer 943
Déployez une application en cluster sur Amazon ECS à l'aide d'AWS Copilot 958
Déployer une application basée sur GRPC sur Amazon EKS 969
Déploiement et débogage de clusters Amazon EKS 982
Déployez des conteneurs à l'aide d'Elastic Beanstalk 1012
Générez une adresse IP sortante statique à l'aide de Lambda et Amazon VPC 1018
Identifiez automatiquement les images de conteneurs dupliquées 1033
Installation de l'agent SSM sur les nœuds de travail Amazon EKS 1063
Installez l'agent SSM et l' CloudWatch agent sur les nœuds de travail Amazon EKS à l'aide de preBootstrapCommands 1069
Migrer les contrôleurs d'entrée NGINX pour le mode automatique EKS 1076
Migrer les charges de travail des conteneurs d'ARO vers ROSA 1097
Optimisation des images Docker générées 1114
Placer des pods Kubernetes sur des nœuds compatibles dans Amazon EKS 1125
Répliquez les images filtrées des conteneurs Amazon ECR sur plusieurs comptes ou régions 1144
Faites pivoter les informations d'identification sans redémarrer les conteneurs 1163
Exécuter des tâches Amazon ECS sur Amazon WorkSpaces 1170
Exécuter un conteneur Docker d'API Web ASP.NET sur AWS 1181
Exécutez des charges de travail basées sur des messages à l'aide d'AWS Fargate 1193
Exécutez des charges de travail dynamiques grâce au stockage permanent des données 1204
Configurer le dimensionnement automatique à l'aide d'Amazon EKS Pod Identity et KEDA 1230
..... 1254
Utiliser le protocole TLS mutuel dans Amazon ECS avec ALB 1276

Plus de modèles 1307
sans serveur 1309
Créez une application React Native à l'aide d'AWS Amplify 1310
Gérez de manière centralisée les locataires de plusieurs produits SaaS 1331
Créez une connexion Amazon EventBridge entre comptes 1345
Fournissez des enregistrements DynamoDB à Amazon S3 à l'aide de Kinesis Data Streams et Firehose 1360
Implémenter la gestion des versions d'API basée sur les chemins à l'aide d'API Gateway . 1367
Importez la bibliothèque psycopg2 dans AWS Lambda 1379
Intégrer API Gateway à Amazon SQS 1390
Traitez de APIs manière asynchrone avec AWS Lambda 1408
Traitez de APIs manière asynchrone avec Amazon DynamoDB Streams 1418
Traitez de APIs manière asynchrone avec Amazon SQS 1428
Exécutez les tâches d'automatisation de Systems Manager de manière synchrone à partir de Step Functions 1439
Exécutez des lectures parallèles d'objets S3 avec AWS Lambda 1454
Envoyer des données de télémétrie depuis Lambda vers OpenSearch 1467
Configuration d'un routeur cellulaire sans serveur 1485
Configurer un accès privé à un compartiment Amazon S3 1505
Résoudre les problèmes liés aux états de Step Functions 1512
Utilisez une approche sans serveur pour enchaîner les services AWS 1522
Plus de modèles 1528
Réseaux 1531
Automatisez le peering pour AWS Transit Gateway 1532
Centralisez la connectivité réseau à l'aide d'AWS Transit Gateway 1539
Configurer le chiffrement HTTPS pour Oracle JD Edwards à EnterpriseOne l'aide d'un Application Load Balancer 1546
Connectez-vous aux données et aux plans de contrôle du service de migration des applications via un réseau privé 1558
Création d'objets Infoblox à l'aide des ressources personnalisées AWS CloudFormation ... 1574
Personnalisez les CloudWatch alertes pour Network Firewall 1588
Déployez des ressources dans une zone Wavelength à l'aide de Terraform 1607
Migrer des enregistrements DNS en masse vers une zone hébergée privée Route 53 1616
Modifiez les en-têtes HTTP lors de la migration de F5 vers un Application Load Balancer sur AWS 1626
Accédez en privé à un point de terminaison de service AWS à partir de plusieurs VPCs 1632

Signaler les résultats de l'analyseur d'accès réseau en plusieurs Comptes AWS 1643
Configuration de la résolution DNS pour les réseaux hybrides dans un environnement multi-comptes AWS 1676
..... 1692
Afficher les journaux et les statistiques d'AWS Network Firewall à l'aide de Splunk 1698
Plus de modèles 1710
Diffusion de contenu 1712
Envoyer AWS WAF des logs à Splunk à l'aide de Firehose 1713
Diffusez du contenu statique dans un compartiment S3 via un VPC en utilisant CloudFront 1722
Plus de modèles 1731
Bases de données et stockage 1732
Bases de données 1733
Accédez aux données SQL Server locales à l'aide de serveurs liés 1736
Ajouter HA à Oracle PeopleSoft sur AWS 1742
Évaluez les performances des requêtes pour la migration des bases de données SQL Server vers MongoDB Atlas sur AWS 1767
Automatisez les déploiements bleu/vert des bases de données mondiales Aurora avec IaC 1778
Automatisez les tâches de base de données avec un AWS Lambda planificateur de tâches 1813
Automatisez le basculement et le retour en arrière avec DR Orchestrator Framework 1827
Automatisez la réplication des instances Amazon RDS sur Comptes AWS 1855
Sauvegardez automatiquement les bases de données SAP HANA 1871
Génération automatique de modèles PynamoDB et de fonctions CRUD pour DynamoDB . 1879
Bloquer l'accès public à Amazon RDS 1887
Configuration de l'accès multicompte à Amazon DynamoDB 1895
Configurer le routage en lecture seule dans un groupe de disponibilité Always On 1909
Connectez-vous en utilisant un tunnel SSH dans pgAdmin 1918
Convertir les requêtes Oracle JSON en SQL de base de données PostgreSQL 1923
Copier les tables Amazon DynamoDB entre les comptes 1955
Copier les tables Amazon DynamoDB entre les comptes 1962
Création de rapports sur les coûts et l'utilisation pour Amazon RDS et Amazon Aurora 1975
Déployez SQL Server FCIs sur Amazon EC2 et Amazon FSx 1983
Émuler des charges de travail Oracle RAC à l'aide d'Aurora PostgreSQL 2000
Activer les connexions chiffrées pour les instances de base de données PostgreSQL 2007
Chiffrer une instance de base de données Amazon RDS pour PostgreSQL existante 2017

Appliquer le balisage automatique des bases de données Amazon RDS au lancement 2026
Estimation des coûts DynamoDB 2032
Estimation des coûts de stockage pour une table Amazon DynamoDB 2044
Estimez la taille du moteur Amazon RDS pour une base de données Oracle à l'aide des rapports AWR 2049
Exporter les tables Amazon RDS for SQL Server vers un compartiment S3 2085
Gérer les blocs anonymes dans les instructions SQL dynamiques 2098
Gérez les fonctions Oracle surchargées dans la compatibilité avec Aurora PostgreSQL 2106
Aidez à appliquer le balisage DynamoDB 2113
Mettre en œuvre la DR interrégionale 2119
Migrez plus de 100 fonctions Oracle à arguments vers PostgreSQL 2137
Migrer les instances de base de données Amazon RDS for Oracle vers des comptes AMS 2143
Migrer les variables de liaison Oracle OUT vers PostgreSQL 2154
Migrez SAP HANA vers AWS à l'aide de HSR 2162
Migrer SQL Server vers AWS à l'aide de groupes de disponibilité distribués 2177
Migrez d'Oracle 8i ou 9i vers Amazon RDS for Oracle à l'aide d'AWS DMS SharePlex 2189
Surveillez le chiffrement d'Amazon Aurora 2198
Surveillez GoldenGate les journaux à l'aide d'Amazon CloudWatch 2204
Replateforme Oracle Database EE vers Amazon RDS for Oracle SE2 2219
Répliquez des bases de données mainframe sur AWS à l'aide de Precisely Connect 2231
Planifier des tâches pour Amazon RDS et Aurora PostgreSQL 2252
Envoyer des notifications pour RDS pour SQL Server à l'aide d'un serveur SMTP local 2258
Configuration de la reprise après sinistre pour SAP sur IBM Db2 sur AWS 2273
Configurer un pipeline CI/CD pour la migration de base de données à l'aide de Terraform . 2297
Configuration d'une architecture HA/DR pour Oracle E-Business Suite sur Amazon RDS Custom 2306
Configurer la réplication des données entre RDS for MySQL et MySQL sur Amazon EC2 . 2315
Rôles de transition pour une PeopleSoft application Oracle 2321
Déchargez les données d'Amazon Redshift entre les comptes 2357
Modèles de migration de base de données par charge de travail 2387
Plus de modèles 2398
Stockage et sauvegarde 2404
Autoriser EC2 les instances à accéder en écriture aux compartiments S3 dans AMS 2405
Automatisez l'ingestion de flux de données dans une base de données Snowflake 2411
Chiffrez automatiquement les volumes EBS 2423
Sauvegardez les serveurs Sun SPARC dans l'émulateur Charon-SSP sur AWS 2435

Sauvegardez et archivez les données sur Amazon S3 avec Veeam 2461
Configuration NetBackup pour VMware le cloud sur AWS 2490
Copiez des objets S3 entre des comptes et des régions à l'aide de l'AWS CLI 2498
Copiez des objets S3 entre des comptes et des régions à l'aide de S3 Batch Replication .. 2513
Migrer les données Hadoop vers Amazon S3 à l'aide d' DistCp AWS PrivateLink pour Amazon S3 2527
Plus de modèles 2544
Outils pour développeurs 2546
DevOps 2547
Automatisez AWS les opérations d'infrastructure 2551
Automatisez les CloudFront mises à jour en cas de modification des terminaux de l'équilibreur de charge 2561
Automatisez les CodeGuru révisions pour les applications AWS CDK Python 2570
Automatisez l'évaluation des ressources AWS 2582
Automatisez l'installation des systèmes SAP 2597
Automatisez le déploiement du portefeuille et des produits Service Catalog à l'aide d'AWS CDK 2611
Automatisez les sauvegardes depuis AWS CodeCommit vers Amazon S3 2630
Automatisez la suppression des CloudFormation piles 2638
Automatisez la gestion dynamique des pipelines pour déployer des solutions de correctifs 2650
Automatisez l'ingestion des métriques personnalisées Amazon MWAA 2679
Automatisez la gestion des ressources Amazon Lex à l'aide AWS CDK des CloudFormation 2696
Automatisez le déploiement d'ensembles de piles à l'aide d'AWS CodePipeline et d'AWS CodeBuild 2716
Associer automatiquement une politique gérée pour Systems Manager aux profils d' EC2 instance 2745
Créez automatiquement des pipelines CI/CD et des clusters Amazon ECS pour les microservices 2761
Créez une architecture faiblement couplée avec des microservices 2775
Créez et envoyez des images Docker vers Amazon ECR 2788
Créez et testez des applications iOS avec les services AWS 2795
Consultez les applications ou les CloudFormation modèles AWS CDK pour connaître les meilleures pratiques à l'aide de packs de règles 2801
Configurer le protocole TLS mutuel pour les applications sur Amazon EKS 2806
Création de ressources AppStream 2.0 à l'aide d'AWS CloudFormation 2818

Créez un analyseur de journal personnalisé pour Amazon ECS à l'aide de Firelens 2824
Création d'un pipeline et d'une AMI à l'aide de CodePipeline and HashiCorp Packer 2834
Créez un pipeline et déployez des mises à jour sur des EC2 instances sur site à l'aide de CodePipeline 2842
Créez des pipelines CI dynamiques pour les projets Java et Python 2852
Déployez des CloudWatch canaris Synthetics 2870
Déployer un pipeline CI/CD pour les microservices Java sur Amazon ECS 2878
Déployez une ChatOps solution pour gérer les résultats du scan SAST 2888
Déployez un pare-feu à l'aide d'AWS Network Firewall et d'AWS Transit Gateway 2906
..... 2921
Déployez un cluster Amazon EKS depuis AWS Cloud9 à l'aide d'un profil d'instance EC2 . 2926
Déployez du code dans plusieurs régions AWS 2938
Exécuter des requêtes SQL Amazon Redshift 2951
Exporter les rapports AWS Backup sous forme de fichier CSV 2964
Exporter les balises d' EC2 instance Amazon vers un fichier CSV 2974
Génération d'un CloudFormation modèle AWS contenant les règles gérées par AWS Config 2981
Donnez aux instances de SageMaker blocs-notes un accès multicompte à un référentiel CodeCommit 2988
Mettre en œuvre une stratégie GitHub de branchement Flow 3000
Mettre en œuvre une stratégie de branchement Gitflow 3011
Mettre en œuvre une stratégie de branchement Trunk 3023
Mettre en œuvre une analyse Checkov personnalisée et centralisée 3030
Initiez différents pipelines CI/CD après avoir détecté des modifications dans un monorepo 3041
Intégrer un référentiel Bitbucket à AWS Amplify 3059
Lancez un CodeBuild projet sur des comptes AWS à l'aide de Lambda 3068
Gérez le basculement multi-AZ pour les clusters EMR à l'aide d'Application Recovery Controller 3081
Gérez les déploiements bleu/vert de microservices sur plusieurs comptes et régions 3098
Surveillez les référentiels Amazon ECR pour détecter les autorisations génériques 3132
Optimisez les déploiements sans serveur multi-comptes 3137
Effectuez des actions personnalisées à partir d' CodeCommit événements AWS 3158
Fournir des AWS Service Catalog produits à l'aide d' GitHub actions 3163
Fournir des rôles IAM dotés de privilèges minimaux 3174
Publier CloudWatch les statistiques Amazon dans un fichier CSV 3188

Supprimer les EC2 entrées Amazon situées en face Comptes AWS de AWS Managed Microsoft AD 3194
Supprimer les EC2 entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD 3212
Exécutez des tests unitaires pour les tâches ETL Python dans AWS Glue 3223
Configuration des graphiques Helm v3 dans Amazon S3 3234
Configurez un pipeline CI/CD avec CodePipeline 3243
Configurez une journalisation centralisée à grande échelle à l'aide de Terraform 3259
Configurer le end-to-end chiffrement pour les applications sur Amazon EKS 3285
Simplifiez le déploiement d'applications multi-locataires Amazon EKS 3299
Abonnement de plusieurs points de terminaison de messagerie à une rubrique SNS 3318
Utilisez la structure du AWS Fargate WaitCondition crochet 3323
Utiliser des dépôts Git tiers dans AWS CodePipeline 3336
Validez les configurations Terraform à l'aide d'AWS CodePipeline 3346
Plus de modèles 3364
Infrastructure 3368
Accédez à un hôte bastion à l'aide du gestionnaire de session et d'Amazon EC2 Instance Connect 3370
Centralisez la résolution DNS en utilisant AWS Managed Microsoft AD 3388
Centralisez la surveillance à l'aide d'Observability Access Manager 3401
Vérifiez la présence de balises obligatoires dans les EC2 instances au lancement 3417
Nettoyez les ressources AFT en toute sécurité après la perte du fichier d'état 3423
Se connecter à une EC2 instance à l'aide du gestionnaire de session 3437
Créez un pipeline dans les régions AWS qui ne prennent pas en charge AWS CodePipeline 3444
Personnalisez les noms de rôles par défaut en utilisant des AWS CDK aspects et des trappes d'échappement 3452
Déployer un cluster Cassandra sur Amazon EC2 avec une statique privée IPs 3461
Étendez VRFs votre accès à AWS à l'aide de Transit Gateway Connect 3468
Recevez des notifications Amazon SNS en cas de modification de l'état des clés AWS KMS 3486
Préservez l'espace IP routable dans les conceptions VPC multi-comptes pour les sous-réseaux autres que les charges de travail 3494
Provisionner un produit Terraform dans Service Catalog à partir d'un référentiel de code 3500
Enregistrez plusieurs comptes AWS avec une seule adresse e-mail 3522

Configuration de la résolution DNS pour les réseaux hybrides dans un environnement AWS à compte unique ... 3539
Configurez automatiquement les robots UiPath RPA sur Amazon EC2 ... 3545
Configuration d'une PeopleSoft architecture à haute disponibilité sur AWS ... 3563
Configuration de la reprise après sinistre pour Oracle JD Edwards EnterpriseOne ... 3592
Configurer la détection et le signalement de la dérive ... 3623
Importation réussie d'un compartiment S3 sous forme de CloudFormation pile ... 3629
Synchronisation des systèmes de fichiers Amazon EFS dans différentes régions ... 3641
AWS Infrastructure de test à l'aide de tests LocalStack et tests Terraform ... 3650
Mettez à niveau les clusters SAP Pacemaker de ENSA1 ENSA2 ... 3658
Utilisez des zones de disponibilité cohérentes VPCs sur les différents comptes ... 3680
Utiliser l'utilisateur IDs dans les politiques IAM ... 3686
Validez le code Account Factory pour Terraform localement ... 3697
Plus de modèles ... 3717
Applications Web et mobiles ... 3721
Authentifier les utilisateurs de l'application Web React ... 3722
Déployez en continu une application Web Amplify ... 3732
Créez une application React à l'aide d'AWS Amplify et Amazon Cognito ... 3740
Création d'un portail pour les micro-frontends ... 3757
Déployez un SPA basé sur React sur Amazon S3 et CloudFront ... 3788
Déployez une API Amazon API Gateway à l'aide de points de terminaison privés et d'un Application Load Balancer ... 3796
Intégrer un tableau de QuickSight bord Amazon dans une application Angular locale ... 3804
Explorez le développement d'applications Web avec Green Boost ... 3826
Exécutez des tests unitaires à l'aide d'AWS CodeBuild ... 3855
Structurer un projet Python en architecture hexagonale ... 3865
Plus de modèles ... 3893
IoT ... 3895
Configurez la journalisation et la surveillance des événements de sécurité dans votre environnement IoT ... 3896
Récapitulatif ... 3896
Conditions préalables et limitations ... 3896
Architecture ... 3897
Outils ... 3899
Épopées ... 3900
Ressources connexes ... 3905

Extraire et interroger AWS IoT SiteWise les attributs de métadonnées 3906
Récapitulatif 3906
Conditions préalables et limitations 3906
Architecture 3907
Outils 3907
Épopées 3908
Ressources connexes 3911
Informations supplémentaires 3912
..... 3914
Récapitulatif 3914
Conditions préalables et limitations 3915
Architecture 3915
Outils 3916
Bonnes pratiques 3916
Épopées 3917
Résolution des problèmes 3932
Ressources connexes 3934
Informations supplémentaires 3935
Plus de modèles 3937
Migration et modernisation 3938
Migration 3939
Création de CloudFormation modèles AWS pour AWS DMS 3940
Commencez par la découverte automatique de portefeuilles 3944
Migrer les charges de travail Cloudera sur site vers AWS 3953
Résoudre les erreurs de connexion après la migration de SQL Server vers AWS 3971
Redémarrez automatiquement l'agent de réplication AWS sans le désactiver SELinux 3974
Ré-architecte 3982
Réhéberger 4407
Déménager 4696
Recréation de plateforme 4754
Schémas de migration par charge de travail 5412
Plus de modèles 5422
Modernisation 5424
Analyser et visualiser l'architecture logicielle dans CAST Imaging 5425
Évaluez l'état de préparation des applications avant de migrer vers AWS à l'aide de CAST Highlight 5436

Archiver automatiquement les données DynamoDB expirées sur Amazon S3 5463
Créez une architecture sans serveur multi-locataires dans Amazon Service OpenSearch .. 5480
Déployez des applications à piles multiples 5529
Déployez des applications imbriquées à l'aide d'AWS SAM 5539
Implémentez l'isolation des locataires SaaS pour Amazon S3 à l'aide d'un AWS Lambda TVM 5548
Implémentez le modèle de saga sans serveur à l'aide d'AWS Step Functions 5574
Gérez les applications de conteneur sur site avec Amazon ECS Anywhere 5589
Modernisez les applications ASP.NET Web Forms sur AWS 5599
Exécutez des charges de travail basées sur des événements avec AWS Fargate 5615
Intégration des locataires dans l'architecture SaaS 5625
Utilisez le CQRS et le sourcing d'événements 5651
Plus de modèles 5677
ordinateurs centraux 5680
Accès Services AWS depuis IBM z/OS en installant le AWS CLI 5682
Sauvegardez et archivez les données du mainframe sur Amazon S3 5704
Créez des programmes COBOL DB2 en utilisant et AWS Mainframe Modernization AWS CodeBuild 5733
Création d'un serveur PAC Micro Focus Enterprise 5759
Création d'une visionneuse de fichiers mainframe dans le cloud AWS 5780
Conteneurisez les applications Blu Age modernisées 5797
Convertir les données EBCDIC en ASCII sur AWS 5807
Convertissez des fichiers EBCDIC du mainframe en fichiers ASCII à l'aide d'AWS Lambda 5826
Convertissez des fichiers de données du mainframe avec des mises en page d'enregistrement complexes 5849
Déployer un environnement pour les applications conteneurisées 5869
Générez des informations sur les données Db2 z/OS 5880
Générez des informations en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight 5933
Intégrer le contrôleur universel Stonebranch à AWS 5952
Migrez et répliquez des fichiers VSAM vers le cloud AWS à l'aide de Precisely 5988
Modernisez la gestion des sorties du mainframe sur AWS 6006
Modernisez l'application CardDemo mainframe en utilisant AWS Transform 6060
Modernisez les charges de travail d'impression par lots de votre mainframe sur AWS 6080
Modernisez votre environnement mainframe avec Rocket Software Enterprise Suite 6110

Modernisez les charges de travail d'impression en ligne de votre mainframe sur AWS 6128
Déplacez les fichiers du mainframe vers Amazon S3 à l'aide de Transfer Family 6163
Accès utilisateur sécurisé dans une base de données de fédération DB2 6177
Transférer des données Db2 z/OS vers AWS 6187
Plus de modèles 6216
Gestion 6217
Gestion des coûts 6218
Créez des rapports détaillés sur les coûts et l'utilisation des tâches AWS Glue 6219
Créez des rapports détaillés sur les coûts et l'utilisation des clusters Amazon EMR 6225
Plus de modèles 6230
Calcul haute performance 6231
Déployez un système de fichiers Lustre à l'aide de Terraform et DRA 6232
Configurer un tableau de bord de surveillance Grafana pour AWS ParallelCluster 6241
Configuration d'un VDI à mise à l'échelle automatique à l'aide de NICE DCV 6256
Cloud hybride 6270
Configuration d'une extension de centre de données pour VMware le cloud sur AWS 6271
Configurer vRealize Automation pour le provisionner VMs sur le VMware cloud sur AWS .. 6276
Intégrer VMware vRealize Network Insight au VMware cloud sur AWS 6289
Migrez VMs vers VMware le cloud sur AWS à l'aide de HCX OSAM 6294
Envoyer des logs depuis VMware le Cloud AWS vers Splunk 6300
Configuration d'un pipeline CI/CD pour les charges de travail hybrides sur Amazon ECS Anywhere 6307
Plus de modèles 6328
Gestion et gouvernance 6329
Alerte lorsque les ressources Amazon Data Firehose ne sont pas chiffrées 6330
Automatisez l'ajout ou la mise à jour d'entrées de registre Windows 6335
Création automatique d'une RFC à l'aide de Python 6340
Arrêter et démarrer automatiquement une instance de base de données Amazon RDS 6348
Centralisez la distribution des packages logiciels dans AWS Organizations à l'aide de Terraform 6364
Configuration de la journalisation pour les applications .NET dans CloudWatch Logs 6377
Copiez les produits AWS Service Catalog entre les comptes et les régions AWS 6386
Création d'une matrice RACI pour les opérations dans le cloud 6396
Créez des alarmes pour des métriques personnalisées à l'aide de CloudWatch 6403
Création d'un IDE AWS Cloud9 avec des volumes EBS chiffrés par défaut 6411
Créez automatiquement des CloudWatch tableaux de bord basés sur des balises 6417

Documentez la conception de votre zone d'atterrissage 6427
Activez Amazon DevOps Guru au sein d'une organisation avec le kit AWS CDK 6431
Implémenter l'AFT en utilisant un pipeline bootstrap 6459
Gérez les produits AWS Service Catalog dans plusieurs comptes et régions AWS 6485
Migrer un compte AWS d'AWS Organizations vers AWS Control Tower 6493
Surveillez les clusters SAP RHEL Pacemaker 6510
Surveillez l'activité des applications avec CloudWatch Logs Insights 6532
Surveillez l'utilisation d'une AMI dans Comptes AWS 6544
Configurez des alertes pour les fermetures de comptes programmatiques dans AWS Organizations 6561
Afficher les détails des instantanés EBS pour votre compte AWS ou votre organisation 6571
Plus de modèles 6578
Messagerie et communications 6581
Automatisez la configuration de RabbitMQ dans Amazon MQ 6582
Améliorez la qualité des appels sur les postes de travail des agents dans Amazon Connect 6590
Plus de modèles 6606
Sécurité, identité et conformité 6607
Accès Services AWS depuis ASP.NET à l'aide d'Amazon Cognito 6610
Récapitulatif 6610
Conditions préalables et limitations 6610
Architecture 6611
Outils 6611
Épopées 6612
Résolution des problèmes 6617
Ressources connexes 6617
Pièces jointes 6617
Authentifier SQL Server à l'aide d'AWS Directory Service 6618
Récapitulatif 6618
Conditions préalables et limitations 6618
Architecture 6618
Outils 6619
Épopées 6619
Ressources connexes 6623
Automatisez la réponse aux incidents et la criminalistique 6624
Récapitulatif 6624

Conditions préalables et limitations 6624
Architecture 6625
Outils 6627
Épopées 6629
Ressources connexes 6633
Informations supplémentaires 6633
Pièces jointes 6633
Automatisez la correction des résultats standard du Security Hub 6634
Récapitulatif 6634
Conditions préalables et limitations 6635
Architecture 6635
Outils 6636
Bonnes pratiques 6636
Épopées 6637
Ressources connexes 6640
Pièces jointes 6640
Automatisez les analyses de sécurité pour les charges de travail entre comptes à l'aide d'Amazon Inspector 6641
Récapitulatif 6641
Conditions préalables et limitations 6641
Architecture 6642
Outils 6643
Épopées 6644
Ressources connexes 6648
Pièces jointes 6648
Audit automatique de l'accès depuis les adresses IP publiques 6649
Récapitulatif 6649
Conditions préalables et limitations 6649
Architecture 6650
Outils 6652
Bonnes pratiques 6653
Épopées 6653
Résolution des problèmes 6658
Ressources connexes 6658
Réactivez automatiquement AWS CloudTrail en utilisant les meilleures pratiques de sécurité 6659
Récapitulatif 6659

Conditions préalables et limitations 6659
Architecture 6660
Outils 6660
Épopées 6661
Ressources connexes 6667
Pièces jointes 6668
Corriger automatiquement les instances et clusters de base de données Amazon RDS non chiffrés 6669
Récapitulatif 6669
Conditions préalables et limitations 6669
Architecture 6671
Outils 6671
Bonnes pratiques 6673
Épopées 6673
Ressources connexes 6680
Informations supplémentaires 6680
Rotation automatique des clés d'accès utilisateur IAM 6682
Récapitulatif 6682
Conditions préalables et limitations 6683
Architecture 6684
Outils 6686
Épopées 6688
Ressources connexes 6698
Validez et déployez automatiquement les politiques et les rôles IAM dans un compte AWS ... 6700
Récapitulatif 6700
Conditions préalables et limitations 6701
Architecture 6702
Outils 6703
Épopées 6703
Ressources connexes 6708
Intégrez Security Hub et Jira de manière bidirectionnelle 6709
Récapitulatif 6709
Conditions préalables et limitations 6710
Architecture 6711
Outils 6712
Épopées 6713

Ressources connexes 6723
Informations supplémentaires 6723
Créez un pipeline pour les images de conteneurs renforcées 6725
Récapitulatif 6725
Conditions préalables et limitations 6725
Architecture 6726
Outils 6729
Épopées 6730
Résolution des problèmes 6738
Ressources connexes 6738
Centralisez la gestion des clés d'accès IAM dans AWS Organizations à l'aide de Terraform ... 6740
Récapitulatif 6740
Conditions préalables et limitations 6741
Architecture 6741
Outils 6743
Bonnes pratiques 6744
Épopées 6744
Résolution des problèmes 6754
Ressources connexes 6754
Consultez une CloudFront distribution Amazon pour la journalisation des accès, les versions HTTPS et TLS 6755
Récapitulatif 6755
Conditions préalables et limitations 6756
Architecture 6756
Outils 6757
Épopées 6758
Ressources connexes 6761
Pièces jointes 6761
Vérifiez les entrées du réseau à hôte unique dans les règles d'entrée du groupe de sécurité pour et IPv4 IPv6 6762
Récapitulatif 6762
Conditions préalables et limitations 6762
Architecture 6762
Outils 6763
Épopées 6764
Ressources connexes 6768

Pièces jointes 6768
Choisissez un flux d'authentification Amazon Cognito 6769
Récapitulatif 6769
Conditions préalables et limitations 6769
Architecture 6770
Outils 6774
Épopées 6775
Ressources connexes 6778
Informations supplémentaires 6779
Créez des règles AWS Config personnalisées à l'aide de Guard 6781
Récapitulatif 6781
Conditions préalables et limitations 6782
Architecture 6782
Outils 6787
Épopées 6787
Résolution des problèmes 6789
Ressources connexes 6790
Créez un rapport contenant les résultats de Prowler à partir de plusieurs Comptes AWS 6792
Récapitulatif 6792
Conditions préalables et limitations 6793
Architecture 6794
Outils 6795
Épopées 6796
Résolution des problèmes 6821
Ressources connexes 6821
Informations supplémentaires 6822
Supprimez les volumes Amazon EBS inutilisés à l'aide de AWS Config 6824
Récapitulatif 6824
Conditions préalables et limitations 6824
Architecture 6825
Outils 6825
Épopées 6826
Résolution des problèmes 6829
Ressources connexes 6830
Déployez AWS Control Tower les contrôles en utilisant AWS CDK 6831
Récapitulatif 6831

Conditions préalables et limitations 6832
Architecture 6833
Outils 6834
Bonnes pratiques 6835
Épopées 6835
Ressources connexes 6842
Informations supplémentaires 6843
Déployez AWS Control Tower des contrôles à l'aide de Terraform 6846
Récapitulatif 6846
Conditions préalables et limitations 6847
Architecture 6848
Outils 6849
Bonnes pratiques 6849
Épopées 6850
Résolution des problèmes 6855
Ressources connexes 6857
Informations supplémentaires 6857
Déployez un pipeline qui détecte les problèmes de sécurité dans le code 6861
Récapitulatif 6861
Conditions préalables et limitations 6861
Architecture 6862
Outils 6863
Épopées 6863
Résolution des problèmes 6866
Ressources connexes 6867
Informations supplémentaires 6867
Déployez des contrôles de détection pour les sous-réseaux publics 6869
Récapitulatif 6869
Conditions préalables et limitations 6870
Architecture 6870
Outils 6871
Bonnes pratiques 6872
Épopées 6872
Ressources connexes 6881
Informations supplémentaires 6882
Déployez des contrôles préventifs pour les sous-réseaux publics 6885

Récapitulatif 6885
Conditions préalables et limitations 6885
Architecture 6886
Outils 6887
Épopées 6888
Ressources connexes 6895
Informations supplémentaires 6896
Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform 6898
Récapitulatif 6898
Conditions préalables et limitations 6898
Architecture 6899
Outils 6899
Bonnes pratiques 6900
Épopées 6900
Résolution des problèmes 6904
Ressources connexes 6904
Détecter les instances Amazon RDS dont les certificats CA expirent 6905
Récapitulatif 6905
Conditions préalables et limitations 6905
Architecture 6906
Outils 6908
Bonnes pratiques 6909
Épopées 6909
Résolution des problèmes 6914
Ressources connexes 6914
Générez dynamiquement une politique IAM avec IAM Access Analyzer 6915
Récapitulatif 6915
Conditions préalables et limitations 6915
Architecture 6916
Outils 6917
Épopées 6919
Ressources connexes 6926
Activer GuardDuty l'utilisation CloudFormation de modèles 6927
Récapitulatif 6927
Conditions préalables et limitations 6927
Architecture 6927

Outils 6928
Épopées 6929
Ressources connexes 6930
Informations supplémentaires 6931
Activez le chiffrement transparent des données dans Amazon RDS for SQL Server 6935
Récapitulatif 6935
Conditions préalables et limitations 6935
Architecture 6935
Outils 6936
Épopées 6936
Ressources connexes 6939
Assurez-vous que les équilibreurs de charge AWS utilisent des protocoles d'écoute sécurisés 6940
Récapitulatif 6940
Conditions préalables et limitations 6940
Architecture 6941
Outils 6941
Bonnes pratiques 6942
Épopées 6942
Résolution des problèmes 6946
Ressources connexes 6946
Pièces jointes 6946
Garantissez le chiffrement des données Amazon EMR au repos 6947
Récapitulatif 6947
Conditions préalables et limitations 6947
Architecture 6948
Outils 6948
Épopées 6949
Ressources connexes 6952
Pièces jointes 6952
Assurez-vous qu'un profil IAM est associé à une instance EC2 6953
Récapitulatif 6953
Conditions préalables et limitations 6953
Architecture 6954
Outils 6954
Épopées 6955

Ressources connexes 6958
Pièces jointes 6958
Assurez-vous que les nouveaux clusters Amazon Redshift sont chiffrés 6959
Récapitulatif 6959
Conditions préalables et limitations 6959
Architecture 6959
Outils 6960
Épopées 6961
Ressources connexes 6963
Pièces jointes 6963
Exporter un rapport sur les identités de l'IAM Identity Center et leurs attributions 6964
Récapitulatif 6964
Conditions préalables et limitations 6964
Architecture 6966
Outils 6966
Épopées 6967
Résolution des problèmes 6968
Ressources connexes 6970
Informations supplémentaires 6971
Empêchez la suppression planifiée des clés KMS 6973
Récapitulatif 6973
Conditions préalables et limitations 6973
Architecture 6974
Outils 6975
Épopées 6976
Ressources connexes 6979
Informations supplémentaires 6980
Pièces jointes 6980
Identifiez les compartiments Amazon S3 publics dans AWS Organizations 6981
Récapitulatif 6981
Conditions préalables et limitations 6981
Architecture 6982
Outils 6983
Épopées 6984
Résolution des problèmes 6988
Ressources connexes 6989

Informations supplémentaires 6989
Ingérez les journaux de sécurité AWS dans Microsoft Sentinel 6990
Récapitulatif 6990
Conditions préalables et limitations 6990
Architecture 6992
Outils 6993
Bonnes pratiques 6994
Épopées 6994
Ressources connexes 7006
Gérez les AWS Organizations politiques sous forme de code 7007
Récapitulatif 7007
Conditions préalables et limitations 7008
Architecture 7008
Outils 7010
Bonnes pratiques 7011
Épopées 7011
Résolution des problèmes 7031
Ressources connexes 7033
Informations supplémentaires 7034
Gérez les ensembles d'autorisations IAM Identity Center à l'aide de CodePipeline 7036
Récapitulatif 7036
Conditions préalables et limitations 7036
Architecture 7038
Outils 7039
Bonnes pratiques 7040
Épopées 7040
Résolution des problèmes 7052
Ressources connexes 7053
Gérez les informations d'identification avec AWS Secrets Manager 7054
Récapitulatif 7054
Conditions préalables et limitations 7054
Architecture 7055
Outils 7055
Épopées 7055
Ressources connexes 7057
Informations supplémentaires 7057

.... 7060
Récapitulatif 7060
Conditions préalables et limitations 7060
Architecture 7061
Outils 7061
Épopées 7062
Ressources connexes 7065
Pièces jointes 7065
Surveillez les clusters Amazon EMR pour le chiffrement en transit lors du lancement 7066
Récapitulatif 7066
Conditions préalables et limitations 7067
Architecture 7067
Outils 7068
Épopées 7069
Ressources connexes 7071
Pièces jointes 7071
Surveillez les ElastiCache clusters Amazon pour le chiffrement au repos 7072
Récapitulatif 7072
Conditions préalables et limitations 7073
Architecture 7074
Outils 7074
Épopées 7075
Ressources connexes 7077
Pièces jointes 7078
Surveiller les paires de clés des EC2 instances 7079
Récapitulatif 7079
Conditions préalables et limitations 7079
Architecture 7079
Outils 7080
Épopées 7081
Ressources connexes 7085
Pièces jointes 7085
Surveiller l'activité de l'utilisateur root IAM 7086
Récapitulatif 7086
Conditions préalables et limitations 7086
Architecture 7087

Outils 7087
Épopées 7089
Ressources connexes 7094
Informations supplémentaires 7094
Avertir lorsqu'un utilisateur IAM est créé 7095
Récapitulatif 7095
Conditions préalables et limitations 7095
Architecture 7095
Outils 7096
Épopées 7097
Ressources connexes 7099
Pièces jointes 7100
Empêchez l'accès à Internet en utilisant un SCP 7101
Récapitulatif 7101
Conditions préalables et limitations 7101
Outils 7102
Bonnes pratiques 7102
Épopées 7103
Ressources connexes 7105
Restreindre l'accès en fonction de l'adresse IP ou de la géolocalisation 7106
Récapitulatif 7106
Conditions préalables et limitations 7106
Outils 7107
Épopées 7108
Ressources connexes 7113
Analyser les référentiels Git à la recherche d'informations sensibles 7115
Récapitulatif 7115
Conditions préalables et limitations 7115
Architecture 7115
Outils 7116
Bonnes pratiques 7116
Épopées 7116
Ressources connexes 7120
Envoyer des alertes depuis AWS Network Firewall vers un canal Slack 7121
Récapitulatif 7121
Conditions préalables et limitations 7121

Architecture 7122
Outils 7123
Épopées 7124
Ressources connexes 7130
Informations supplémentaires 7130
Simplifiez la gestion des certificats privés en utilisant AWS Private CA et AWS RAM 7135
Récapitulatif 7135
Conditions préalables et limitations 7136
Architecture 7136
Outils 7137
Épopées 7138
Ressources connexes 7148
Informations supplémentaires 7148
Désactiver les contrôles standard de sécurité sur tous les comptes membres du Security Hub 7149
Récapitulatif 7149
Conditions préalables et limitations 7149
Architecture 7150
Outils 7151
Épopées 7152
Ressources connexes 7156
Mettez à jour les informations d'identification de la CLI AWS depuis IAM Identity Center à l'aide de PowerShell 7157
Récapitulatif 7157
Conditions préalables et limitations 7157
Architecture 7158
Outils 7158
Bonnes pratiques 7159
Épopées 7159
Résolution des problèmes 7162
Ressources connexes 7162
Informations supplémentaires 7163
Utiliser AWS Config pour surveiller Amazon Redshift 7165
Récapitulatif 7165
Conditions préalables et limitations 7165
Architecture 7166

Outils 7166
Épopées 7167
Ressources connexes 7170
Informations supplémentaires 7171
Utilisez Network Firewall pour capturer les noms de domaine DNS à partir du trafic réseau sortant 7172
Récapitulatif 7172
Conditions préalables et limitations 7172
Architecture 7173
Outils 7173
Épopées 7174
Utilisez Terraform pour activer automatiquement GuardDuty 7191
Récapitulatif 7191
Conditions préalables et limitations 7192
Architecture 7194
Outils 7195
Épopées 7196
Ressources connexes 7205
Informations supplémentaires 7206
Vérifiez les meilleures pratiques pour la norme PCI DSS 4.0 7207
Récapitulatif 7207
Conditions préalables et limitations 7208
Outils 7209
Épopées 7209
Ressources connexes 7212
Informations supplémentaires 7212
Pièces jointes 7213
..... 7214
Récapitulatif 7214
Conditions préalables et limitations 7214
Architecture 7215
Outils 7215
Épopées 7216
Ressources connexes 7219
Pièces jointes 7219
..... 7220

Récapitulatif 7220
Conditions préalables et limitations 7220
Architecture 7221
Outils 7221
Épopées 7222
Ressources connexes 7225
Pièces jointes 7225
Plus de modèles 7226
..... 7229

AWS Modèles d'orientation prescriptifs

Les modèles de directives prescriptives d'Amazon Web Services (AWS) fournissent des step-by-step instructions, une architecture, des outils et du code pour la mise en œuvre de scénarios spécifiques de migration, de modernisation et de déploiement dans le cloud. Ces modèles, qui sont approuvés par des experts en la matière chez AWS, sont destinés aux créateurs et aux utilisateurs pratiques qui envisagent ou sont en train de migrer vers. AWS Ils prennent également en charge les utilisateurs déjà connectés AWS et qui cherchent des moyens d'optimiser ou de moderniser leurs opérations dans le cloud.

Vous pouvez utiliser ces modèles pour transférer vos charges de travail sur site ou dans le cloud de complexité variable vers le cloud AWS et pour accélérer vos efforts d'adoption, d'optimisation et de modernisation du cloud, que vous en soyez à la phase de validation de concept, de planification ou de mise en œuvre de votre projet. Par exemple, pour un projet de migration vers le cloud :

- Au cours de la phase de planification, vous pouvez évaluer les différentes options de migration disponibles AWS. Vous pouvez choisir le modèle adapté à vos besoins, selon que vous souhaitez déménager, réhéberger, replateforme ou réarchitecture. Vous pouvez également comprendre les différents outils disponibles pour la migration et commencer à planifier l'achat de licences ou entamer des conversations initiales avec les fournisseurs.
- Au cours des phases de validation du concept et de mise en œuvre, vous pouvez suivre les step-by-step instructions fournies dans le modèle pour migrer votre charge de travail vers AWS. Chaque modèle inclut des détails tels que les prérequis, les architectures de référence cibles, les outils, step-by-step les tâches, les meilleures pratiques, le dépannage et le code.
- Si vous utilisez déjà le AWS Cloud, vous pouvez trouver des modèles qui vous aideront à moderniser, optimiser, adapter et sécuriser votre utilisation des ressources du cloud.

Pour consulter les listes de modèles par domaine technique, utilisez les liens suivants ou les options de filtrage et de recherche sur la page d'accueil du guide AWS prescriptif.

- Fondements du cloud
- IA et apprentissage automatique
- Analyse
- Calcul
- Bases de données et stockage

- Outils pour développeurs
- IoT
- Migration et modernisation
- Gestion
- Sécurité, identité et conformité

Pour consulter toutes les publications, y compris les guides, les stratégies et les modèles, consultez la page d'accueil des directives AWS prescriptives.

Fondements du cloud

Rubriques

- Automatisez la création de comptes à l'aide de l'accélérateur Landing Zone sur AWS
- Inventaire automatique AWS des ressources sur plusieurs comptes et régions
- Configurer les journaux de flux VPC pour les centraliser sur les comptes AWS
- Marquez automatiquement les pièces jointes à Transit Gateway à l'aide d'AWS Organizations
- Plus de modèles

Automatisez la création de comptes à l'aide de l'accélérateur Landing Zone sur AWS

Créée par Justin Kuskowski (AWS), Joe Behrens (AWS) et Nathan Scott (AWS)

Récapitulatif

Ce modèle explique comment utiliser la AWS solution Landing Zone Accelerator pour déployer automatiquement une nouvelle solution Compte AWS lorsqu'un utilisateur autorisé soumet une demande. Il permet AWS Step Functions d'orchestrer un certain nombre de AWS Lambda fonctions. Les fonctions Lambda ajoutent les informations du compte à un référentiel Git, initient un AWS CodePipeline pipeline et valident le provisionnement AWS des ressources nécessaires. Lorsque le processus est terminé, l'utilisateur reçoit une notification indiquant que le compte a été créé.

Vous pouvez éventuellement intégrer des groupes d'identifiants Microsoft Entra et attribuer des ensembles AWS IAM Identity Center d'autorisations lors du processus de création de compte. Si votre organisation utilise l'identifiant Microsoft Entra comme source d'identité, cette fonctionnalité facultative vous permet de gérer et de configurer automatiquement l'accès au nouveau compte.

Conditions préalables et limitations

Prérequis

- Accès au compte de gestion dans AWS Organizations
- AWS Cloud Development Kit (AWS CDK) version 2.118.0 ou ultérieure, installée et configurée
- Python version 3.9 ou ultérieure, installée
- AWS Command Line Interface (AWS CLI) version 2.13.19 ou ultérieure, installée
- Docker version 24.0.6 ou ultérieure, installé
- Landing Zone Accelerator sur AWS solution, déployé dans le compte de gestion
- (Facultatif) Microsoft Entra ID et IAM Identity Center, intégrés

Limites

Le flux de travail de création de compte prend en charge les exécutions séquentielles pour déployer un compte unique Compte AWS. Cette limitation garantit que le processus de création de compte s'est terminé avec succès sans avoir à se disputer les ressources lors d'une exécution parallèle.

Architecture

Architecture cible

L'image suivante montre l'architecture de haut niveau permettant d'automatiser la création d'une nouvelle zone à l'aide Compte AWS de l'accélérateur de zone d'atterrissage activé AWS. AWS Step Functions orchestre l'automatisation. Chaque tâche du flux de travail Step Functions est exécutée par une ou plusieurs AWS Lambda fonctions.

Le schéma suivant illustre le flux de travail suivant :

1. L'utilisateur demande un compte en exécutant un script Python ou en utilisant Amazon API Gateway.
2. Le flux de travail Account Creation Orchestrator démarre dans. AWS Step Functions
3. Le flux de travail met à jour le `account-config.yaml` fichier dans le référentiel de code source. Il lance également l'accélérateur de zone d'atterrissage sur le AWS pipeline et vérifie l'état du pipeline. Ce pipeline crée et configure le nouveau compte. Pour plus d'informations sur son fonctionnement, consultez la présentation de l'architecture de l'accélérateur de zone d'atterrissage activé AWS.
4. (Facultatif) Lorsque le pipeline est terminé, le flux de travail vérifie si le groupe existe dans Microsoft Entra ID. Si le groupe n'existe pas dans l'identifiant Microsoft Entra, le flux de travail l'ajoute à l'identifiant Microsoft Entra.
5. Le flux de travail exécute des étapes supplémentaires que la AWS solution Landing Zone Accelerator ne peut pas effectuer. Les étapes par défaut sont les suivantes :
   - Création d'un alias de compte dans AWS Identity and Access Management (IAM)
   - Attacher des tags au compte dans AWS Organizations
   - Création de paramètres dans AWS Systems Manager Parameter Store en fonction des balises attribuées au compte
6. (Facultatif) Le flux de travail attribue un ou plusieurs ensembles d'autorisations au groupe Microsoft Entra ID que vous avez précédemment spécifié. Les ensembles d'autorisations permettent aux utilisateurs du groupe d'accéder au nouveau compte et d'effectuer les actions que vous configurez.
7. Une AWS Lambda fonction exécute des tests d'assurance qualité et de validation. Il valide la création des ressources, vérifie que les balises ont été créées et que les ressources de sécurité ont été déployées.

8. Le flux de travail libère le compte et utilise Amazon Simple Email Service (Amazon SES) pour informer l'utilisateur que le processus s'est terminé avec succès.

Pour plus d'informations sur le flux de travail Step Functions, voir le diagramme de flux de travail Step Functions dans la section Informations supplémentaires de ce modèle.

Applications Microsoft Entra ID

Si vous choisissez d'intégrer Microsoft Entra ID, vous créez les deux applications suivantes lorsque vous déployez ce modèle :

- Application liée à IAM Identity Center et garantissant que les groupes d'identifiants Microsoft Entra sont disponibles dans IAM Identity Center. Dans cet exemple, cette application Microsoft Entra ID est nomméeLZA2.
- Application qui permet à une fonction Lambda de communiquer avec l'identifiant Microsoft Entra et d'appeler le Microsoft Graph. APIs Dans ce modèle, cette application est nomméecreate_aws_account.

Ces applications collectent des données qui sont utilisées pour synchroniser le groupe d'identifiants Microsoft Entra et attribuer des ensembles d'autorisations.

Outils

Services AWS

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle. Dans ce modèle, vous utilisez API Gateway pour vérifier la disponibilité des Compte AWS noms, lancer le AWS Step Functions flux de travail et vérifier le statut de l'exécution de Step Functions.
- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, des AWS Lambda fonctions, des points de terminaison d'invocation HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS Cette solution utilise

une EventBridge règle qui lance une fonction Lambda si l'état du flux de travail Step Functions passe à `FailedTimed-out`, ou. `Aborted`

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS IAM Identity Centervous permet de gérer de manière centralisée l'accès par authentification unique (SSO) à toutes vos applications Comptes AWS et à celles du cloud.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données. Dans ce modèle, AWS KMS les clés sont utilisées pour chiffrer les données, telles que les données stockées dans Amazon Simple Storage Service (Amazon S3), les variables d'environnement Lambda et les données dans Step Functions.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- Amazon Simple Email Service (Amazon SES) vous permet d'envoyer et de recevoir des e-mails en utilisant vos propres adresses e-mail et domaines. Une fois qu'un nouveau compte a été créé avec succès, vous recevez une notification via Amazon SES.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Si une erreur se produit lors du processus de création du compte, Amazon SNS envoie une notification aux adresses e-mail que vous configurez.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.
- AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Autres outils

- awscurl automatise le processus de signature des demandes d' AWS API et vous aide à effectuer des demandes sous la forme d'une commande curl standard.
- Microsoft Entra ID, anciennement connu sous le nom d'Azure Active Directory, est un service de gestion des identités et des accès basé sur le cloud.

- Microsoft Graph APIs vous permet d'accéder aux données et aux informations dans les services cloud de Microsoft, tels que Microsoft Entra et Microsoft 365.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub lza-account-creation-workflowréférentiel.

Le répertoire lambda_layer contient les couches suivantes, qui sont référencées dans plusieurs fonctions Lambda :

- account_creation_helper — Cette couche inclut les modules permettant d'assumer des rôles et de suivre la progression. AWS Service Catalog
- boto3 — Cette couche inclut le AWS SDK pour Python (Boto3)module pour s'assurer qu'il AWS Lambda dispose de la dernière version.
- identity_center_helper — Cette couche prend en charge les appels à IAM Identity Center.

Le répertoire lambda_src contient les fonctions Lambda suivantes :

- AccountTagToSsmParameter— Cette fonction utilise les balises associées au compte afin AWS Organizations de créer des paramètres dans Parameter Store. Chaque paramètre commence par un `/account/tags/` préfixe.
- AttachPermissionSet— Cette fonction ajoute un ensemble d'autorisations à un groupe IAM Identity Center.
- Azure ADGroup Sync — Cette fonction synchronise le groupe d'identifiants Microsoft Entra cible avec IAM Identity Center.
- CheckForRunningProcesses— Cette fonction vérifie si le `AWSAccelerator-Pipeline` pipeline est en cours d'exécution. Si le pipeline est en cours d'exécution, la fonction retarde le AWS Step Functions flux de travail.
- CreateAccount— Cette fonction utilise AWS Service Catalog et AWS Control Tower pour créer le nouveau Compte AWS.
- CreateAdditionalResources— Cette fonction crée les AWS ressources qui ne sont pas gérées par Landing Zone Accelerator AWS CloudFormation, telles que l'alias et les AWS Service Catalog tags du compte.
- GetAccountStatus— Cette fonction recherche le produit approvisionné afin de AWS Service Catalog déterminer si le processus de création de compte est terminé.

- GetExecutionStatus— Cette fonction récupère le statut d'une AWS Step Functions exécution en cours ou terminée.
- NameAvailability— Cette fonction vérifie si un Compte AWS nom existe déjà dans AWS Organizations.
- ReturnResponse— Si la création du compte est réussie, cette fonction renvoie l'identifiant du nouveau compte. Si la création du compte n'a pas abouti, un message d'erreur est renvoyé.
- RunStepFunction— Cette fonction exécute le AWS Step Functions flux de travail qui crée le compte.
- SendEmailWithSES — Cette fonction envoie des e-mails aux utilisateurs qui attendent la fin de la création du compte.
- ADGroupSyncToValider l'authentification unique : cette fonction vérifie si les groupes d'identifiants Microsoft Entra spécifiés sont synchronisés avec IAM Identity Center.
- ValidateResources— Cette fonction vérifie que toutes les AWS Control Tower personnalisations ont été exécutées avec succès.

Bonnes pratiques

Nous recommandons les conventions de dénomination suivantes pour AWS CDK :

- Commencez tous les paramètres par un `p` préfixe.
- Commencez toutes les conditions par un `c` préfixe.
- Commencez toutes les ressources par un `r` préfixe.
- Démarrez toutes les sorties par un `o` préfixe.

Épopées

Déployer les rôles IAM pour la validation et le balisage

Tâche	Description	Compétences requises
Préparez l'accélérateur de zone d'atterrissage à AWS des fins de personnalisation.	1. Dans le référentiel de AWS code Landing Zone Accelerator on, créez un fichier nommé`customizations-config.yaml` .	AWS DevOps

Tâche	Description	Compétences requises
	Vous utilisez ce fichier pour définir les personnalisations de la solution principale. Pour plus d'informations, consultez la section Personnalisation de la solution. 2. Dans le `customizations-config.yaml` fichier, créez une section intituléecloudFormationStacks .	

Tâche	Description	Compétences requises
Préparez-vous à déployer le `lza-account-creation-validation` rôle.	À présent, vous pouvez personnaliser la solution pour déployer le rôle `lza-account-creation-validation` IAM dans tous les comptes autres que le compte de gestion. Ce rôle fournit à la fonction `ValidateResources` Lambda un accès en lecture seule aux nouveaux comptes. 1. Téléchargez le fichier account-creation-validation-role.yaml depuis. GitHub 2. Enregistrez le fichier à l'emplacement indiqué dans la section des modèles du `customizations-config.yaml` fichier. 3. Ouvrez le fichier `customizations-config.yaml` . 4. Dans la `cloudFormationStacks` section, ajoutez le code suivant. Mettez à jour la cible Région AWS selon les besoins pour votre zone d'atterrissage : `- deploymentTargets: organizationalUnits:`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>- Root
	excludedA
	ccounts:
	-
	Management
	
	descripti
	on: IAM Role to allow
	Account Validation
	name: lza-
	account-creation-
	validation
	regions:
	- us-
	east-1
	template:
	cloudformation/acc
	ount-creation-vali
	dation-role.yaml
	runOrder: 1
	terminati
	onProtection: true
	parameters:
	- name:
	pManagementAccount
	Id
	value:
	"{{ account Managemen
	t }}"</pre> 5. Enregistrez et fermez le fichier `customiza tions-config.yaml` .	

Tâche	Description	Compétences requises
Préparez-vous à déployer le `account-tagging-to-ssm-parameter-role` rôle.	À présent, vous pouvez personnaliser la solution pour déployer le rôle `account-tagging-to-ssm-parameter-role` IAM dans tous les comptes autres que le compte de gestion. Ce rôle est utilisé pour créer les paramètres dans AWS Systems Manager Parameter Store. 1. Téléchargez le fichier account-tagging-to-ssm-parameter-role.yaml depuis. GitHub 2. Enregistrez le fichier à l'emplacement indiqué dans la section des modèles du `customizations-config.yaml` fichier. 3. Ouvrez le fichier `customizations-config.yaml` . 4. Dans la `cloudFormationStacks` section, ajoutez le code suivant. Mettez à jour la cible Région AWS selon les besoins pour votre zone d'atterrissage : `- deploymentTargets:`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>organizat
	ionalUnits:
	- Root
	excludedA
	ccounts:
	-
	Management
	descripti
	on: IAM Role to
	create SSM Parameter
	s based on Account
	Tagging
	name: lza-
	account-tagging-to-
	ssm-parameter
	regions:
	- us-
	east-1
	template:
	cloudformation/acc
	ount-tagging-to-ss
	m-parameter-role.y
	aml
	runOrder: 1
	terminati
	onProtection: true
	
	parameters:
	- name:
	pManagementAccount
	Id
	value:
	"{{ account Managemen
	t }}"</pre> 5. Enregistrez et fermez le fichier `customizations-config.yaml` .	

Tâche	Description	Compétences requises
Préparez-vous à déployer le `config-log-validation-role` rôle.	À présent, vous pouvez personnaliser la solution pour déployer le rôle `config-log-validation-role` IAM dans le compte d'archivage des journaux. Ce rôle permet à la fonction `ValidateResources` Lambda d'accéder au compartiment Amazon S3 pour les règles de journalisation et d'accès AWS Config . 1. Téléchargez le fichier config-log-validation-role.yaml depuis. GitHub 2. Enregistrez le fichier à l'emplacement indiqué dans la section des modèles du `customizations-config.yaml` fichier. 3. Ouvrez le fichier `customizations-config.yaml` . 4. Dans la `cloudFormationStacks` section, ajoutez le code suivant. Mettez à jour la cible Région AWS selon les besoins pour votre zone d'atterrissage : `- deploymentTargets: accounts:`	AWS DevOps

Tâche	Description	Compétences requises
	<pre> - LogArchive description: IAM Role to validate Config and Logs name: lza-config-log-validation-role regions: - us-east-1 template: cloudformation/config-log-validation-role.yaml runOrder: 1 terminationProtection: true parameters: - name: pManagementAccountId value: "{{ account Management }}"</pre>5. Enregistrez, fermez et validez les modifications apportées au `customizations-config.yaml` fichier.	

(Facultatif) Obtenir des données à partir de l'identifiant Microsoft Entra

Tâche	Description	Compétences requises

Créez l'application qui permet à une fonction Lambda de communiquer avec l'identifiant Microsoft Entra.	1. Dans le centre d'administration Microsoft Entra ID, enregistrez l'`create_aws_account` application. Pour obtenir des instructions, voir Enregistrer une application dans la documentation Microsoft.
	2. Suivez les instructions de la section Mettre à jour les autorisations demandées par une application dans la documentation Microsoft pour configurer les autorisations Microsoft Graph suivantes pour l'`create_aws_account` application :
	• Application. Tout lire
	  • Type : Demande
	  • Consentement de l'administrateur requis : Oui
	• AppRoleAssignment. ReadWrite.Tout
	  • Type : Demande
	  • Consentement de l'administrateur requis : Oui
	• Groupe. ReadWrite.Tout
	  • Type : Demande
		Identifiant Microsoft Entra

Tâche	Description	Compétences requises

	• Consentement de l'administrateur requis : Oui
	• ServicePrincipalEndpoint. Lisez. Tout
	  • Type : Demande
	  • Consentement de l'administrateur requis : Oui
	• Synchronisation. ReadWrite.Tout
	  • Type : Demande
	  • Consentement de l'administrateur requis : Oui
	• Utilisateur.Read
	  • Type : Délégué
	  • Consentement de l'administrateur requis : Non	

Tâche	Description	Compétences requises
Récupérez les valeurs de l'`create_aws_account` application.	À présent, vous pouvez récupérer les valeurs dont vous avez besoin pour l'`create_aws_account` application. 1. Dans le centre d'administration Microsoft Entra ID, accédez à Inscriptions d'applications, puis choisissez`create_aws_account` . 2. Dans le volet de gauche, sélectionnez Vue d'ensemble. 3. Sur la page Vue d'ensemble, notez les valeurs suivantes : • ID de l'application (client) • ID du répertoire (locataire) 4. Dans le volet de gauche, sous Gérer, sélectionnez Certificats et secrets. 5. Sur la page Certificats et secrets, choisissez l'onglet Secrets clients, puis notez les valeurs suivantes : • Valeur secrète du client • ID secret du client	Identifiant Microsoft Entra

Tâche	Description	Compétences requises
Créez l'application qui intègre Microsoft Entra ID à IAM Identity Center.	Dans le centre d'administration Microsoft Entra ID, enregistrez l'`LZA2`application. Pour obtenir des instructions, voir Enregistrer une application dans la documentation Microsoft.	Identifiant Microsoft Entra

Tâche	Description	Compétences requises
Récupérez les valeurs de l'LZA2application.	À présent, vous pouvez récupérer les valeurs dont vous avez besoin pour l'LZA2application. 1. Dans le centre d'administration Microsoft Entra ID, accédez aux applications d'entreprise, puis choisissez zLZA2. 2. Dans le volet de gauche, sélectionnez Vue d'ensemble. 3. Sur la page Vue d'ensemble, notez les valeurs suivantes : • Nom • ID de l'objet 4. Dans le volet de gauche, sous Gérer, sélectionnez Manifest. 5. Dans le fichier JSON, dans la `appRoles` section, recherchez le rôle d'application nomméUser. 6. Notez la `id` valeur de ce rôle d'application.	Identifiant Microsoft Entra

Tâche	Description	Compétences requises

Créez un secret.	1. Dans le AWS CLI, entrez la commande suivante pour créer les variables. Utilisez les valeurs que vous avez récupérées pour les LZA2 applications `create_aws_account` et :
	`# Variables for create_aws_account app`
	`TENANT_ID='<Directory ID>'`
	`CLIENT_ID='<Application ID>'`
	`SECRET_ID='<Client secret ID>'`
	`SECRET_VALUE='<Client secret value>'`
	`# Variables for LZA2 app`
	`OBJECT_ID='<Object ID>'`
	`APP_ROLE_ID='<App role ID>'`
	`ENTERPRISE_APP_NAME='<Name>'`
	2. Entrez la commande suivante pour créer un secret nommé `GraphApiSecret` dans AWS Secrets Manager :
	`aws secretsmanager create-secret \`
	`--name GraphApiSecret \`
		AWS DevOps

Tâche	Description	Compétences requises

	<pre>--secret-string
	"{\"client_id\":
	\"${CLIENT_ID}\",
	\"tenant_id\":
	\"${TENANT_ID}\",
	\"object_id\":
	\"${OBJECT_ID}\",
	\"app_role_id\":
	\"${APP_ROLE_ID}\"
	, \"secret_value\":
	\"${SECRET_VALUE}\
	", \"secret_id\":
	\"${SECRET_ID}\"}"</pre> Si vous devez mettre à jour le secret à l'avenir, vous pouvez mettre à jour les variables et exécuter la commande suivante : <pre>aws secretsmanager
	update-secret \
	--secret-id
	GraphApiSecret \
	--secret-string
	"{\"client_id\":
	\"${CLIENT_ID}\",
	\"tenant_id\":
	\"${TENANT_ID}\",
	\"object_id\":
	\"${OBJECT_ID}\",
	\"app_role_id\":
	\"${APP_ROLE_ID}\"
	, \"secret_value\":
	\"${SECRET_VALUE}\
	", \"secret_id\":
	\"${SECRET_ID}\"}"</pre>	

Déployez la solution

Tâche	Description	Compétences requises

Clonez le code source.	1. Entrez la commande suivante pour cloner le lza-account-creation-workflowréférentiel :
	`git clone https://github.com/aws-samples/lza-account-creation-workflow`
	2. Entrez la commande suivante pour accéder au `config` répertoire du dépôt cloné :
	`cd lza-account-creation-workflow/config`
		DevOps ingénieur

Mettez à jour le `deploy-config.yaml` fichier.	1. Ouvrez le fichier `deploy-config.yaml` . 2. Passez en revue le modèle et mettez à jour les valeurs selon les besoins pour le déploiement dans votre AWS environnement. Par exemple, mettez à jour les valeurs pour les éléments suivants : • `accountCreationFailure` • `accountCompletionFromEmail` • `ssoLoginUrl`	AWS DevOps

Tâche	Description	Compétences requises
	• `rootEmailPrefix` • `rootEmailDomain` 3. Si vous effectuez l'intégration à l'aide de Microsoft Entra ID, procédez comme suit : • Définissez `enableAzureADIntegration` sur `true`. • Pour `graphApiSecretName` valeur, entrez le secret que vous avez créé précédemment (`GraphApiSecret`). 4. Enregistrez et fermez le fichier `deploy-config.yaml` .	

Tâche	Description	Compétences requises

Déployez la solution dans votre AWS environnement.	1. Entrez la commande suivante :
	`cdk bootstrap <account-number>/<Region>`
	Pour plus d'informations, consultez Bootstrap ping dans la AWS CDK documentation.
	2. Entrez la commande suivante pour synthétiser le CloudFormation modèle :
	`cdk synth`
	Pour plus d'informations, voir Configurer et effectuer une synthèse de AWS CDK pile dans la AWS CDK documentation.
	3. Entrez la commande suivante pour déployer la solution.
	`cdk deploy`
	Pour plus d'informations, consultez la section Déployer AWS CDK des applications dans la AWS CDK documentation.
		AWS DevOps

Tâche	Description	Compétences requises
	Note Cette solution utilise un compartiment Amazon S3 pour stocker le code source de cette solution. Vous pouvez utiliser le script upload_to_source_bucket.py pour créer une archive du code source et télécharger une version mise à jour.	

Option 1 — Création d'un compte en Python

Tâche	Description	Compétences requises
Identifiez les arguments à utiliser.	Choisissez les arguments à utiliser lorsque vous exécutez le script Python qui lance le flux de travail Step Functions. Pour une liste complète des arguments, consultez la section Informations supplémentaires de ce modèle.	AWS DevOps, Python
Lancez le script Python.	1. Entrez la commande suivante pour accéder au référentiel cloné :	DevOps ingénieur, Python

Tâche	Description	Compétences requises

	`cd lza-account-creation-workflow`
	2. Exécutez le script Python qui lance le flux de travail Step Functions. Voici un exemple de commande qui inclut des exemples d'arguments et de valeurs :
	`python ./run-stepfunction.py \ --account-name "lza-test-01" \ --support-dl "johnsmith@example.com" \ --managed-org-unit "Workloads/Workload-1" \ --purpose "Testing new micro service" \ --force-update true \ --ad-integration "{\"CustomerAccountAdmin\": \"platform-admin\", \"CustomerAccountDev\": \"workload1-app1\"}" \ --bypass-creation true \ --tags APPLICATION=TestingMicroService`
	3. Attendez de recevoir une notification indiquant que	

Tâche	Description	Compétences requises
	le compte a été créé avec succès. **Note** Si le processus de création de compte échoue, Amazon SNS envoie une notification aux adresses e-mail que vous avez définies `accountCreationFailure` dans le `deploy-config.yaml` fichier. Le demandeur du compte n'est pas averti.	

Option 2 — Créez un compte à l'aide d'API Gateway et d'awscurl

Tâche	Description	Compétences requises
Configurez les variables pour awscurl.	1. Entrez la commande suivante pour accéder au répertoire du code source : `cd lza-account-creation-workflow` 2. Entrez la commande suivante pour définir les variables de clé AWS	AWS DevOps

Tâche	Description	Compétences requises

	d'accès. Vous pouvez copier les variables depuis le portail AWS d'accès, puis les coller dans un shell. Voici un exemple :
	`export AWS_ACCES S_KEY_ID="<id>" export AWS_SECRE T_ACCESS_KEY="<key >" export AWS_SESSI ON_TOKEN="<token>"`
	3. Entrez la commande suivante pour définir les Région AWS appels d'API :
	`export AWS_REGION= $(aws configure get region)`
	4. Entrez la commande suivante pour récupérer le point de terminaison API Gateway à partir de la `lza-account-creati on-workflow-applic ation` CloudFormation sortie :
	`export API_GATEW AY_ENDPOINT=$(aws cloudformation describe-stacks -- stack-name "lza-acco unt-creation-workf low-application"`	

Tâche	Description	Compétences requises
	`--query 'Stacks[*].Outputs[?OutputKey==`oApiGatewayCreateAccountEndpoint`].OutputValue' --output text)`	
Vérifiez la disponibilité des noms.	Entrez la commande suivante pour vérifier que le nom est disponible pour Compte AWS. Remplacez `<AWS_ACCOUNT_NAME>` par le nom du compte cible : `awscurl --service execute-api \ --region ${AWS_REGION} \ --access_key ${AWS_ACCESS_KEY_ID} \ --secret_key ${AWS_SECRET_ACCESS_KEY} \ --security_token ${AWS_SESSION_TOKEN} \ -X POST ${API_GATEWAY_ENDPOINT}check_name?account_name=<AWS_ACCOUNT_NAME>`	AWS DevOps

Tâche	Description	Compétences requises
Exécutez le flux de travail de création de compte.	1. Dans le dossier racine du dépôt cloné, ouvrez le `api_example.json` fichier. 2. Mettez à jour les paramètre s avec vos valeurs de configuration : `{ "account_name": "lza-test-01", "account_email": "johnsmith+lzatest01@example.com", "support_dl": "johnsmith@example.com", "managed_org_unit": "Workloads/Workload-1", "ad_integration": [{ "PermissionSetName": "CustomerAccountAdmin", "ActiveDirectoryGroupName": "platform-admin" }, { "PermissionSetName": "CustomerAccountDev", "ActiveDirectoryGroupName": "workload1-app1" }`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>],
	    "force_update":
	 "true",
	    "bypass_c
	reation": "false",
	    "account_tags": [
	        {
	            "Key":
	 "Environment",
	            "Value":
	 "Dev"
	        }, {
	            "Key":
	 "DeploymentMethod",
	            "Value":
	 "ApiGateway"
	        }
	    ]
	}</pre>	

	3. Enregistrez et fermez le fichier `api_examp le.json` .	

	4. Entrez la commande suivante pour lancer le flux de travail Step Functions :
	<pre>awscurl --service
	 execute-api \
	    --data @api-exam
	ple.json \
	    --region ${AWS_REG
	ION} \
	    --access_key
	 ${AWS_ACCESS_KEY_I
	D} \
	    --secret_key
	 ${AWS_SECRET_ACCES
	S_KEY} \</pre>	

Tâche	Description	Compétences requises
	--security_token ${AWS_SESSION_TOKEN} \ -X POST ${API_GATEWAY_ENDPOINT}execute 5. Dans le résultat de la commande précédente, notez l'exécution de Step Functions Amazon Resource Name (ARN). 6. Si vous souhaitez vérifier l'état du flux de travail Step Functions, entrez la commande suivante. Remplacez <STEP_FUNCTION_EXECUTION_NAME> par l'ARN ou le nom d'exécution de Step Functions : awscurl --service execute-api \ --region ${AWS_REGION} \ --access_key ${AWS_ACCESS_KEY_ID} \ --secret_key ${AWS_SECRET_ACCESS_KEY} \ --security_token ${AWS_SESSION_TOKEN} \ -X GET ${API_GATEWAY_ENDPOINT}get_execution_status?execution=<STEP_FUN	

Tâche	Description	Compétences requises
	`CTION_EXECUTION_NA ME>` 7. Attendez de recevoir une notification indiquant que le compte a été créé avec succès. **Note** Si le processus de création de compte échoue, Amazon SNS envoie une notification aux adresses e-mail que vous avez définies `accountCr eationFailure` dans le `deploy-config.yaml` fichier. Le demandeur du compte n'est pas averti.	

(Facultatif) Nettoyez la solution

Tâche	Description	Compétences requises
Supprimez des objets des compartiments Amazon S3.	Supprimez tous les objets des compartiments Amazon S3 suivants :	AWS DevOps

Tâche	Description	Compétences requises
	• `lza-account-creation-work-<CDK_UNIQUE_ID>` • `lza-account-creation-workflow-src-<AWS_REGION>-<AWS_ACCOUNT>` • `lza-account-creation-workflow-<AWS_REGION>-<AWS_ACCOUNT>`	

Supprimez la CloudFormation pile.	Entrez la commande suivante pour supprimer la CloudFormation pile :
	`aws cloudformation delete-stack \ --stack-name lza-account-creation-workflow-application`
	`aws cloudformation wait stack-delete-complete \ --stack-name lza-account-creation-workflow-application`
		AWS DevOps

Supprimez le pipeline.	Entrez la commande suivante pour supprimer le `lza-account-creation-workflow-pipeline` pipeline : `cdk destroy lza-account-creation-workflow-pipeline --force`	AWS DevOps

Ressources connexes

- Accélérateur de zone d'atterrissage activé AWS (bibliothèque de AWS solutions)
- Résolution des AWS CDK problèmes courants (AWS CDK documentation)

Informations supplémentaires

Schéma de flux de travail Step Functions

L'image suivante montre les états du flux de travail Step Functions.

Arguments

Voici les arguments que vous pouvez utiliser lorsque vous exécutez le script Python qui lance le flux de travail Step Functions.

Les arguments suivants sont obligatoires :

- `account-name (-a)`(string) — Le nom du nouveau Compte AWS.
- `support-dl (-s)`(chaîne) — Adresse e-mail qui reçoit la notification lorsque le processus de création du compte est terminé.
- `managed-org-unit (-m)`(string) — Unité organisationnelle (UO) gérée qui contiendra le nouveau compte.

Les arguments suivants sont facultatifs :

- `ad-integration (-ad)`(dictionnaire de chaînes) — Le groupe d'identifiants Microsoft Entra et l'ensemble d'autorisations attribuées. Voici un exemple d'utilisation de cet argument :

```
--ad-integration "{\"<PermissionSetName>\": \"<EntraIdGroupName>\"}"
```

- `account-email (-e)`(string) — Adresse e-mail de l'utilisateur root du nouveau Compte AWS.

> **Note**
>
> Si cet argument n'est pas utilisé, une adresse e-mail sera générée en utilisant les valeurs `rootEmailPrefix` et `rootEmailDomain` à partir du `configs/deploy-config.yaml`

fichier. Si aucune adresse e-mail n'est fournie, une adresse e-mail est générée en utilisant le format suivant :`rootEmailPrefix+accountName@rootEmailDomain`.

- `region (-r)`(string) — L' Région AWS endroit où le flux de travail Step Functions a été déployé. La valeur par défaut est `us-east-1`.
- `force-update (-f)`(chaîne booléenne) — Entrez `true` pour forcer la mise AWS Service Catalog à jour du produit approvisionné.
- `bypass-creation (-b)`(chaîne booléenne) — Entrez `true` pour éviter d'ajouter le compte au `accounts-config.yaml` fichier et d'exécuter le `AWSAccelerator-Pipeline` pipeline. Cet argument est généralement utilisé pour tester le processus de création de compte ou pour exécuter le reste des étapes de Step Functions en cas d'erreur dans le `Landing Zone Accelerator` pipeline.
- `tags (-t)`(string) — Balises supplémentaires que vous souhaitez ajouter au Compte AWS. Par défaut, les balises suivantes sont ajoutées : `account-namesupport-dl`, et`purpose`. Voici un exemple d'utilisation de cet argument :

```
--tags TEST1=VALUE1 TEST2=VALUE2
```

Inventaire automatique AWS des ressources sur plusieurs comptes et régions

Créée par Matej Macek (AWS)

Récapitulatif

Ce modèle décrit une approche automatisée pour maintenir un inventaire complet des AWS ressources sur plusieurs comptes et Régions AWS. Il est conçu pour aider les ingénieurs en infrastructure et en sécurité à améliorer leurs pratiques de gestion des ressources. Il est utilisé AWS Config pour suivre l'évolution des ressources, Amazon Athena pour les requêtes et Amazon QuickSight pour les tableaux de bord interactifs. Vous implémentez cette solution en déployant une AWS CloudFormation pile.

Cette solution est similaire à celle présentée dans Visualization AWS Config data using Amazon Athena and QuickSight AmazonAWS (article de blog). Ce modèle développe cette solution pour répondre aux exigences courantes suivantes et offrir les principaux avantages suivants :

- Axée sur la conformité — Cette approche peut vous aider à répondre aux exigences réglementaires telles que les normes PCI DSS, NIST SP 800-53, ISO/IEC 27001, HIPAA, GDPRet d'autres qui imposent des inventaires d'actifs précis.
- Cadre de personnalisation : il fournit une base pour créer QuickSight des tableaux de bord pour différentes AWS ressources, afin que vous puissiez personnaliser la solution en fonction de vos besoins spécifiques.
- Améliorations axées sur l'utilisateur : cette approche intègre les commentaires issus de cas d'utilisation réels et répond aux demandes de solution plus complète.

Les équipes chargées de l'infrastructure, de la sécurité et des finances sont souvent confrontées à des problèmes de visibilité et de collaboration dans des environnements dynamiques, multicomptes ou multirégionaux. Cette solution est conçue pour relever ces défis et réduire considérablement le temps et les efforts nécessaires à la création et à la maintenance d'un inventaire des ressources. Le résultat est une vue centralisée des ressources qui vous aide à améliorer les décisions d'allocation des ressources, à identifier et à atténuer les risques, à optimiser les coûts et à améliorer la visibilité globale et la collaboration. Cette approche comble le fossé entre les solutions conceptuelles et les besoins de mise en œuvre réels à des fins de sécurité, de conformité et d'exploitation.

Conditions préalables et limitations

Prérequis

- Les actifs suivants Comptes AWS :
  - Compte de gestion : compte centralisé pour la facturation, la création de comptes et le contrôle des accès au sein de l'organisation
  - Compte d'audit : plateforme centralisée pour la surveillance de la sécurité, les contrôles de conformité et les notifications de dérive
  - Compte d'archivage des journaux — Un compte centralisé pour le stockage et l'analyse des données collectées
- Dans le compte d'audit, un AWS Config agrégateur qui collecte et agrège les données de configuration de vos comptes cibles et de vos régions
- Dans le compte d'archivage du journal, configurez les éléments suivants :
  - Un bucket Amazon Simple Storage Service (Amazon S3) dans lequel vous stockez les données de l'agrégateur AWS Config
  - Un QuickSight abonnement Amazon
  - Une connexion autorisée entre QuickSight et Amazon Athena
  - Autorisations d'accès au compartiment Amazon S3 via une requête Athena
- AWS Command Line Interface (AWS CLI), installé et configuré
- Autorisations permettant de déployer une CloudFormation pile fournissant les ressources suivantes :
  - Une AWS Lambda fonction
  - Une configuration de notification Amazon S3
  - Base de données, tables et vues Athena
  - QuickSight ensembles de données et sources de données
- Autorisations pour exécuter des automatisations dans AWS Systems Manager
- Autorisations d'accès QuickSight

Limites

- La solution repose sur AWS Config. AWS Config enregistre généralement les modifications de configuration de vos ressources juste après la détection d'une modification, ou à la fréquence que

vous spécifiez. Cependant, cela se fait dans la mesure du possible et peut parfois prendre plus de temps.

- Cette solution suit uniquement les types de ressources AWS Config compatibles.
- La solution ne suit pas l'inventaire des ressources chez les autres fournisseurs de cloud ou dans les environnements sur site.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité des régions, consultez la page Points de terminaison et quotas du service dans la AWS documentation et choisissez le lien du service.

Architecture

Le schéma suivant montre un processus rationalisé de collecte, d'organisation, d'analyse et de visualisation des données de configuration et de conformité sur plusieurs comptes d'une AWS organisation.

Le schéma suivant illustre le flux de travail suivant :

1. De façon périodique, l' AWS Config agrégateur collecte des données de configuration et de conformité concernant les ressources des comptes cibles et des régions, puis transmet les données au compartiment Amazon S3 dans le compte d'archivage des journaux.
2. L'ajout de nouvelles AWS Config données au compartiment Amazon S3 appelle une AWS Lambda fonction.
3. La fonction Lambda partitionne les données en configurant des clés avec des valeurs correspondant à la région et à la date de chaque fichier de capture instantanée. Cela permet d'interroger et de traiter AWS Glue efficacement les données de configuration et de conformité.
4. Amazon Athena utilise un AWS Glue schéma pour exécuter des requêtes SQL sur les données stockées dans le compartiment Amazon S3. Il utilise les métadonnées du schéma AWS Glue pour comprendre la structure des données.
5. Les vues d'Athena définissent et extraient les ensembles de données cibles.
6. Les tableaux de bord d'Amazon vous QuickSight aident à visualiser et à analyser les ensembles de données.

Outils

Services AWS

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps. Un AWS Config agrégateur collecte des données AWS Config de configuration et de conformité provenant de plusieurs Comptes AWS régions.
- AWS Glueest un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données. Ce modèle utilise un catalogue de AWS Glue données et un registre de schémas.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle. AWS Systems Manager L'automatisation simplifie les tâches courantes de maintenance, de déploiement et de correction pour de nombreuses personnes Services AWS.

Référentiel de code

Le AWS CloudFormation modèle de ce modèle est disponible dans le GitHub référentiel AWS Config de visualisation. Ce CloudFormation modèle déploie un runbook AWS Systems Manager d'automatisation configuré AWS Config pour être utilisé avec Amazon Athena. Cette automatisation prépare la connexion AWS Glue au compartiment Amazon S3 désigné, crée des vues dans Amazon Athena et configure QuickSight Amazon pour la visualisation du tableau de bord.

Bonnes pratiques

- Nous vous recommandons de suivre les meilleures pratiques de la section Configuration et gestion d'un AWS environnement multi-comptes sécurisé, conformément aux directives AWS Control Tower AWS prescriptives.
- Nous vous recommandons de créer un AWS Config agrégateur qui collecte les données de configuration et de conformité pour l'ensemble de l' AWS organisation. Pour plus d'informations, consultez la section Agrégation de données multicomptes et multirégions dans la AWS Config documentation.
- Avant de déployer cette solution, nous vous recommandons de consulter les informations tarifaires actuelles pour Amazon S3 AWS Config, Athena et. QuickSight

Épopées

Déployez la CloudFormation pile

Tâche	Description	Compétences requises
Téléchargez le CloudFormation modèle.	Téléchargez le modèle Config-QuickSight CloudFormation - Visualization-SSM-Automation.yaml.	Administrateur AWS, administrateur cloud, DevOps ingénieur
Modifiez le CloudFormation modèle.	Effectuez cette étape uniquement si vous utilisez AWS Control Toweret AWS Config êtes géré par AWS Control Tower. Vous devez modifier le CloudFormation modèle.	DevOps ingénieur, administrateur AWS

Tâche	Description	Compétences requises

	1. Connectez-vous au compte de gestion .
	2. Ouvrez la AWS Organizations console.
	3. Accédez à la page Paramètres. Cette page affiche des informations sur l'organisation, notamment son identifiant.
	4. Copiez l'identifiant de l'organisation.
	5. Dans votre éditeur de texte préféré, ouvrez le fichier Config- QuickSight -Visualization-SSM-Automation.yaml.
	6. Trouvez la ligne suivante :
	`return re.match( '^AWSLogs/(\d+)/Config/([\w-]+)/(\d+)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)`
	7. Remplacez cette ligne par la ligne suivante, où se <ORGANIZATION_ID> trouve l'identifiant que vous avez précédemment copié :
	`return re.match( '^<ORGANIZATION_ID>/AWSLogs/(\d+)/Config/([\w-]+)/(\d+`	

Tâche	Description	Compétences requises
	`)/(\d+)/(\d+)/ConfigSnapshot/[^\\\]+$', object_key)` 8. Enregistrez et fermez le fichier Config- QuickSight - Visualization-SSM-Automation.yaml.	
Créez une CloudFormation pile.	Suivez les instructions de la section Créer une pile depuis la CloudFormation console. Remarques : 1. Choisissez Télécharger un fichier modèle, puis sélectionnez le fichier YAML que vous avez téléchargé. 2. Dans le champ Nom de la pile, saisissez `Config-QuickSight-Visualization-SSM-Automation` . 3. Sélectionnez Envoyer.	Administrateur AWS, administrateur cloud, DevOps ingénieur

Exécutez l'automatisation dans Systems Manager

Tâche	Description	Compétences requises
Trouvez votre nom QuickSight d'utilisateur.	1. Ouvrez la QuickSight console. 2. Ouvrez le menu du profil.	Administrateur AWS, administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	3. Notez le nom d'utilisateur. Vous aurez besoin de cette valeur plus tard.	
Trouvez le nom du canal de diffusion et le nom du compartiment Amazon S3.	1. Dans le AWS CLI, entrez la commande suivante : `aws configservice describe-delivery-channels` 2. Notez le nom du compartiment Amazon S3 et le nom de votre canal de AWS Config diffusion. Vous aurez besoin de ces valeurs ultérieurement.	Administrateur AWS, administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
Exécutez l'automatisation dans Systems Manager.	1. Ouvrez la AWS Systems Manager console. 2. Dans le panneau de navigation, cliquez sur Documents. 3. Choisissez Possédé par moi. 4. Choisissez Config-QuickSight -Visualization. 5. Choisissez Execute automation (Exécuter l'automatisation). 6. Dans la section Paramètres d'entrée, entrez les valeurs des paramètres suivants : • `ConfigDeliveryChannelName` — Entrez le nom de votre canal AWS Config de diffusion. Ce paramètre est obligatoire. • `ConfigS3BucketLocation` — Entrez le nom du compartiment Amazon S3 dans lequel vous stockez les données AWS Config de configuration. Ce paramètre est obligatoire. • `QuickSightUserName` — Entrez un nom d'utilisateur disposant d'un accès administratif à	Administrateur AWS, administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	QuickSight. Ce paramètre est obligatoire. • `AutomationAssumeRole` — L'Amazon Resource Name (ARN) du rôle AWS Identity and Access Management (IAM) qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Ce paramètre est facultatif. Laissez ce paramètre vide. • `DeleteConfigVisualization` — Choisissez `false`. 7. Sélectionnez Execute (Exécuter).	

Visualisez les données sur Amazon QuickSight

Tâche	Description	Compétences requises
Actualisez les données.	Pour planifier des actualisations de jeux de données en fonction de vos besoins spécifiques, suivez les instructions de la section Actualisation des données SPICE.	Administrateur AWS, DevOps ingénieur, administrateur cloud
Créez une analyse .	Pour créer un tableau de bord QuickSight qui vous aide à visualiser les ressources,	QuickSight administrateur

Tâche	Description	Compétences requises
	suivez les instructions de la section Lancer une analyse sur Amazon QuickSight.	
Créez un tableau de bord.	1. Une fois que vous avez terminé de modifier votre QuickSight analyse, suivez les instructions de la section Publication de tableaux de bord pour créer un tableau de bord. Un tableau de bord est une analyse que vous pouvez partager avec d'autres QuickSight utilisateurs. 2. Suivez les instructions de la section Autoriser l'accès à un tableau de bord pour partager le tableau de bord avec vos QuickSight utilisateurs cibles.	QuickSight administrateur

(Facultatif) Nettoyer

Tâche	Description	Compétences requises
Supprimez les ressources créées par l'automatisation de Systems Manager.	1. Ouvrez la AWS Systems Manager console. 2. Dans le panneau de navigation, cliquez sur Documents. 3. Choisissez Possédé par moi.	Administrateur AWS, administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	4. Choisissez Config-QuickSight -Visualization. 5. Choisissez Execute automation (Exécuter l'automatisation). 6. Dans la section Paramètres d'entrée, entrez le `DeleteConfigVisualization` paramètre `true`. 7. Sélectionnez Execute (Exécuter).	
Supprimez la CloudFormation pile.	Pour supprimer les ressources de la `Config-QuickSight-Visualization-SSM-Automation` pile, suivez les instructions de la section Supprimer une pile de la CloudFormation console.	Administrateur AWS, administrateur cloud, DevOps ingénieur

Résolution des problèmes

Problème	Solution
Amazon essaie de QuickSight se connecter à la `us-east-1` Région AWS, mais la création de ressources dans cette région n'est pas autorisée.	Une politique de contrôle des services restreint votre abonnement à Amazon QuickSight dans cette région. Dans la politique de contrôle des services, spécifiez manuellement la cible Région AWS. Remplacez `<REGION_ID>` par l'identifiant de région approprié : `https://<REGION_ID>.quicksight.aws.amazon.com/sn/start/dashboards`

Problème	Solution
	Voici un exemple : `https://eu-central-1.quicksight.aws.amazon.com/sn/start/dashboards`
Dans Amazon Athena, le message suivant s'affiche : `Before you run your first query, you need to set up a query result location in Amazon S3.`	Assurez-vous d'avoir préparé un compartiment Amazon S3 dans lequel vous stockerez les résultats des requêtes provenant d'Amazon Athena. Suivez ensuite les instructions de la section Spécifier l'emplacement des résultats de requête à l'aide de la console Amazon Athena.

Ressources connexes

AWS documentation

- AWS Config documentation
- QuickSight Documentation Amazon

AWS article de blog

- Automatisez la visualisation des AWS Config données avec AWS Systems Manager
- Comment enregistrer régulièrement les modifications de configuration des ressources avec AWS Config

Autres ressources

- Centre de formation QuickSight communautaire Amazon
- Galerie de QuickSight la communauté Amazon

Configurer les journaux de flux VPC pour les centraliser sur les comptes AWS

Créée par Benjamin Morris (AWS) et Aman Kaur Gandhi (AWS)

Récapitulatif

Dans un cloud privé virtuel (VPC) Amazon Web Services (AWS), la fonctionnalité VPC Flow Logs peut fournir des données utiles pour le dépannage opérationnel et de sécurité. Cependant, l'utilisation des journaux de flux VPC dans un environnement multi-comptes est limitée. Plus précisément, les journaux de flux entre comptes d'Amazon CloudWatch Logs ne sont pas pris en charge. Vous pouvez plutôt centraliser les journaux en configurant un compartiment Amazon Simple Storage Service (Amazon S3) avec la politique de compartiment appropriée.

> **Note**
>
> Ce modèle décrit les exigences relatives à l'envoi de journaux de flux vers un emplacement centralisé. Toutefois, si vous souhaitez également que les journaux soient disponibles localement dans les comptes membres, vous pouvez créer plusieurs journaux de flux pour chaque VPC. Les utilisateurs n'ayant pas accès au compte Log Archive peuvent consulter les journaux de trafic pour résoudre les problèmes. Vous pouvez également configurer un journal de flux unique pour chaque VPC qui envoie des journaux à CloudWatch Logs. Vous pouvez ensuite utiliser un filtre d'abonnement Amazon Data Firehose pour transférer les journaux vers un compartiment S3. Pour plus d'informations, consultez la section Ressources connexes.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une organisation AWS Organizations disposant d'un compte utilisé pour centraliser les journaux (par exemple, Log Archive)

Limites

Si vous utilisez la clé gérée par AWS Key Management Service (AWS KMS) `aws/s3` pour chiffrer votre compartiment central, celui-ci ne recevra pas les journaux d'un autre compte. Au lieu de cela, vous verrez un code `Unsuccessful` d'erreur 400 avec un message tel que `"LogDestination: <bucketName> is undeliverable"` pour votre compte`ResourceId`.

Cela est dû au fait que les clés gérées par AWS d'un compte ne peuvent pas être partagées entre les comptes.

La solution consiste à utiliser le chiffrement géré par Amazon S3 (SSE-S3) ou une clé gérée par le client AWS KMS que vous pouvez partager avec les comptes des membres.

Architecture

Pile technologique cible

Dans le schéma suivant, deux journaux de flux sont déployés pour chaque VPC. L'un d'eux envoie des journaux à un groupe de CloudWatch journaux local. L'autre envoie les journaux vers un compartiment S3 dans un compte de journalisation centralisé. La politique de compartiment autorise le service de livraison de journaux à écrire des journaux dans le compartiment.

> **Note**
>
> Depuis novembre 2023, prend AWS désormais en charge la clé de condition aws : SourceOrg ID. Cette condition vous permet de refuser d'écrire dans le compartiment centralisé pour les comptes extérieurs à votre AWS Organizations organisation.

Architecture cible

Automatisation et mise à l'échelle

Chaque VPC est configuré pour envoyer des journaux au compartiment S3 du compte de journalisation central. Utilisez l'une des solutions d'automatisation suivantes pour vous assurer que les journaux de flux sont correctement configurés :

- AWS CloudFormation StackSets
- AWS Control Tower Account Factory pour Terraform (AFT)
- Une règle AWS Config avec correction

Outils

Outils

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS. Ce modèle utilise la fonctionnalité VPC Flow Logs pour capturer des informations sur le trafic IP à destination et en provenance des interfaces réseau de votre VPC.

Bonnes pratiques

L'utilisation de l'infrastructure en tant que code (IaC) peut considérablement simplifier le processus de déploiement des journaux de flux VPC. Si vous extrayez les définitions de déploiement de votre VPC pour inclure une structure de ressources de journal de flux, VPCs vous serez automatiquement déployé avec les journaux de flux. Cela est démontré dans la section suivante.

Journaux de flux centralisés

Exemple de syntaxe pour ajouter des journaux de flux centralisés à un module VPC dans Terraform HashiCorp

Ce code crée un journal de flux qui envoie les journaux d'un VPC vers un compartiment S3 centralisé. Notez que ce modèle ne couvre pas la création du compartiment S3.

Pour les déclarations de politique relatives aux compartiments recommandées, consultez la section Informations supplémentaires.

```
variable "vpc_id" { type = string }
locals { custom_log_format_v5 = "$${version} $${account-id} $${interface-id} $
${srcaddr} $${dstaddr} $${srcport} $${dstport} $${protocol} $${packets} $${bytes}
 $${start} $${end} $${action} $${log-status} $${vpc-id} $${subnet-id} $${instance-
id} $${tcp-flags} $${type} $${pkt-srcaddr} $${pkt-dstaddr} $${region} $${az-id} $
${sublocation-type} $${sublocation-id} $${pkt-src-aws-service} $${pkt-dst-aws-service}
 $${flow-direction} $${traffic-path}" }
resource "aws_flow_log" "centralized_flow_log" {
```

```
  log_destination      = "arn:aws:s3:::centralized-vpc-flow-logs-
<log_archive_account_id>" # Optionally, a prefix can be added after the ARN.
  log_destination_type = "s3"
  traffic_type         = "ALL"
  vpc_id               = var.vpc_id
  log_format           = local.custom_log_format_v5 # If you want fields from VPC Flow
 Logs v3+, you will need to create a custom log format.
}
```

Pour plus d'informations sur le format de journal personnalisé, consultez la documentation AWS.

Journaux de flux locaux

Exemple de syntaxe pour ajouter des journaux de flux locaux à un module VPC dans Terraform avec les autorisations requises

Ce code crée un journal de flux qui envoie des journaux d'un VPC à un groupe de CloudWatch journaux local.

```
data "aws_region" "current" {}
variable "vpc_id" { type = string }
resource "aws_iam_role" "local_flow_log_role" {
  name = "flow-logs-policy-${var.vpc_id}"
  assume_role_policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Principal": {"Service": "vpc-flow-logs.amazonaws.com"},
      "Action": "sts:AssumeRole"
  }]
}
EOF
}
resource "aws_iam_role_policy" "logs_permissions" {
  name = "flow-logs-policy-${var.vpc_id}"
  role = aws_iam_role.local_flow_log_role.id
  policy = <<EOF
{
  "Version": "2012-10-17",
  "Statement": [{
      "Action": ["logs:CreateLog*", "logs:PutLogEvents", "logs:DescribeLog*",
 "logs:DeleteLogDelivery"],
```

```
      "Effect": "Allow",
      "Resource": "arn:aws:logs:${data.aws_region.current.name}:*:log-group:vpc-flow-
logs*"
  }]
}
EOF
}
resource "aws_cloudwatch_log_group" "local_flow_logs" {
  name              = "vpc-flow-logs/${var.vpc_id}"
  retention_in_days = 30
}
resource "aws_flow_log" "local_flow_log" {
  iam_role_arn    = aws_iam_role.local_flow_log_role.arn
  log_destination = aws_cloudwatch_log_group.local_flow_logs.arn
  traffic_type    = "ALL"
  vpc_id          = var.vpc_id
}
```

Épopées

Déployer une infrastructure de journaux de flux VPC

Tâche	Description	Compétences requises
Déterminez la stratégie de chiffrement et créez la politique pour le compartiment S3 central.	Le compartiment central ne prend pas en charge la clé `aws/s3` AWS KMS. Vous devez donc utiliser SSE-S3 ou une clé gérée par le client AWS KMS. Si vous utilisez une clé AWS KMS, la politique en matière de clés doit autoriser les comptes membres à utiliser la clé.	Conformité d'
Créez le compartiment à journaux de flux central.	Créez le compartiment central vers lequel les journaux de flux seront envoyés et appliquez la stratégie de chiffrement que vous avez	AWS général

Tâche	Description	Compétences requises
	choisie à l'étape précédente. Cela doit se trouver dans une archive de journaux ou dans un compte à usage similaire. Obtenez la politique de compartiment dans la section Informations supplémentaires et appliquez-la à votre compartiment central après avoir mis à jour les espaces réservés avec les valeurs spécifiques à votre environnement.	
Configurez les journaux de flux VPC pour envoyer les journaux au bucket de journaux de flux central.	Ajoutez des journaux de flux à chaque VPC à partir duquel vous souhaitez collecter des données. La méthode la plus évolutive consiste à utiliser des outils IaC tels que AFT ou AWS Cloud Development Kit (AWS CDK). Par exemple, vous pouvez créer un module Terraform qui déploie un VPC parallèlement à un journal de flux. Si nécessaire, vous ajoutez les journaux de flux manuellement.	Administrateur réseau

Tâche	Description	Compétences requises
Configurez les journaux de flux VPC à envoyer aux journaux locaux CloudWatch .	(Facultatif) Si vous souhaitez que les journaux de flux soient visibles dans les comptes sur lesquels ils sont générés, créez un autre journal de flux pour envoyer des données aux CloudWatch journaux du compte local. Vous pouvez également envoyer les données vers un compartim ent S3 spécifique au compte dans le compte local.	AWS général

Ressources connexes

- Comment faciliter l'analyse des données et répondre aux exigences de sécurité en utilisant des données de journal de flux centralisées (article de blog)
- Comment activer automatiquement les journaux de flux VPC à l'aide des règles AWS Config (article de blog)

Informations supplémentaires

Politique relative aux compartiments

Cet exemple de politique de compartiment peut être appliqué à votre compartiment S3 central pour les journaux de flux, après avoir ajouté des valeurs pour les noms d'espaces réservés.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceOrgID": "<ORG_ID>"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>",
            "Condition": {
                "StringEquals": {
                    "aws:SourceOrgID": "<ORG_ID>"
                }
            }
        },
        {
            "Sid": "DenyUnencryptedTraffic",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BUCKET_NAME>/*",
                "arn:aws:s3:::<BUCKET_NAME>"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        }
    ]
}
```

Marquez automatiquement les pièces jointes à Transit Gateway à l'aide d'AWS Organizations

Créée par Richard Milner-Watts (AWS), Haris Bin Ayub (AWS) et John Capps (AWS)

Récapitulatif

Sur Amazon Web Services (AWS), vous pouvez utiliser AWS Resource Access Managerpour partager Compte AWS au-delà des AWS Transit Gatewayfrontières. Cependant, lorsque vous créez des pièces jointes Transit Gateway au-delà des limites du compte, elles sont créées sans étiquette Name. Cela peut rendre l'identification des pièces jointes fastidieuse.

Cette solution fournit un mécanisme automatisé pour recueillir des informations sur chaque pièce jointe à Transit Gateway pour les comptes d'une organisation gérée par AWS Organizations. Le processus consiste à rechercher la plage de routage interdomaines sans classe (CIDR) à partir de la table de routage Transit Gateway. La solution applique ensuite une étiquette de nom sous la forme de `<CIDR-range>-<AccountName>` à la pièce jointe du compte qui contient la passerelle de transit.

Cette solution peut être utilisée conjointement avec une solution telle que le Serverless Transit Network Orchestrator de la bibliothèque de AWS solutions. Serverless Transit Network Orchestrator permet la création automatique de pièces jointes Transit Gateway Gateway à grande échelle.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une AWS Organizations organisation qui contient tous les comptes associés
- Accès au compte de gestion de l'organisation, sous la racine de l'organisation, pour créer le rôle AWS Identity and Access Management (IAM) requis
- Un compte de membre du réseau partagé contenant une ou plusieurs passerelles de transport partagées avec l'organisation et comportant des pièces jointes

Architecture

La capture d'écran suivante AWS Management Console montre des exemples de pièces jointes Transit Gateway sans étiquette de nom associée et de deux pièces jointes Transit Gateway avec

des balises de nom générées par cette solution. La structure de la balise Name générée est`<CIDR-range>-<AccountName>`.

Cette solution permet AWS CloudFormationde déployer un AWS Step Functionsflux de travail qui gère la création de balises Transit Gateway Name sur toutes les configurations Régions AWS. Le flux de travail invoque AWS Lambdades fonctions qui exécutent les tâches sous-jacentes.

Une fois que la solution a obtenu les noms des comptes AWS Organizations, la machine d'état Step Functions obtient toutes les pièces jointes Transit Gateway IDs. Elles sont traitées en parallèle par Region. Ce traitement inclut la recherche de la plage CIDR pour chaque pièce jointe. La plage CIDR est obtenue en recherchant dans les tables de routage de Transit Gateway de la région un ID de pièce jointe Transit Gateway correspondant. Si toutes les informations requises sont disponibles, la solution applique un tag Name à la pièce jointe. La solution ne remplacera aucune balise Name existante.

La solution s'exécute selon un calendrier contrôlé par un EventBridge événement Amazon. L'événement initie la solution chaque jour à 6 h 00 UTC.

Pile technologique cible

- Amazon EventBridge
- AWS Lambda
- AWS Organizations
- AWS Transit Gateway
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS X-Ray

Architecture cible

L'architecture de la solution et le flux de travail sont illustrés dans le schéma suivant.

1. L'événement planifié initie la règle.
2. La EventBridge règle démarre la machine d'état Step Functions.
3. La machine à états invoque la fonction `tgw-tagger-organizations-account-query` Lambda.

4. La fonction `tgw-tagger-organizations-account-query` Lambda assume le rôle dans le compte de gestion de l'organisation.
5. La fonction `tgw-tagger-organizations-account-query` Lambda appelle l'API Organizations pour renvoyer Compte AWS des métadonnées.
6. La machine à états invoque la fonction `tgw-tagger-attachment-query` Lambda.
7. Pour chaque région, en parallèle, la machine à états invoque la fonction `tgw-tagger-rtb-query` Lambda pour lire la plage CIDR de chaque pièce jointe.
8. Pour chaque région, en parallèle, la machine à états invoque la fonction `tgw-tagger-attachment-tagger` Lambda.
9. Des étiquettes nominatives sont créées pour les pièces jointes Transit Gateway dans le compte Shared Networking.

Automatisation et mise à l'échelle

La solution traite chaque région en parallèle afin de réduire la durée totale de l'exécution.

Outils

Services AWS

- AWS CloudFormationpermet de modéliser un ensemble de ressources connexes AWS et tierces, de les approvisionner rapidement et de manière cohérente, et de les gérer tout au long de leur cycle de vie, en traitant l'infrastructure comme du code.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez AWS en temps réel.
- Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. EventBridge reçoit un événement, un indicateur d'un changement d'environnement, et applique une règle pour acheminer l'événement vers une cible. Les règles associent les événements aux cibles en fonction de la structure de l'événement, appelée schéma d'événements, ou d'un calendrier.
- AWS Lambdaest un service de calcul qui prend en charge l'exécution de code sans provisionnement ni gestion de serveurs. Lambda exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, passant de quelques requêtes par jour à des milliers par seconde. Vous payez uniquement pour le temps de calcul consommé. Aucun frais n'est facturé si votre code n'est pas en cours d'exécution.

- AWS Organizationsvous permet de gérer et de gouverner votre environnement de manière centralisée à mesure que vous développez et faites évoluer vos AWS ressources. Organizations vous permet de créer de nouvelles ressources Comptes AWS et de les allouer par programmation, de regrouper des comptes pour organiser vos flux de travail, d'appliquer des politiques aux comptes ou aux groupes à des fins de gouvernance et de simplifier la facturation en utilisant un mode de paiement unique pour tous vos comptes.
- AWS Step Functionsest un service de flux de travail visuel à faible code utilisé pour orchestrer Services AWS, automatiser les processus métier et créer des applications sans serveur. Les flux de travail gèrent les échecs, les nouvelles tentatives, la parallélisation, les intégrations de services et l'observabilité afin que les développeurs puissent se concentrer sur une logique métier à plus forte valeur ajoutée.
- AWS Transit Gatewayconnecte VPCs et met en place des réseaux sur site via un hub central. Cela simplifie votre réseau et met fin aux relations de peering complexes. Il agit comme un routeur cloud, de sorte que chaque nouvelle connexion n'est établie qu'une seule fois.
- Amazon Virtual Private Cloud (Amazon VPC) est un service permettant de lancer AWS des ressources dans un réseau virtuel logiquement isolé que vous définissez.
- AWS X-Raycollecte des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour afficher, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation.

Code

Le code source de cette solution est disponible dans le GitHub référentiel Transit Gateway Attachment Tagger. Le référentiel inclut les fichiers suivants :

- `tgw-attachment-tagger-main-stack.yaml`crée toutes les ressources nécessaires à la prise en charge de cette solution dans le compte réseau partagé.
- `tgw-attachment-tagger-organizations-stack.yaml`crée un rôle dans le compte de gestion de l'organisation.

Épopées

Déployez la pile de solutions principale

Tâche	Description	Compétences requises
Rassemblez les informations préalables requises.	Pour configurer l'accès entre comptes depuis la fonction Lambda vers AWS Organizations l'API, vous avez besoin de l'ID de compte du compte de gestion de l'organisation. **Note** L'ordre dans lequel les deux AWS CloudFormation piles sont créées est important. Vous devez d'abord déployer des ressources dans le compte réseau partagé. Le rôle dans le compte de réseau partagé doit déjà exister avant de déployer des ressources dans le compte de gestion de l'organisation. Pour plus d'informations, consultez la documentation AWS.	DevOps ingénieur

Tâche	Description	Compétences requises
Lancez le AWS CloudFormation modèle pour la pile de solutions principale.	Le modèle de la pile de solutions principale déploiera les rôles IAM, le flux de travail Step Functions, les fonctions Lambda et l'événement Amazon CloudWatch . Ouvrez le compte AWS Management Console pour le réseau partagé, puis ouvrez la console : &CFN. Créez la pile en utilisant le `tgw-attachment-tagger-main-stack.yaml` modèle et les valeurs suivantes : • Nom de la pile — tgw-attachment-tagger-main-stack • awsOrganizationsRootAccountId— Numéro de compte pour le compte de gestion de l'organisation • TGWRegionsparamètre — Régions AWS pour la solution, saisi sous forme de chaîne séparée par des virgules • TGWListparamètre — Passerelle IDs de transit à exclure de la solution, saisie dans une chaîne séparée par des virgules	DevOps ingénieur

Tâche	Description	Compétences requises
	Pour plus d'informations sur le lancement d'une AWS CloudFormation pile, consultez la AWS documentation.	
Vérifiez que la solution a été lancée avec succès.	Attendez que la CloudFormation pile atteigne le statut CREATE_COMPLETE. Cela devrait prendre moins d'une minute. Ouvrez la console Step Functions et vérifiez qu'une nouvelle machine à états a été créée avec le nom tgw-attachment-tagger-state-machine.	DevOps ingénieur

Déployez le stack AWS Organizations

Tâche	Description	Compétences requises
Rassemblez les informations préalables requises.	Pour configurer l'accès entre comptes depuis la fonction Lambda vers l'API AWS Organizations, vous avez besoin de l'ID de compte du compte réseau partagé.	DevOps ingénieur
Lancez le CloudFormation modèle pour la pile Organizations	Le modèle de la pile AWS Organizations déploiera le rôle IAM dans le compte de gestion de l'organisation. Accédez à la console AWS pour le compte de gestion de	DevOps ingénieur

Tâche	Description	Compétences requises
	l'organisation, puis ouvrez la CloudFormation console. Créez la pile en utilisant le `tgw-attachment-tagger-organizations-stack.yaml` modèle et les valeurs suivantes : • Nom de la pile — tgw-attachment-tagger-organizations-stack • NetworkingAccountId paramètre — ID de compte pour le compte réseau partagé Pour les autres options de création de pile, utilisez les valeurs par défaut.	
Vérifiez que la solution a été lancée avec succès.	Attendez que la AWS CloudFormation pile atteigne le statut CREATE_COMPLETE. Cela devrait prendre moins d'une minute. Ouvrez la console AWS Identity and Access Management (IAM) et vérifiez qu'un nouveau rôle a été créé avec le nom tgw-attachment-tagger-organization-query-role.	DevOps ingénieur

Vérifiez la solution

Tâche	Description	Compétences requises
Lancez la machine d'état.	Ouvrez la console Step Functions pour le compte Shared Networking et choisissez State machines dans le volet de navigation. Sélectionnez l'état machine tgw-attachment-tagger-state-machine, puis choisissez Start Execution. Comme l'entrée de cette machine à états n'est pas utilisée par la solution, vous pouvez utiliser la valeur par défaut. `{ "Comment": "Insert your JSON here" }` Choisissez Démarrer une exécution.	DevOps ingénieur
Surveillez la machine à états jusqu'à ce qu'elle soit terminée.	Sur la nouvelle page qui s'ouvre, vous pouvez regarder la machine d'état fonctionner. La durée dépendra du nombre de pièces jointes Transit Gateway à traiter. Sur cette page, vous pouvez examiner chaque étape de	DevOps ingénieur

Tâche	Description	Compétences requises
	la machine à états. Vous pouvez consulter les différent es tâches de la machine à états et suivre les liens vers les CloudWatch journaux des fonctions Lambda. Pour les tâches exécutées en parallèle sur la carte, vous pouvez utiliser la liste déroulant e Index pour afficher les implémentations spécifiques à chaque région.	
Vérifiez les balises de pièce jointe de Transit Gateway.	Ouvrez la console VPC pour le compte réseau partagé et choisissez Transit Gateway Attachments. Sur la console, un tag Name est fourni pour les pièces jointes répondant aux critères (la pièce jointe est propagée vers une table de routage Transit Gateway et le propriétaire de la ressource est membre de l'organisation).	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez le déclenchement de l' CloudWatch événement.	Attendez que l' CloudWatch événement démarre. Cela est prévu pour 06h00 UTC. Ouvrez ensuite la console Step Functions pour le compte Shared Networking et choisissez State machines dans le volet de navigation. Sélectionnez l'état machine tgw-attachment-tagger-state -machine. Vérifiez que la solution a été exécutée à 6 h 00 UTC.	DevOps ingénieur

Ressources connexes

- AWS Organizations
- AWS Resource Access Manager
- Orchestrateur de réseau de transit sans serveur
- Création de rôles IAM
- Création d'une pile sur la AWS CloudFormation console

Plus de modèles

- Provisionner AWS Service Catalog des produits basés sur AWS CloudFormation des modèles à l'aide d' GitHub actions
- Fournissez des rôles IAM avec le moindre privilège en déployant une solution de distribution automatique de rôles

IA et apprentissage automatique

Rubriques

- Données agrégées dans Amazon DynamoDB pour les prévisions de machine learning dans Athena
- Associer un AWS CodeCommit référentiel dans un compte Compte AWS à Amazon SageMaker AI Studio Classic dans un autre compte
- Extrayez automatiquement le contenu de fichiers PDF à l'aide d'Amazon Textract
- Créez un modèle de prévision de démarrage à froid en utilisant DeePar pour les séries chronologiques dans Amazon SageMaker AI Studio Lab
- Créez un MLOps flux de travail à l'aide d'Amazon SageMaker AI et d'Azure DevOps
- Configurez la journalisation des appels de modèles dans Amazon Bedrock en utilisant AWS CloudFormation
- Créez une image de conteneur Docker personnalisée SageMaker et utilisez-la pour la formation des modèles dans AWS Step Functions
- Utilisez les agents Amazon Bedrock pour automatiser la création de contrôles d'accès dans Amazon EKS via des instructions textuelles
- Déployez un cas d'utilisation de RAG AWS en utilisant Terraform et Amazon Bedrock
- Déployez une logique de prétraitement dans un modèle de machine learning sur un seul point de terminaison à l'aide d'un pipeline d'inférence sur Amazon SageMaker
- Développez des assistants avancés basés sur l'IA générative basés sur le chat en utilisant RAG et des instructions ReAct
- Développez un assistant entièrement automatisé basé sur le chat en utilisant les agents et les bases de connaissances Amazon Bedrock
- Documentez les connaissances institutionnelles à partir de saisies vocales à l'aide d'Amazon Bedrock et Amazon Transcribe
- Générez des recommandations personnalisées et reclassées à l'aide d'Amazon Personalize
- Rationalisez les flux de travail d'apprentissage automatique, du développement local aux expériences évolutives en utilisant l' SageMaker IA et Hydra
- Formez et déployez un modèle de machine learning personnalisé supporté par GPU sur Amazon SageMaker
- Translate le langage naturel en requêtes DSL pour OpenSearch et requêtes Elasticsearch

- Utilisez Amazon Q Developer comme assistant de codage pour augmenter votre productivité
- Utiliser SageMaker le traitement pour l'ingénierie des fonctionnalités distribuées d'ensembles de données ML à l'échelle du téraoctet
- Visualisez les résultats du modèle AI/ML à l'aide de Flask et AWS Elastic Beanstalk
- Plus de modèles

Données agrégées dans Amazon DynamoDB pour les prévisions de machine learning dans Athena

Créée par Sachin Doshi (AWS) et Peter Molnar (AWS)

Récapitulatif

Ce modèle vous montre comment créer des agrégations complexes de données de l'Internet des objets (IoT) dans une table Amazon DynamoDB à l'aide d'Amazon Athena. Vous apprendrez également à enrichir les données grâce à l'inférence d'apprentissage automatique (ML) à l'aide d'Amazon SageMaker AI et à interroger des données géospatiales à l'aide d'Athena. Vous pouvez utiliser ce modèle comme base pour créer une solution de prévision ML répondant aux exigences de votre organisation.

À des fins de démonstration, ce modèle utilise un exemple de scénario d'une entreprise qui exploite un service de covoiturage et souhaite prédire le nombre optimal de scooters à déployer pour les clients de différents quartiers urbains. L'entreprise utilise un modèle de machine learning préformé qui prédit la demande des clients pour l'heure suivante en fonction des quatre dernières heures. Le scénario utilise un ensemble de données public du Bureau de l'innovation et de la technologie civiques du gouvernement du métro de Louisville. Les ressources pour ce scénario sont disponibles dans un GitHub référentiel.

Conditions préalables et limitations

- Un actif Compte AWS
- Autorisations permettant de créer une AWS CloudFormation pile avec des rôles AWS Identity and Access Management (IAM) pour les éléments suivants :
  - Compartiment Amazon Simple Storage Service (Amazon S3)
  - Athena
  - DynamoDB
  - SageMaker IA
  - AWS Lambda

Architecture

Pile technologique

- Amazon QuickSight
- Amazon S3
- Athena
- DynamoDB
- Lambda
- SageMaker IA

Architecture cible

Le schéma suivant montre une architecture permettant de créer des agrégations complexes de données dans DynamoDB à l'aide des fonctionnalités d'interrogation d'Athena, d'une fonction Lambda, du stockage Amazon S3, d'un point de terminaison AI et d'un tableau de bord. SageMaker QuickSight

Le schéma suivant illustre le flux de travail suivant :

1. Une table DynamoDB ingère les données IoT transmises par un parc de scooters.
2. Une fonction Lambda charge la table DynamoDB avec les données ingérées.
3. Une requête Athena crée une nouvelle table DynamoDB pour les données géospatiales qui représentent les quartiers urbains.
4. L'emplacement de la requête est enregistré dans un compartiment S3.
5. Une fonction Athena interroge l'inférence de machine learning à partir du point de terminaison SageMaker AI qui héberge le modèle de machine learning préentraîné.
6. Athena interroge les données directement depuis les tables DynamoDB et agrège les données à des fins d'analyse.
7. Un utilisateur affiche le résultat des données analysées dans un QuickSight tableau de bord.

Outils

Services AWS

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon SageMaker AI est un service de machine learning géré qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Utiliser les prédictions ML sur les données Amazon DynamoDB avec Amazon Athena ML. Vous pouvez utiliser le CloudFormation modèle du référentiel pour créer les ressources suivantes utilisées dans l'exemple de scénario :

- Table DynamoDB
- Une fonction Lambda pour charger le tableau avec les données pertinentes
- Un point de terminaison basé sur l' SageMaker IA pour les demandes d'inférence, avec le XGBoost modèle préentraîné stocké dans Amazon S3
- Un groupe de travail Athéna nommé `V2EngineWorkGroup`
- Named Athena interroge les fichiers de formes géospatiaux et prédit la demande de scooters
- Un connecteur Amazon Athena DynamoDB prédéfini qui permet à Athena de communiquer avec DynamoDB et AWS SAM utilise () pour créer l'application en référence au connecteur AWS Serverless Application Model DynamoDB

Épopées

Obtenez l'exemple de jeu de données

Tâche	Description	Compétences requises
Téléchargez le jeu de données et les ressources.	1. Téléchargez un ensemble de données public sur les locations de véhicules sans station d'accueil. À des fins de démonstration, ces données sont préremplies dans DynamoDB dans le cadre du cas d'utilisation, mais dans un environnement de production, vous envoyez ces données à DynamoDB par le biais de divers mécanismes tels que les appareils IoT ou les consommateurs Amazon Kinesis. Ces mécanismes utilisent Lambda pour insérer des données dans DynamoDB. 2. Téléchargez les fichiers de formes SIG qui représentent les limites des quartiers historiques et culturels de la ville de Louisville, dans le Kentucky. L'ensemble de données public est fourni par le Louisville and Jefferson County, KY Information Consortium. Les fichiers de formes d'origine sont déjà convertis	Développeur d'applications, data scientist

Tâche	Description	Compétences requises
	en un fichier texte que vous pouvez interroger avec Athena, mais vous pouvez trouver le code Python pour transformer les fichiers de formes dans le bloc-notes Jupyter à la rubrique Traitement géospatial des fichiers de formes SIG avec Amazon Athena in. GitHub 3. Téléchargez le code Python préentraîné qui entraîne le modèle ML pour les prévisions horaires à l'aide de l' SageMaker IA et d'Athena. 4. Obtenez la requête SQL dans Athena qui réunit tous les éléments nécessair es pour des prédictions en temps réel à partir des données stockées dans DynamoDB. 5. (Facultatif) QuickSight À utiliser pour visualiser les données géospatiales sur une carte de Louisville, dans le Kentucky.	

Utiliser un CloudFormation modèle pour déployer les ressources requises

Tâche	Description	Compétences requises
Créez une CloudFormation pile.	1. Téléchargez le CloudFormation modèle depuis le GitHub référentiel. 2. **Note** Connectez-vous au AWS Management Console, puis choisissez `us-east-1` . : Le modèle ML est stocké dans l'Amazon Elastic Container Registry (Amazon ECR) pour `us-east-1` Région AWS le, mais le modèle est indépendant de la région. Vous pouvez reproduire le modèle dans n'importe quelle région où les éléments Services AWS utilisés dans ce modèle sont pris en charge. 3. Ouvrez la CloudFormation console, puis choisissez Stacks dans le volet de navigation.	AWS DevOps

Tâche	Description	Compétences requises
	4. Choisissez Créer une pile, puis sélectionnez Avec les ressources existantes (ressources d'importation). 5. Sur la page Identifier les ressources, choisissez Next. 6. Dans la section Spécifier le modèle, pour Source du modèle, sélectionnez Télécharger un fichier modèle. 7. Choisissez Fichier, puis le CloudFormation modèle que vous avez téléchargé précédemment. 8. Choisissez Next, acceptez les valeurs des paramètres par défaut, puis choisissez Next pour passer au reste de l'assistant de configuration. 9. Cochez la case Je reconnais que des ressources IAM AWS CloudFormation pourraient être créées avec des noms personnalisés. 10. Sélectionnez Créer la pile.	

Tâche	Description	Compétences requises
	Note La création de ces ressources par la CloudFormation pile peut prendre de 15 à 20 minutes.	

Tâche	Description	Compétences requises
Vérifiez le CloudFormation déploiement.	Pour vérifier que les exemples de données du CloudFormation modèle sont chargés dans DynamoDB, procédez comme suit : 1. Ouvrez la console DynamoDB, puis choisissez Tables dans le volet de navigation. 2. Dans la section Tables, recherchez le `DynamoDBTableDocklessVehicles` tableau. 3. Une fois la création des ressources terminée, ouvrez la console Athena, puis choisissez Workgroups dans le volet de navigation. 4. Choisissez le `V2EngineWorkGroup` groupe de travail, puis choisissez Changer de groupe de travail. 5. Si vous êtes invité à enregistrer l'emplacement du résultat de la requête, choisissez un emplacement Amazon S3 où vous avez des autorisations d'écriture. 6. Choisissez Enregistrer. 7. Dans le volet de navigation, choisissez l'éditeur de requêtes, puis sélectionnez	Développeur d’applications

Tâche	Description	Compétences requises
	la `athena-ml-db-<your-AWS-account-number>` base de données.	

Charger des fichiers de géolocalisation dans Athena

Tâche	Description	Compétences requises
Créez une table Athena avec des données géospatiales.	Pour charger les fichiers de géolocalisation dans Athena, procédez comme suit : 1. Ouvrez la console Athena, puis choisissez Éditeur de requêtes dans le volet de navigation. 2. Choisissez l'onglet Requêtes enregistrées. 3. Recherchez et sélectionnez Q1 : Quartiers. 4. Pour revenir à l'éditeur de requêtes, cliquez sur l'onglet Editeur. 5. Cliquez sur Exécuter. Cela crée une table nommée `louisville_ky_neighborhoods` dans votre base de données. Assurez-vous que la table est créée dans la `athena-ml-db-<your-AWS-account-number>` base de données.	Ingénieur de données

Tâche	Description	Compétences requises
	La requête crée une nouvelle table pour les données géospatiales qui représent ent les quartiers urbains. La table de données est créée à partir de fichiers de formes SIG. L'`CREATE EXTERNAL TABLE`instruction définit le schéma de la table ainsi que l'emplacement et le format du fichier de données sous-jace nt. Pour le code Python permettant de traiter les fichiers de formes et de produire cette table, voir Traitement géospatia l des fichiers de formes SIG avec Amazon Athena dans Samples. AWS Pour obtenir un code SQL détaillé, consultez le fichier create_ne ighborhood_table.sql sur GitHub.	

Prédisez la demande de scooters par quartier à partir des données agrégées de DynamoDB

Tâche	Description	Compétences requises
Déclarez une fonction dans Athena pour interroger SageMaker l'IA.	1. Ouvrez la console Athena, choisissez l'éditeur de requêtes dans le volet de navigation, puis l'onglet Éditeur.	Scientifique des données, Ingénieur de données

Tâche	Description	Compétences requises
	2. Copiez et collez l'instruction SQL suivante dans l'éditeur de requêtes. `USING EXTERNAL FUNCTION predict_demand ( location_id BIGINT, hr BIGINT , dow BIGINT, n_pickup_1 BIGINT, n_pickup_2 BIGINT, n_pickup_3 BIGINT, n_pickup_4 BIGINT, n_dropoff_1 BIGINT, n_dropoff_2 BIGINT, n_dropoff_3 BIGINT, n_dropoff_4 BIGINT ) RETURNS DOUBLE SAGEMAKER '<Your SageMaker endpoint>'` La première partie de l'instruction SQL déclare la fonction externe chargée d'interroger les inférences ML à partir du point de terminaison SageMaker AI qui héberge le modèle préentraîné. 3. Définissez l'ordre et le type des paramètres d'entrée ainsi que le type des valeurs de retour. 4. Cliquez sur Exécuter.	

Tâche	Description	Compétences requises
Prédisez la demande de scooters par quartier à partir des données agrégées de DynamoDB.	Vous pouvez désormais utiliser Athena pour interroger des données transactionnelles directement depuis DynamoDB, puis agréger les données à des fins d'analyse et de prévision. Cela n'est pas facile à réaliser en interrogeant directement une base de données DynamoDB NoSQL. 1. Ouvrez la console Athena, puis choisissez l'éditeur de requêtes dans le volet de navigation. 2. Choisissez l'onglet Requêtes enregistrées. 3. Recherchez et sélectionnez Q2 : Dynamo DBAthena MLScooter Predict. 4. Pour revenir à l'éditeur de requêtes, cliquez sur l'onglet Editeur. 5. Cliquez sur Exécuter. L'instruction SQL effectue les opérations suivantes : • Utilise une requête fédérée Athena pour interroger la table DynamoDB contenant les données de trajet brutes • Place les coordonnées géographiques dans les	Développeur d'applications, data scientist

Tâche	Description	Compétences requises
	quartiers à l'aide des fonctions géospatiales d'Athéna • Enrichit les données grâce à l'inférence ML à l'aide de l'IA SageMaker Pour plus d'informations sur l'utilisation de SQL pour agréger les données DynamoDB SageMaker et les données d'inférence AI dans Athena, consultez le fichier athena_long.sql dans. GitHub	

Tâche	Description	Compétences requises
Vérifiez la sortie.	La table en sortie inclut le voisinage, la longitude et la latitude du centre de gravité du voisinage. Il inclut également le nombre de véhicules prévus pour l'heure suivante. La requête produit les prédictions pour un moment sélectionné. Vous pouvez faire des prédictions pour tout autre moment en modifiant l'expression `TIMESTAMP '2019-09-07 15:00'` partout dans l'instruction. Si votre table DynamoDB contient un flux de données en temps réel, remplacez l'horodatage par. `NOW()`	Développeur d'applications, data scientist

Nettoyez l'environnement

Tâche	Description	Compétences requises
Supprimez des ressources.	1. Ouvrez la console Athena et videz le bucket que vous avez créé dans le cadre de la CloudFormation pile. 2. Ouvrez la CloudFormation console, puis supprimez la pile nomméebdb-1462-	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	`athena-dynamodb-ml-stack` . 3. Ouvrez la CloudWatch console Amazon, puis supprimez le groupe de journaux nommé `/aws/sagemaker/Endpoints/Sg-athena-ml-dynamodb-model-endpoint` .	

Ressources connexes

- SDK Amazon Athena Query Federation () GitHub
- Interrogation de données géospatiales (documentation)AWS
- Utilisez les prédictions ML sur les données Amazon DynamoDB avec Amazon Athena ML (Big Data Blog)AWS
- Amazon ElastiCache (Redis OSS) (AWS documentation)
- Amazon Neptune (documentation)AWS

Associer un AWS CodeCommit référentiel dans un compte Compte AWS à Amazon SageMaker AI Studio Classic dans un autre compte

Créée par Laurens van der Maas (AWS) et Aubrey Oosthuizen (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle fournit des instructions et du code expliquant comment associer un AWS CodeCommit référentiel dans un compte Compte AWS (compte A) à Amazon SageMaker AI Studio Classic dans un autre Compte AWS (compte B). Pour configurer l'association, vous devez créer une politique et un rôle AWS Identity and Access Management (IAM) dans le compte A et une politique IAM en ligne dans le compte B. Ensuite, vous devez utiliser un script shell pour cloner le CodeCommit référentiel du compte A vers Amazon SageMaker AI Classic dans le compte B.

Conditions préalables et limitations

Prérequis

- Deux Comptes AWS, l'un contenant le CodeCommit référentiel et l'autre contenant un domaine SageMaker AI avec un utilisateur
- Domaine et utilisateur SageMaker AI provisionnés, avec accès à Internet ou accès à CodeCommit et AWS Security Token Service (AWS STS) via des points de terminaison de réseau privé virtuel (VPC)
- Compréhension de base de l'IAM
- Compréhension de base d'SageMaker AI Studio Classic
- Compréhension de base de Git et CodeCommit

Limites

Ce modèle s'applique uniquement à SageMaker AI Studio Classic, et non RStudio à Amazon SageMaker AI.

Architecture

Pile technologique

- Amazon SageMaker AI
- Amazon SageMaker AI Studio classique
- AWS CodeCommit
- AWS Identity and Access Management (JE SUIS)
- Git

Architecture cible

Le schéma suivant montre une architecture qui associe un CodeCommit référentiel du compte A à SageMaker AI Studio Classic dans le compte B.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur assume le `MyCrossAccountRepositoryContributorRole` rôle dans le compte A par le biais du `sts:AssumeRole` rôle, tandis qu'il utilise le rôle d'exécution SageMaker SageMaker AI dans AI Studio Classic dans le compte B. Le rôle assumé inclut les CodeCommit autorisations de clonage et d'interaction avec le référentiel spécifié.
2. L'utilisateur exécute des commandes Git depuis le terminal système dans SageMaker AI Studio Classic.

Automatisation et mise à l'échelle

Ce modèle comprend des étapes manuelles qui peuvent être automatisées à l'aide de AWS Cloud Development Kit (AWS CDK)AWS CloudFormation, ou Terraform.

Outils

Outils AWS

- Amazon SageMaker AI est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.

- Amazon SageMaker AI Studio Classic est un environnement de développement intégré (IDE) basé sur le Web pour l'apprentissage automatique qui vous permet de créer, de former, de déboguer, de déployer et de surveiller vos modèles d'apprentissage automatique.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.

  Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.

Autres outils

- Git est un système de contrôle de version distribué permettant de suivre les modifications du code source pendant le développement de logiciels.

Épopées

Création d'une politique IAM et d'un rôle IAM dans le compte A

Tâche	Description	Compétences requises
Créez une politique IAM pour l'accès au référentiel dans le compte A.	1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la. 2. Dans le volet de navigation, sélectionnez Politiques, puis Créer une politique. 3. Sélectionnez l'onglet JSON. 4. Copiez la déclaration de politique depuis Example IAM policy dans la section Informations supplémentaires de ce modèle, puis collez l'instruction dans	AWS DevOps

Tâche	Description	Compétences requises
	l'éditeur JSON. Assurez-vous de remplacer toutes les valeurs d'espace réservé dans la politique. 5. Choisissez Next:Tags, puis Next:Review. 6. Pour le Name (Nom), saisissez le nom de la politique. Remarque : Dans ce modèle, la stratégie IAM est appelée`CrossAccountAccessForMySharedDemoRepo` , mais vous pouvez choisir le nom de politique que vous préférez. 7. Choisissez Create Policy (Créer une politique). **Tip** Il est recommandé de limiter la portée de vos politiques IAM aux autorisations minimales requises pour votre cas d'utilisation.	

Tâche	Description	Compétences requises
Créez un rôle IAM pour accéder au référentiel dans le compte A.	1. Dans le volet de navigation de la console IAM, choisissez Rôles, puis Créer un rôle. 2. Pour le type d'entité de confiance, sélectionnez un compte AWS. 3. Dans la section Compte AWS, sélectionnez Un autre compte AWS. 4. Pour ID de compte, entrez l'ID de compte pour le compte B. 5. Sur la page Ajouter des autorisations, recherchez et choisissez la `CrossAccountAccessForMySharedDemoRepo` politique que vous avez créée précédemment. 6. Choisissez Suivant. 7. Pour Nom du rôle (Role name), saisissez un nom. Remarque : Dans ce modèle, le nom du rôle IAM est appelé`MyCrossAccountRepositoryContributorRole` , mais vous pouvez choisir le nom de rôle que vous préférez. 8. Choisissez Create role, puis copiez le Amazon Resource	AWS DevOps

Tâche	Description	Compétences requises
	Name (ARN) du nouveau rôle.	

Créez une politique en ligne IAM dans le compte B

Tâche	Description	Compétences requises
Associez une politique intégrée au rôle d'exécution associé à votre utilisateur de SageMaker domaine dans le compte B.	1. Dans le volet de navigation de la console IAM, choisissez Rôles. 2. Recherchez et choisissez le rôle d'exécution associé à votre utilisateur de domaine SageMaker AI dans le compte B. 3. Sélectionnez Ajouter des autorisations, puis Ajouter la politique. 4. Choisissez l'onglet JSON. 5. Copiez la déclaration de politique suivante, puis collez-la dans l'éditeur JSON. `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole",`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>"Resource": "arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>"
	}
	]
	}</pre>
	6. Remplacez `<Account_A_ID>` par l'ID de compte du compte A. Remplacez `<Account_A_Role_Name>` par le nom du rôle IAM que vous avez créé précédemment.
	7. Choisissez Examiner une politique.
	8. Dans Nom, entrez le nom de votre politique en ligne.
	9. Choisissez Create Policy (Créer une politique).	

Cloner le référentiel dans SageMaker AI Studio Classic pour le compte B

Tâche	Description	Compétences requises
Créez le script shell dans SageMaker AI Studio Classic dans le compte B.	1. Dans le volet de navigation de la SageMaker console, choisissez Studio. 2. Sélectionnez votre profil utilisateur, puis choisissez Open Studio. 3. Dans la section Accueil, choisissez Open Launcher.	AWS DevOps

Tâche	Description	Compétences requises
	4. Dans la section Utilitaires et fichiers, sélectionnez Fichier texte. 5. Copiez le script depuis SageMaker Example shell script dans la section Informations supplémentaires de ce modèle, puis collez l'instruction dans le nouveau fichier. Assurez-vous de remplacer toutes les valeurs d'espace réservé dans le script. 6. Cliquez avec le bouton droit sur l'onglet untitled.txt de votre nouveau fichier, puis choisissez Renommer le texte. Pour Nouveau nom, entrez cross_account_git_clone.sh, puis choisissez Renommer.	

Tâche	Description	Compétences requises
Appelez le script shell depuis le terminal système.	1. Dans la section Accueil de la SageMaker console, choisissez Open Launcher. 2. Dans la section Utilitaires et fichiers, choisissez Terminal système. 3. Dans le terminal, exécutez la commande suivante : `chmod u+x ./cross_account_git_clone.sh && ./cross_account_git_clone.sh` Vous avez cloné votre CodeCommit dépôt dans un compte croisé SageMaker AI Studio. Vous pouvez désormais exécuter toutes les commandes Git depuis le terminal système.	AWS DevOps

Informations supplémentaires

Exemple de politique IAM

Si vous utilisez cet exemple de politique, procédez comme suit :

- Remplacez `<CodeCommit_Repository_Region>` par le Région AWS pour le référentiel.
- Remplacez `<Account_A_ID>` par le numéro de compte du compte A.
- Remplacez `<CodeCommit_Repository_Name>` par le nom de votre CodeCommit dépôt dans le compte A.

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "codecommit:BatchGet*",
            "codecommit:Create*",
            "codecommit:DeleteBranch",
            "codecommit:Get*",
            "codecommit:List*",
            "codecommit:Describe*",
            "codecommit:Put*",
            "codecommit:Post*",
            "codecommit:Merge*",
            "codecommit:Test*",
            "codecommit:Update*",
            "codecommit:GitPull",
            "codecommit:GitPush"
        ],
        "Resource": [

 "arn:aws:codecommit:<CodeCommit_Repository_Region>:<Account_A_ID>:<CodeCommit_Repository_Name>
        ]
    }
]
}
```

Exemple de script shell SageMaker AI

Si vous utilisez cet exemple de script, procédez comme suit :

- Remplacez <Account_A_ID> par le numéro de compte du compte A.
- <Account_A_Role_Name>Remplacez-le par le nom du rôle IAM que vous avez créé précédemment.
- Remplacez <CodeCommit_Repository_Region> par le Région AWS pour le référentiel.
- Remplacez <CodeCommit_Repository_Name> par le nom de votre CodeCommit dépôt dans le compte A.

```
#!/usr/bin/env bash
```

```
#Launch from system terminal
pip install --quiet git-remote-codecommit

mkdir -p ~/.aws
touch ~/.aws/config

echo "[profile CrossAccountAccessProfile]
region = <CodeCommit_Repository_Region>
credential_source=EcsContainer
role_arn = arn:aws:iam::<Account_A_ID>:role/<Account_A_Role_Name>
output = json" > ~/.aws/config

echo '[credential "https://git-
codecommit.<CodeCommit_Repository_Region>.amazonaws.com"]
        helper = !aws codecommit credential-helper $@ --profile
 CrossAccountAccessProfile
        UseHttpPath = true' > ~/.gitconfig

git clone codecommit::<CodeCommit_Repository_Region>://
CrossAccountAccessProfile@<CodeCommit_Repository_Name>
```

Extrayez automatiquement le contenu de fichiers PDF à l'aide d'Amazon Textract

Créée par Tianxia Jia (AWS)

Récapitulatif

De nombreuses entreprises ont besoin d'extraire des informations à partir de fichiers PDF qui sont téléchargés vers leurs applications professionnelles. Par exemple, une organisation peut avoir besoin d'extraire avec précision des informations de fichiers PDF fiscaux ou médicaux à des fins d'analyse fiscale ou de traitement des demandes médicales.

Sur le cloud Amazon Web Services (AWS), Amazon Textract extrait automatiquement les informations (par exemple, le texte imprimé, les formulaires et les tableaux) des fichiers PDF et produit un fichier au format JSON contenant les informations du fichier PDF d'origine. Vous pouvez utiliser Amazon Textract dans l'AWS Management Console ou en implémentant des appels d'API. Nous vous recommandons d'utiliser des appels d'API programmatiques pour redimensionner et traiter automatiquement un grand nombre de fichiers PDF.

Lorsqu'Amazon Textract traite un fichier, il crée la liste d'`Block`objets suivante : pages, lignes et mots de texte, formulaires (paires clé-valeur), tableaux et cellules, et éléments de sélection. D'autres informations sur les objets sont également incluses, par exemple les cadres de délimitation, les intervalles de confiance et les relations. IDs Amazon Textract extrait les informations relatives au contenu sous forme de chaînes. Des valeurs de données correctement identifiées et transformées sont nécessaires car elles peuvent être plus facilement utilisées par vos applications en aval.

Ce modèle décrit un step-by-step flux de travail permettant d'utiliser Amazon Textract pour extraire automatiquement le contenu des fichiers PDF et le transformer en un résultat propre. Le modèle utilise une technique de correspondance de modèles pour identifier correctement le champ, le nom de clé et les tables requis, puis applique des corrections de post-traitement à chaque type de données. Vous pouvez utiliser ce modèle pour traiter différents types de fichiers PDF, puis redimensionner et automatiser ce flux de travail pour traiter des fichiers PDF au format identique.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.

- Un bucket Amazon Simple Storage Service (Amazon S3) existant pour stocker les fichiers PDF après leur conversion au format JPEG en vue de leur traitement par Amazon Textract. Pour plus d'informations sur les compartiments S3, consultez la présentation des compartiments dans la documentation Amazon S3.
- Le bloc-notes `Textract_PostProcessing.ipynb` Jupyter (joint), installé et configuré. Pour plus d'informations sur les blocs-notes Jupyter, consultez la section Créer un bloc-notes Jupyter dans la documentation Amazon. SageMaker
- Fichiers PDF existants au format identique.
- Compréhension de Python.

Limites

- Vos fichiers PDF doivent être de bonne qualité et clairement lisibles. Les fichiers PDF natifs sont recommandés, mais vous pouvez utiliser des documents numérisés convertis au format PDF si tous les mots sont clairs. Pour plus d'informations à ce sujet, consultez la section Prétraitement de documents PDF avec Amazon Textract : détection et suppression de visuels sur le blog AWS Machine Learning.
- Pour les fichiers de plusieurs pages, vous pouvez utiliser une opération asynchrone ou diviser les fichiers PDF en une seule page et utiliser une opération synchrone. Pour plus d'informations sur ces deux options, consultez les sections Détection et analyse du texte dans des documents multipages et Détection et analyse du texte dans des documents d'une seule page dans la documentation Amazon Textract.

Architecture

Le flux de travail de ce modèle exécute d'abord Amazon Textract sur un exemple de fichier PDF (première exécution), puis sur des fichiers PDF dont le format est identique à celui du premier PDF (exécution répétée). Le schéma suivant montre le flux de travail combiné de première exécution et de répétition qui extrait automatiquement et de manière répétée le contenu de fichiers PDF aux formats identiques.

Le diagramme montre le flux de travail suivant pour ce modèle :

1. Convertissez un fichier PDF au format JPEG et stockez-le dans un compartiment S3.

2. Appelez l'API Amazon Textract et analysez le fichier JSON de réponse Amazon Textract.
3. Modifiez le fichier JSON en ajoutant la bonne `KeyName:DataType` paire pour chaque champ obligatoire. Créez un `TemplateJSON` fichier pour l'étape Repeat run.
4. Définissez les fonctions de correction après le traitement pour chaque type de données (par exemple, float, entier et date).
5. Préparez les fichiers PDF dont le format est identique à celui de votre premier fichier PDF.
6. Appelez l'API Amazon Textract et analysez le JSON de réponse Amazon Textract.
7. Associez le fichier JSON analysé au `TemplateJSON` fichier.
8. Implémentez les corrections de post-traitement.

Le fichier de sortie JSON final contient le bon `KeyName` et `Value` pour chaque champ obligatoire.

Pile technologique cible

- Amazon SageMaker
- Amazon S3
- Amazon Textract

Automatisation et mise à l'échelle

Vous pouvez automatiser le flux de travail de répétition à l'aide d'une fonction AWS Lambda qui lance Amazon Textract lorsqu'un nouveau fichier PDF est ajouté à Amazon S3. Amazon Textract exécute ensuite les scripts de traitement et le résultat final peut être enregistré sur un emplacement de stockage. Pour plus d'informations à ce sujet, consultez la section Utilisation d'un déclencheur Amazon S3 pour appeler une fonction Lambda dans la documentation Lambda.

Outils

- Amazon SageMaker est un service de machine learning entièrement géré qui vous permet de créer et de former rapidement et facilement des modèles de machine learning, puis de les déployer directement dans un environnement hébergé prêt pour la production.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Textract permet d'ajouter facilement la détection et l'analyse du texte des documents à vos applications.

Épopées

Première course

Tâche	Description	Compétences requises
Convertissez le fichier PDF.	Préparez le fichier PDF pour votre première utilisation en le divisant en une seule page et en le convertissant au format JPEG pour l'opération synchrone Amazon Textract (). `Syn API` **Note** Vous pouvez également utiliser l'opération asynchrone Amazon Textract (`Asyn API`) pour les fichiers PDF de plusieurs pages.	Data scientist, développeur
Analysez le code JSON de réponse Amazon Textract.	Ouvrez le bloc-notes `Textract_PostProcessing.ipynb` Jupyter (joint) et appelez l'API Amazon Textract en utilisant le code suivant : `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET,`	Data scientist, développeur

Tâche	Description	Compétences requises
	<pre>'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])</pre> Analysez le JSON de réponse dans un formulaire et un tableau à l'aide du code suivant : <pre>parseformKV=form_kv_from_JSON(response) parseformTables=get_tables_fromJSON(response)</pre>	
Modifiez le fichier TemplateJSON.	Modifiez le JSON analysé pour chacun `KeyName` des en-têtes correspondants `DataType` (par exemple, chaîne, valeur flottante, entier ou date) et des en-têtes de tableau (par exemple, `ColumnNames` et `RowNames`). Ce modèle est utilisé pour chaque type de fichier PDF individuel, ce qui signifie qu'il peut être réutilisé pour des fichiers PDF au format identique.	Data scientist, développeur

Tâche	Description	Compétences requises
Définissez les fonctions de correction après le traitement.	Les valeurs figurant dans la réponse d'Amazon Textract pour le `TemplateJSON` fichier sont des chaînes. Il n'y a aucune différenciation pour la date, le flottant, le nombre entier ou la devise. Ces valeurs doivent être converties dans le type de données adapté à votre cas d'utilisation en aval. Corrigez chaque type de données en fonction du `TemplateJSON` fichier en utilisant le code suivant : `finalJSON=postprocessingCorrection(parsedJSON,templateJSON)`	Data scientist, développeur

Répéter la course

Tâche	Description	Compétences requises
Préparez les fichiers PDF.	Préparez les fichiers PDF en les divisant en une seule page et en les convertissant au format JPEG pour l'opération synchrone Amazon Textract (). `Syn API`	Data scientist, développeur

Tâche	Description	Compétences requises
	Note Vous pouvez également utiliser l'opération asynchrone Amazon Textract (`Asyn API`) pour les fichiers PDF de plusieurs pages.	
Appelez l'API Amazon Textract.	Appelez l'API Amazon Textract à l'aide du code suivant : `response = textract.analyze_document( Document={ 'S3Object': { 'Bucket': BUCKET, 'Name': '{}'.format(filename) } }, FeatureTypes=["TABLES", "FORMS"])`	Data scientist, développeur

Tâche	Description	Compétences requises

Analysez le code JSON de réponse Amazon Textract.	Analysez le JSON de réponse dans un formulaire et un tableau à l'aide du code suivant :
	`parseformKV=form_kv_from_JSON(response)`
	`parseformTables=get_tables_fromJSON(response)`
		Data scientist, développeur

Chargez le fichier TemplateJSON et associez-le au JSON analysé.	Utilisez le `TemplateJSON` fichier pour extraire les paires clé-valeur et le tableau corrects à l'aide des commandes suivantes :
	`form_kv_corrected=form_kv_correction(parseformKV,templateJSON)`
	`form_table_corrected=form_Table_correction(parseformTables, templateJSON)`
	`form_kv_table_corrected_final={**form_kv_corrected , **form_table_corrected}`
		Data scientist, développeur

Tâche	Description	Compétences requises
Corrections après le traitement.	Utilisez `DataType` les fonctions de `TemplateJSON` fichier et de post-traitement pour corriger les données à l'aide du code suivant : `finalJSON=postprocessingCorrection(form_kv_table_corrected_final,templateJSON)`	Data scientist, développeur

Ressources connexes

- Extrayez automatiquement du texte et des données structurées à partir de documents avec Amazon Textract
- Extrayez du texte et des données structurées avec Amazon Textract
- Ressources Amazon Textract

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez un modèle de prévision de démarrage à froid en utilisant DeePar pour les séries chronologiques dans Amazon SageMaker AI Studio Lab

Créée par Ivan Cui (AWS) et Eyal Shacham (AWS)

Récapitulatif

Que vous allouiez les ressources plus efficacement au trafic Web, que vous prédisiez la demande de patients pour les besoins en personnel ou que vous anticipiez les ventes des produits d'une entreprise, les prévisions sont un outil essentiel. Les prévisions de démarrage à froid établissent des prévisions pour une série chronologique contenant peu de données historiques, comme un nouveau produit qui vient d'entrer sur le marché de détail. Ce modèle utilise l'algorithme de prévision DeePar d'Amazon SageMaker AI pour entraîner un modèle de prévision de démarrage à froid et montre comment effectuer des prévisions sur des éléments de démarrage à froid.

DeepAR est un algorithme d'apprentissage supervisé permettant de prévoir des séries chronologiques scalaires (unidimensionnelles) à l'aide de réseaux neuronaux récurrents (RNN). DeePar adopte l'approche qui consiste à former un seul modèle conjointement sur toutes les séries chronologiques des produits connexes.

Les méthodes traditionnelles de prévision des séries chronologiques telles que la moyenne mobile intégrée autorégressive (ARIMA) ou le lissage exponentiel (ETS) s'appuient largement sur les séries chronologiques historiques de chaque produit individuel. Par conséquent, ces méthodes ne sont pas efficaces pour la prévision des démarrages à froid. Lorsque votre jeu de données contient des centaines de séries chronologiques connexes, DeepAR surpasse les méthodes ARIMA et ETS standard. Vous pouvez également utiliser le modèle entraîné pour générer des prévisions pour de nouvelles séries chronologiques similaires aux séries chronologiques sur lesquelles il a été entraîné.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Un domaine Amazon SageMaker AI.
- Une application de laboratoire Amazon SageMaker AI Studio ou Jupiter.

- Un bucket Amazon Simple Storage Service (Amazon S3) doté d'autorisations de lecture et d'écriture.
- Connaissance de la programmation en Python.
- Connaissance de l'utilisation d'un bloc-notes Jupyter.

Limites

- L'appel du modèle de prévision sans aucun point de données historique renverra une erreur. L'invocation du modèle avec un minimum de points de données historiques renverra des prédictions inexactes avec un niveau de confiance élevé. Ce schéma suggère une approche pour résoudre ces limites connues de la prévision des démarrages à froid.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Python version 3.10 ou ultérieure.
- Le bloc-notes du modèle a été testé dans Amazon SageMaker AI Studio sur une instance ml.t3.medium avec le noyau Python 3 (Data Science).

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Le flux de travail exécute les tâches suivantes :

1. Les fichiers d'entrée contenant les données d'entraînement et de test sont synthétisés puis téléchargés dans un compartiment Amazon S3. Ces données incluent plusieurs séries chronologiques avec des caractéristiques catégoriques et dynamiques, ainsi que des valeurs cibles (à prévoir). Le bloc-notes Jupyter visualise les données afin de mieux comprendre les exigences relatives aux données d'entraînement et les valeurs prédites attendues.
2. Une tâche de tuner d'hyperparamètres est créée pour entraîner le modèle et trouver le meilleur modèle en fonction de métriques prédéfinies.

3. Les fichiers d'entrée sont téléchargés depuis le compartiment Amazon S3 vers chaque instance des tâches de réglage des hyperparamètres.
4. Une fois que la tâche du tuner a sélectionné le meilleur modèle en fonction du seuil prédéfini du tuner, le modèle est déployé en tant que point de terminaison SageMaker AI.
5. Le modèle déployé est alors prêt à être invoqué et ses prédictions sont validées par rapport aux données de test.

Le carnet montre dans quelle mesure le modèle prédit les valeurs cibles lorsqu'un nombre suffisant de points de données historiques sont disponibles. Cependant, lorsque nous invoquons le modèle avec moins de points de données historiques (ce qui représente un produit froid), les prédictions du modèle ne correspondent pas aux données de test d'origine, même dans les limites des niveaux de confiance du modèle. Dans le modèle, un nouveau modèle est créé pour les produits froids, dont la longueur de contexte initiale (points prédits) est définie comme le nombre de points historiques disponibles, et un nouveau modèle est entraîné de manière itérative à mesure que de nouveaux points de données sont acquis. Le bloc-notes indique que le modèle produira des prévisions précises tant que la quantité de points de données historiques est proche de la longueur du contexte.

Outils

Services AWS

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon SageMaker AI est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.
- Amazon SageMaker AI Studio est un environnement de développement intégré (IDE) basé sur le Web pour le ML qui vous permet de créer, de former, de déboguer, de déployer et de surveiller vos modèles de ML.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub DeePar- ColdProduct -Pattern.

Bonnes pratiques

- Entraînez votre modèle dans un environnement virtuel et utilisez toujours le contrôle de version pour optimiser la reproductibilité.
- Incluez autant de fonctionnalités catégoriques de haute qualité que possible pour obtenir le meilleur modèle prédictif possible.
- Assurez-vous que les métadonnées contiennent des éléments catégoriels similaires afin que le modèle puisse déduire correctement les prévisions relatives aux produits de démarrage à froid.
- Exécutez une tâche de réglage des hyperparamètres pour obtenir le modèle prédictif le plus élevé.
- Dans ce modèle, le modèle que vous créez a une durée de contexte de 24 heures, ce qui signifie qu'il prédira les 24 prochaines heures. Si vous essayez de prévoir les prochaines 24 heures alors que vous disposez de moins de 24 heures de données historiques, la précision des prévisions du modèle se dégrade de manière linéaire en fonction du nombre de points de données historiques. Pour atténuer ce problème, créez un nouveau modèle pour chaque ensemble de points de données historiques jusqu'à ce que ce nombre atteigne la longueur de prédiction (contexte) souhaitée. Par exemple, commencez par un modèle de durée de contexte de 2 heures, puis augmentez progressivement le modèle à 4 heures, 8 heures, 16 heures et 24 heures.

Épopées

Démarrez votre application SageMaker AI Studio Classic

Tâche	Description	Compétences requises
Démarrez l'environnement de votre ordinateur portable.	1. Connectez-vous à et ouvrez AWS Managemen t Console la page d'accueil d' SageMaker AI Studio. Choisissez ensuite Open Studio. 2. Dans le volet de navigatio n de gauche, choisisse	Spécialiste des données

Tâche	Description	Compétences requises
	z l'icône Studio Classic dans Applications. Cliquez ensuite sur le bouton Ouvrir dans la liste des applicati ons. Pour plus d'informations, consultez la section Lancer Amazon SageMaker AI Studio dans la documentation sur l' SageMaker IA.	

Création et activation du bloc-notes

Tâche	Description	Compétences requises
Configurez votre environne ment virtuel pour la formation des modèles.	Pour configurer votre environnement virtuel pour l'entraînement des modèles, procédez comme suit : 1. Téléchargez le `deepar_sy nthetic.ipynb` bloc-notes depuis le GitHub référentiel de ce modèle sur votre machine locale. 2. Dans Amazon SageMaker AI Studio Classic, cliquez sur l'icône Charger des fichiers dans la barre de menu de Studio Classic et sélectionnez le bloc-notes téléchargé.	Spécialiste des données

Tâche	Description	Compétences requises
	3. Choisissez le bloc-notes dans le navigateur de fichiers dans le volet de navigation de gauche. Suivez les instructions pour configurer un environnement de bloc-notes. Sélectionnez l'image Data Science 3.0 et le noyau Python 3. Pour plus d'informations, consultez la section Charger des fichiers vers SageMaker AI Studio Classic dans la documentation sur l' SageMaker IA.	
Créez et validez un modèle de prévision.	• Suivez les instructions du bloc-notes pour créer les données d'entraînement et de test, entraîner le modèle, puis invoquer le modèle. • Observez la précision des prédictions du modèle lorsqu'il est fourni avec des points de données historiques adéquats.	Spécialiste des données

Ressources connexes

- Hyperparamètres DeePar
- Prévision de la demande pour le lancement de nouveaux produits à l'aide de services d'apprentissage AWS automatique

- Lancez Amazon SageMaker AI Studio Classic
- Utilisez l'algorithme de SageMaker prévision AI DeePar

Créez un MLOps flux de travail à l'aide d'Amazon SageMaker AI et d'Azure DevOps

Créée par Deepika Kumar (AWS), Philips Kokoh Prasetyo (AWS) et Sara van de Moosdijk (AWS)

Récapitulatif

Les opérations d'apprentissage automatique (MLOps) sont un ensemble de pratiques qui automatisent et simplifient les flux de travail et les déploiements de machine learning (ML). MLOps se concentre sur l'automatisation du cycle de vie du machine learning. Cela permet de garantir que les modèles ne sont pas seulement développés, mais également déployés, surveillés et réentraînés de manière systématique et répétée. Il apporte DevOps des principes au ML. MLOps se traduit par un déploiement plus rapide des modèles de machine learning, une meilleure précision au fil du temps et une meilleure assurance qu'ils apportent une réelle valeur commerciale.

Organisations disposent souvent d' DevOps outils et de solutions de stockage de données existants avant de commencer leur MLOps parcours. Ce modèle montre comment exploiter les points forts de Microsoft Azure et AWS. Il vous aide à intégrer Azure DevOps à Amazon SageMaker AI pour créer un MLOps flux de travail.

La solution simplifie le travail entre Azure et AWS. Vous pouvez utiliser Azure pour le développement et AWS l'apprentissage automatique. Il promeut un processus efficace pour créer des modèles d'apprentissage automatique du début à la fin, y compris le traitement des données, la formation et le déploiement AWS. Pour plus d'efficacité, vous gérez ces processus par le biais de DevOps pipelines Azure. La solution est applicable aux opérations de modèles de base (FMOps) et aux opérations de grands modèles de langage (LLMOps) dans l'IA générative, qui incluent le réglage fin, les bases de données vectorielles et la gestion rapide.

Conditions préalables et limitations

Prérequis

- Abonnement Azure : accès aux services Azure, tels qu'Azure DevOps, pour configurer les pipelines d'intégration continue et de déploiement continu (CI/CD).
- Compte AWS actif : autorisations d' Services AWS utilisation de l'utilisateur dans ce modèle.
- Données — Accès aux données historiques pour l'entraînement du modèle d'apprentissage automatique.

- Connaissance des concepts de machine learning — Compréhension de Python, des blocs-notes Jupyter et du développement de modèles d'apprentissage automatique.
- Configuration de sécurité : configuration appropriée des rôles, des politiques et des autorisations dans Azure et AWS afin de garantir un transfert et un accès sécurisés aux données.
- (Facultatif) Base de données vectorielle — Si vous utilisez une approche RAG (Retrieval Augmented Generation) et un service tiers pour la base de données vectorielle, vous devez accéder à la base de données vectorielle externe.

Limites

- Ce guide ne traite pas des transferts de données sécurisés entre clouds. Pour plus d'informations sur les transferts de données entre clouds, consultez la section AWS Solutions pour le cloud hybride et multicloud.
- Les solutions multicloud peuvent augmenter la latence pour le traitement des données en temps réel et l'inférence de modèles.
- Ce guide fournit un exemple d' MLOps architecture multi-comptes. Des ajustements sont nécessaires en fonction de votre AWS stratégie et de votre apprentissage automatique.
- Ce guide ne décrit pas l'utilisation de services d'intelligence artificielle et de machine learning autres qu'Amazon SageMaker AI.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Architecture cible

L'architecture cible intègre Azure DevOps à Amazon SageMaker AI, créant ainsi un flux de travail ML multicloud. Elle utilise Azure pour les CI/CD processes and SageMaker AI for ML model training and deployment. It outlines the process of obtaining data (from sources such as Amazon S3, Snowflake, and Azure Data Lake) through model building and deployment. Key components include CI/CD pipelines destinés à la création et au déploiement de modèles, à la préparation des données, à la gestion de l'infrastructure, et Amazon SageMaker AI pour la formation, le réglage, l'évaluation et le déploiement de modèles de machine learning. Cette architecture est conçue pour fournir des flux de travail ML efficaces, automatisés et évolutifs sur toutes les plateformes cloud.

L'architecture comprend les composants suivants :

1. Les data scientists réalisent des expériences de machine learning dans le compte de développement afin d'explorer différentes approches pour les cas d'utilisation du machine learning en utilisant différentes sources de données. Les data scientists réalisent des tests unitaires et des essais, et pour suivre leurs expériences, ils peuvent utiliser Amazon SageMaker AI avec MLflow. Dans le cadre du développement de modèles d'IA générative, les data scientists affinent les modèles de base à partir d'Amazon SageMaker AI JumpStart Model Hub. À la suite de l'évaluation du modèle, les data scientists transmettent et fusionnent le code dans le référentiel Model Build, qui est hébergé sur Azure DevOps. Ce référentiel contient le code d'un pipeline de création de modèles en plusieurs étapes.
2. Sur Azure DevOps, le pipeline Model Build, qui fournit une intégration continue (CI), peut être activé automatiquement ou manuellement lors de la fusion du code avec la branche principale. Dans le compte Automation, cela active le pipeline d' SageMaker IA pour le prétraitement des données, l'entraînement et le réglage précis des modèles, l'évaluation des modèles et l'enregistrement conditionnel des modèles en fonction de leur précision.
3. Le compte Automation est un compte central sur toutes les plateformes de ML qui héberge des environnements ML (Amazon ECR), des modèles (Amazon S3), des métadonnées de modèles (SageMaker AI Model Registry), des fonctionnalités (SageMaker AI Feature Store), des pipelines automatisés (SageMaker AI Pipelines) et des informations de journal ML (CloudWatch). Dans le cas d'une charge de travail d'IA générative, vous pouvez avoir besoin d'évaluations supplémentaires pour les invites dans les applications en aval. Une application de gestion rapide permet de rationaliser et d'automatiser le processus. Ce compte permet la réutilisation des actifs de ML et applique les meilleures pratiques pour accélérer la diffusion des cas d'utilisation du ML.
4. La dernière version du modèle est ajoutée au registre des modèles SageMaker AI pour examen. Il suit les versions des modèles et les artefacts respectifs (lignée et métadonnées). Il gère également le statut du modèle (approbation, rejet ou en attente) et gère la version pour le déploiement en aval.
5. Une fois qu'un modèle entraîné dans Model Registry a été approuvé via l'interface du studio ou un appel d'API, un événement peut être envoyé à Amazon EventBridge. EventBridge démarre le pipeline Model Deploy sur Azure DevOps.
6. Le pipeline Model Deploy, qui fournit un déploiement continu (CD), extrait la source du référentiel Model Deploy. La source contient le code, la configuration pour le déploiement du modèle et des scripts de test pour les tests de qualité. Le pipeline Model Deploy peut être adapté à votre type d'inférence.

7. Après des contrôles de qualité, le pipeline Model Deploy déploie le modèle sur le compte Staging. Le compte Staging est une copie du compte Production, et il est utilisé pour les tests et évaluations d'intégration. Pour une transformation par lots, le pipeline Model Deploy peut automatiquement mettre à jour le processus d'inférence par lots afin d'utiliser la dernière version approuvée du modèle. Pour une inférence en temps réel, sans serveur ou asynchrone, il configure ou met à jour le point de terminaison du modèle correspondant.
8. Après un test réussi dans le compte Staging, un modèle peut être déployé sur le compte Production par approbation manuelle via le pipeline Model Deploy. Ce pipeline fournit un point de terminaison de production lors de l'étape Déploiement vers la production, y compris la surveillance du modèle et un mécanisme de retour des données.
9. Une fois le modèle en production, utilisez des outils tels que SageMaker AI Model Monitor et SageMaker AI Clarify pour identifier les biais, détecter les dérives et surveiller en permanence les performances du modèle.

Automatisation et mise à l'échelle

Utilisez l'infrastructure en tant que code (IaC) pour le déployer automatiquement sur plusieurs comptes et environnements. En automatisant le processus de configuration d'un MLOps flux de travail, il est possible de séparer les environnements utilisés par les équipes de ML travaillant sur différents projets. AWS CloudFormationvous aide à modéliser, à approvisionner et à gérer les AWS ressources en traitant l'infrastructure comme du code.

Outils

Services AWS

- Amazon SageMaker AI est un service de machine learning géré qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.
- AWS Glueest un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données. Dans ce modèle, Amazon S3 est utilisé pour le stockage des données et intégré à l' SageMaker IA pour l'entraînement des modèles et les objets modèles.

- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez. Dans ce modèle, Lambda est utilisé pour les tâches de prétraitement et de post-traitement des données.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable. Dans ce modèle, il stocke les conteneurs Docker que l' SageMaker IA utilise comme environnements de formation et de déploiement.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Dans ce modèle, EventBridge orchestre des flux de travail basés sur des événements ou basés sur le temps qui initient le réentraînement ou le déploiement automatiques des modèles.
- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle. Dans ce modèle, il est utilisé pour créer un point d'entrée unique orienté vers l'extérieur pour les points de terminaison de l' SageMaker IA.
- Pour les applications RAG, vous pouvez les utiliser Services AWS, comme Amazon OpenSearch Service et Amazon RDS for PostgreSQL, pour stocker les intégrations vectorielles qui fournissent au LLM vos données internes.

Autres outils

- Azure vous DevOps aide à gérer les pipelines CI/CD et à faciliter la création, les tests et le déploiement de code.
- Azure Data Lake Storage ou Snowflake sont des sources tierces possibles de données de formation pour les modèles de machine learning.
- Pinecone, Milvus ou ChromaDB sont des bases de données vectorielles tierces possibles pour stocker des intégrations vectorielles.

Bonnes pratiques

Avant de mettre en œuvre un composant de ce MLOps flux de travail multicloud, effectuez les activités suivantes :

- Définissez et comprenez le flux de travail d'apprentissage automatique et les outils nécessaires pour le soutenir. Les différents cas d'utilisation nécessitent des flux de travail et des composants différents. Par exemple, un feature store peut être nécessaire pour la réutilisation des

fonctionnalités et l'inférence à faible latence dans un cas d'utilisation de personnalisation, mais il peut ne pas être nécessaire pour les autres cas d'utilisation. Il est nécessaire de comprendre le flux de travail cible, les exigences des cas d'utilisation et les méthodes de collaboration préférées de l'équipe de science des données pour personnaliser correctement l'architecture.

- Créez une séparation claire des responsabilités pour chaque composant de l'architecture. La répartition du stockage des données entre Azure Data Lake Storage, Snowflake et Amazon S3 peut accroître la complexité et les coûts. Si possible, choisissez un mécanisme de stockage cohérent. De même, évitez d'utiliser une combinaison de DevOps services Azure et AWS, ou une combinaison de services Azure et AWS ML.
- Choisissez un ou plusieurs modèles et ensembles de données existants pour end-to-end tester le MLOps flux de travail. Les artefacts de test doivent refléter des cas d'utilisation réels développés par les équipes de data science lorsque la plateforme entre en production.

Épopées

Concevez votre MLOps architecture

Tâche	Description	Compétences requises
Identifiez les sources de données.	Sur la base des cas d'utilisation actuels et futurs, des sources de données disponibles et des types de données (telles que les données confidentielles), documentez les sources de données qui doivent être intégrées à la MLOps plateforme. Les données peuvent être stockées dans Amazon S3, Azure Data Lake Storage, Snowflake ou d'autres sources. Pour les charges de travail génératives liées à l'IA, les données peuvent également inclure une base	Ingénieur de données, data scientist, architecte cloud

Tâche	Description	Compétences requises
	de connaissances qui fonde la réponse générée. Ces données sont stockées sous forme d'intégrations vectorielles dans des bases de données vectorielles. Créez un plan pour intégrer ces sources à votre plateforme et sécuriser l'accès aux bonnes ressources.	
Choisissez les services applicables.	Personnalisez l'architecture en ajoutant ou en supprimant des services en fonction du flux de travail souhaité par l'équipe de data science, des sources de données applicables et de l'architecture cloud existante. Par exemple, les ingénieurs de données et les scientifiques des données peuvent effectuer le prétraitement des données et l'ingénierie des fonctionnalités dans le domaine de l' SageMaker IA ou d'Amazon EMR. AWS Glue Il est peu probable que les trois services soient nécessaires.	Administrateur AWS, ingénieur de données, scientifique des données, ingénieur ML

Tâche	Description	Compétences requises
Analysez les exigences de sécurité.	Rassemblez et documentez les exigences de sécurité. Il s'agit notamment de déterminer : • Quelles équipes ou quels ingénieurs peuvent accéder à des sources de données spécifiques • Quelles équipes ou quels ingénieurs peuvent accéder à des modèles de base préformés • Si les équipes sont autorisées à accéder au code et aux modèles des autres équipes • Quelles autorisations (le cas échéant) les membres de l'équipe devraient avoir pour les comptes non liés au développement • Quelles mesures de sécurité doivent être mises en œuvre pour le transfert de données entre clouds Pour plus d'informations sur la sécurisation des charges de travail d'IA générative, voir Sécurisation de l'IA générative : introduction à la matrice de cadrage de la sécurité de	Administrateur AWS, architecte du cloud

Tâche	Description	Compétences requises
	l'IA générative (article de AWS blog).	

Configurez AWS Organizations

Tâche	Description	Compétences requises
Configurez AWS Organizations.	Configurez AWS Organizations à la racine Compte AWS. Cela vous permet de gérer les comptes suivants que vous créerez dans le cadre d'une MLOps stratégie multi-comptes. Pour plus d’informations, consultez la documentation AWS Organizations.	Administrateur AWS

Configuration de l'environnement de développement et de la gestion des versions

Tâche	Description	Compétences requises
Créez un compte AWS de développement.	Créez un environnement Compte AWS dans lequel les ingénieurs de données et les scientifiques des données sont autorisés à expérimenter et à créer des modèles de machine learning. Pour obtenir des instructions, consultez la section Création d'un compte membre dans votre organisation dans la AWS Organizations documentation.	Administrateur AWS

Tâche	Description	Compétences requises
Créez un référentiel Model Build.	Créez un référentiel Git dans Azure dans lequel les data scientists pourront transférer le code de création et de déploiement de leur modèle une fois la phase d'expérimentation terminée. Pour obtenir des instructions, consultez la section Configurer un référentiel Git dans la DevOps documentation Azure.	DevOps ingénieur, ingénieur ML
Créez un référentiel Model Deploy.	Créez un référentiel Git dans Azure qui stocke le code de déploiement standard et les modèles. Il doit inclure du code pour chaque option de déploiement utilisée par l'organisation, telle qu'identifiée lors de la phase de conception. Par exemple, il doit inclure des points de terminaison en temps réel, des points de terminaison asynchrones, une inférence sans serveur ou des transformations par lots. Pour obtenir des instructions, consultez la section Configurer un référentiel Git dans la DevOps documentation Azure.	DevOps ingénieur, ingénieur ML

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR.	Configurez un référentiel Amazon ECR qui stocke les environnements ML approuvés sous forme d'images Docker. Permettez aux data scientists et aux ingénieurs ML de définir de nouveaux environnements. Pour obtenir des instructions, consultez la section Création d'un référentiel privé dans la documentation Amazon ECR.	Ingénieur ML
Configurez SageMaker AI Studio.	Configurez SageMaker AI Studio sur le compte de développement conformément aux exigences de sécurité définies précédemment, aux outils de science des données préférés (tels que MLflow) et à l'environnement de développement intégré (IDE) préféré. Utilisez les configurations du cycle de vie pour automatiser l'installation des fonctionnalités clés et créer un environnement de développement uniforme pour les data scientists. Pour plus d'informations, consultez Amazon SageMaker AI Studio et le serveur MLflow de suivi dans la documentation sur l'SageMaker IA.	Data scientist, ingénieur ML, ingénieur Prompt

Intégrez les pipelines CI/CD

Tâche	Description	Compétences requises
Créez un compte Automation.	Créez un environnement Compte AWS dans lequel s'exécutent les pipelines et les tâches automatisés. Vous pouvez donner aux équipes de data science un accès en lecture à ce compte. Pour obtenir des instructions, consultez la section Création d'un compte membre dans votre organisation dans la AWS Organizations documentation.	Administrateur AWS
Configurez un registre de modèles.	Configurez le registre des modèles SageMaker AI dans le compte Automation. Ce registre stocke les métadonnées des modèles de machine learning et aide certains data scientists ou chefs d'équipe à approuver ou rejeter les modèles. Pour plus d'informations, consultez la section Enregistrer et déployer des modèles avec Model Registry dans la documentation de l' SageMaker IA.	Ingénieur ML
Créez un pipeline de construction de modèles.	Créez un pipeline CI/CD dans Azure qui démarre manuellement ou automatiquement lorsque le code est	DevOps ingénieur, ingénieur ML

Tâche	Description	Compétences requises
	transféré vers le référentiel Model Build. Le pipeline doit vérifier le code source et créer ou mettre à jour un pipeline d' SageMaker IA dans le compte Automation. Le pipeline doit ajouter un nouveau modèle au registre des modèles. Pour plus d'informations sur la création d'un pipeline, consultez la documentation Azure Pipelines.	

Construisez la pile de déploiement

Tâche	Description	Compétences requises
Créez des AWS comptes de préparation et de déploiement.	Créez Comptes AWS pour la mise en scène et le déploiement de modèles de machine learning. Ces comptes doivent être identiques pour permettre de tester avec précision les modèles lors de la mise en scène avant de passer à la production. Vous pouvez donner aux équipes de data science un accès en lecture au compte de mise en scène. Pour obtenir des instructions, consultez la section Création d'un compte membre dans votre organisation	Administrateur AWS

Tâche	Description	Compétences requises
	dans la AWS Organizations documentation.	
Configurez des compartiments S3 pour la surveillance des modèles.	Effectuez cette étape si vous souhaitez activer la surveillance des modèles pour les modèles déployés créés par le pipeline Model Deploy. Créez des compartiments Amazon S3 pour stocker les données d'entrée et de sortie. Pour plus d'informations sur la création de compartiments S3, consultez la section Création d'un compartiment dans la documentation Amazon S3. Configurez des autorisations entre comptes afin que les tâches de surveillance automatique des modèles s'exécutent dans le compte Automation. Pour plus d'informations, consultez la section Surveillance des données et de la qualité des modèles dans la documentation de l' SageMaker IA.	Ingénieur ML

Tâche	Description	Compétences requises
Créez un pipeline Model Deploy.	Créez un pipeline CI/CD dans Azure qui démarre lorsqu'un modèle est approuvé dans le registre des modèles. Le pipeline doit vérifier le code source et l'artefact du modèle, créer les modèles d'infrast ructure pour déployer le modèle dans les comptes de test et de production, déployer le modèle dans le compte de test, exécuter des tests automatisés, attendre l'approbation manuelle et déployer le modèle approuvé dans le compte de productio n. Pour plus d'informations sur la création d'un pipeline, consultez la documentation Azure Pipelines.	DevOps ingénieur, ingénieur ML

(Facultatif) Automatisez l'infrastructure de l'environnement ML

Tâche	Description	Compétences requises
Créez AWS CDK des CloudFormation modèles.	Définissez AWS Cloud Development Kit (AWS CDK) nos AWS CloudForm ation modèles pour tous les environnements qui doivent être déployés automatiq uement. Cela peut inclure l'environnement de développe ment, l'environnement	AWS DevOps

Tâche	Description	Compétences requises
	d'automatisation et les environnements de préparation et de déploiement. Pour plus d'informations, consultez la CloudFormationdocumentation AWS CDKet.	
Créez un pipeline d'infrastructure.	Créez un pipeline CI/CD dans Azure pour le déploiement de l'infrastructure. Un administrateur peut lancer ce pipeline pour créer de nouveaux environnements Comptes AWS et configurer les environnements dont l'équipe ML a besoin.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Surveillance et détection de la dérive insuffisantes — Une surveillance inadéquate peut entraîner la non-détection des problèmes de performance du modèle ou une dérive des données.	Renforcez les cadres de surveillance avec des outils tels qu'Amazon CloudWatch, SageMaker AI Model Monitor et SageMaker AI Clarify. Configurez des alertes pour une action immédiate en cas de problèmes identifiés.
Erreurs de déclenchement du pipeline CI — Le pipeline CI dans Azure DevOps peut ne pas être déclenché lors de la fusion de code en raison d'une mauvaise configuration.	Vérifiez les paramètres du DevOps projet Azure pour vous assurer que les webhooks sont correctement configurés et pointent vers les points de terminaison d' SageMaker IA appropriés.
Gouvernance — Le compte d'automatisation central risque de ne pas appliquer les meilleure	Auditez les paramètres du compte Automation, en vous assurant que tous les environne

Problème	Solution
s pratiques sur les plateformes d'apprentissage automatique, ce qui entraîne des flux de travail incohérents.	ments et modèles de ML sont conformes aux meilleures pratiques et politiques prédéfinies.
Retards d'approbation du registre des modèles : cela se produit lorsque la vérificat ion et l'approbation du modèle sont retardées , soit parce que les utilisateurs mettent du temps à l'examiner, soit en raison de problèmes techniques.	Mettez en œuvre un système de notification pour avertir les parties prenantes des modèles en attente d'approbation et rationaliser le processus de révision.
Défaillances liées aux événements de déploiement de modèles : les événement s envoyés pour démarrer les pipelines de déploiement de modèles peuvent échouer, ce qui entraîne des retards de déploiement.	Vérifiez qu'Amazon EventBridge dispose des autorisations et des modèles d'événements appropriés pour appeler correctement les DevOps pipelines Azure.
Goulets d'étranglement liés au déploiement de la production — Les processus d'approbation manuels peuvent créer des goulets d'étrangl ement et retarder le déploiement des modèles en production.	Optimisez le flux de travail d'approbation au sein du pipeline de déploiement des modèles, en promouvant des révisions en temps opportun et des canaux de communication clairs.

Ressources connexes

AWS documentation

- Documentation Amazon SageMaker AI
- Machine Learning Lens (framework AWS Well Architected)
- Planifier pour réussir MLOps (directives AWS prescriptives)

Autres AWS ressources

- MLOps feuille de route de base pour les entreprises utilisant Amazon SageMaker AI (article de AWS blog)

- AWS Summit ANZ 2022 - End-to-end MLOps pour les architectes (YouTube vidéo)
- FMOps/LLMOps: Opérationnalisez l'IA générative et ses différences avec MLOps (article de AWS blog)
- Opérationnalisez l'évaluation du LLM à grande échelle à l'aide d'Amazon SageMaker AI Clarify et MLOps des services (AWS article de blog)
- Le rôle des bases de données vectorielles dans les applications d'IA générative (article de AWS blog)

Documentation Azure

- DevOps Documentation Azure
- Documentation Azure Pipelines

Configurez la journalisation des appels de modèles dans Amazon Bedrock en utilisant AWS CloudFormation

Créée par Vikramaditya Bhatnagar (AWS)

Récapitulatif

Vous pouvez configurer Amazon Bedrock pour collecter les journaux d'invocation, les données d'entrée du modèle et les données de sortie du modèle pour toutes les invocations de modèle dans votre. Compte AWS Il s'agit d'une bonne pratique pour créer des applications d'IA générative robustes avec Amazon Bedrock. Vous pouvez stocker les journaux d'invocation des modèles dans un groupe de CloudWatch journaux Amazon Logs, dans un compartiment Amazon Simple Storage Service (Amazon S3), ou dans les deux. La présence de données de journal dans CloudWatch Logs vous permet de créer des filtres métriques, des alarmes et des tableaux de bord personnalisés. Amazon S3 est idéal pour répliquer des données sur Régions AWS ou pour le stockage à long terme, conformément aux politiques de votre entreprise.

Ce modèle fournit un exemple de AWS CloudFormation modèle qui utilise une approche d'infrastructure en tant que code (IaC) pour configurer la journalisation des appels de modèles pour Amazon Bedrock. Le modèle configure le stockage des journaux à la fois dans CloudWatch Logs et Amazon S3.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Les autorisations suivantes :
  - Autorisations pour créer des CloudFormation piles
  - Autorisations d'accès à Amazon Bedrock
  - Autorisations pour créer des buckets Amazon S3 et y accéder
  - Autorisations permettant de créer des groupes de CloudWatch journaux et d'y accéder
  - Autorisations pour créer des AWS Lambda fonctions et y accéder
  - Autorisations pour créer des clés et y accéder AWS Key Management Service (AWS KMS)

Limites

Ce modèle enregistre les appels du modèle à la fois vers CloudWatch Logs et Amazon S3. Il ne soutient pas le choix d'un seul de ces deux services.

Architecture

Architecture cible

Le CloudFormation modèle fournit les ressources suivantes dans votre cible Compte AWS :

- Un groupe de CloudWatch journaux pour stocker les journaux d'invocation des modèles
- Un compartiment Amazon S3 pour stocker les journaux d'invocation des modèles et une politique de compartiment correspondante
- Un compartiment Amazon S3 pour stocker les journaux d'accès côté serveur et une politique de compartiment correspondante
- Une AWS Lambda fonction qui configure les paramètres de journalisation dans Amazon Bedrock
- Un AWS KMS key et un alias de clé correspondant
- Un rôle de service AWS Identity and Access Management (IAM) pour Amazon Bedrock

Le schéma suivant montre comment les journaux d'invocation sont stockés après le déploiement de la CloudFormation pile associée à ce modèle. Amazon Bedrock publie des données de journal lorsque le modèle de base fournit du texte, une image, une vidéo ou intègre des données. Comme le montre le schéma, les compartiments Amazon S3 et le groupe de CloudWatch journaux Logs sont chiffrés avec un AWS KMS key.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur soumet une requête à un modèle de base dans Amazon Bedrock.
2. Amazon Bedrock assume le rôle de service IAM.
3. Amazon Bedrock génère des données de journal et les stocke dans un groupe de CloudWatch journaux de journaux et dans un compartiment Amazon S3.
4. Si un utilisateur lit, télécharge ou supprime des fichiers du compartiment Amazon S3 contenant les journaux d'invocation du modèle, ces activités sont enregistrées dans un autre compartiment Amazon S3 pour les journaux d'accès côté serveur.

Automatisation et mise à l'échelle

Pour adapter cette solution, vous pouvez déployer le CloudFormation modèle sous la forme d'une pile définie sur plusieurs Régions AWS et Comptes AWS. Pour plus d'informations, consultez la section Gestion des piles entre les comptes et les régions StackSets dans la CloudFormation documentation.

Outils

Services AWS

- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) des principales sociétés d'IA et d'Amazon via une API unifiée.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe.

Autres outils

- Git est un système de contrôle de version distribué et open source.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub enable-bedrock-logging-using-cloudformation.

Épopées

Créez la CloudFormation pile

Tâche	Description	Compétences requises
Téléchargez le CloudFormation modèle.	Téléchargez le CloudFormation modèle depuis le GitHub référentiel.	Architecte du cloud
Déployez le modèle.	Créez une pile dans votre compte cible et dans votre région. Dans la section Paramètres, spécifiez les valeurs des paramètres définis dans le modèle. Pour obtenir des instructions, consultez la section Création d'une pile dans la CloudFormation documentation.	Architecte du cloud

Tester la solution

Tâche	Description	Compétences requises
Activez l'accès aux modèles.	Dans Amazon Bedrock, ajoutez l'accès au modèle de base. Pour obtenir des instructions, consultez la section Ajouter ou supprimer l'accès aux modèles de fondation Amazon Bedrock dans la documentation Amazon Bedrock.	Architecte du cloud
Exécutez un exemple d'invite.	Dans Amazon Bedrock Playgrounds, lancez un	Architecte du cloud

Tâche	Description	Compétences requises
	exemple de demande. Pour obtenir des instructions, consultez la section Générer des réponses dans la console à l'aide de terrains de jeu dans la documentation Amazon Bedrock.	
Passez en revue la configuration de journalisation.	1. Connectez-vous à la console Amazon Bedrock. 2. Dans la barre de navigation, choisissez l' Région AWS endroit où vous avez déployé la CloudFormation pile. 3. Dans le volet de navigation de gauche, sous Configurations de Bedrock, choisissez Paramètres. 4. Assurez-vous des points suivants : • La journalisation des invocations du modèle est activée. • Tous les types de données sont sélectionnés. • Pour les destinations de journalisation, S3 et CloudWatch Logs sont sélectionnés.	Architecte du cloud

Tâche	Description	Compétences requises
Passez en revue le compartiment Amazon S3.	1. Dans la section Configurations S3, choisissez Browse S3. Cela ouvre le compartiment cible dans la console Amazon S3. 2. Vérifiez que les données de journalisation sont présentes pour l'exemple d'invite que vous avez exécuté précédemment.	Architecte du cloud

Tâche	Description	Compétences requises
Passez en revue le groupe de journaux.	1. Retournez à la page Paramètres de la console Amazon Bedrock. 2. Dans la section Configurations CloudWatch des journaux, passez en revue les paramètres du groupe de CloudWatch journaux des journaux. Notez le nom du groupe de journaux. 3. Ouvrez la CloudWatch console. 4. Dans le panneau de navigation, choisissez Journaux, Groupes de journaux. 5. Choisissez le nom du groupe de journaux dans lequel Amazon Bedrock publie les données de journal. 6. Vérifiez que les données de journalisation sont présentes pour l'exemple d'invite que vous avez exécuté précédemment.	Architecte du cloud

Ressources connexes

AWS documentation

- Accès à un compartiment Amazon S3 (documentation Amazon S3)
- Création et gestion de piles (CloudFormation documentation)

- Surveiller l'invocation du modèle (documentation Amazon Bedrock)
- Utilisation de groupes de journaux et de flux de CloudWatch journaux (documentation sur les journaux)

AWS articles de blog

- Surveillance des applications d'IA générative à l'aide d'Amazon Bedrock et de l'intégration d'Amazon CloudWatch
- Meilleures pratiques pour créer des applications d'IA générative robustes avec Amazon Bedrock Agents — Partie 1
- Meilleures pratiques pour créer des applications d'IA générative robustes avec Amazon Bedrock Agents — Partie 2

Créez une image de conteneur Docker personnalisée SageMaker et utilisez-la pour la formation des modèles dans AWS Step Functions

Créée par Julia Bluszcz (AWS), Neha Sharma (AWS), Aubrey Oosthuizen (AWS), Mohan Gowda Purushothama (AWS) et Mateusz Zaremba (AWS)

Récapitulatif

Ce modèle montre comment créer une image de conteneur Docker pour Amazon SageMaker et l'utiliser comme modèle de formation dans AWS Step Functions. En regroupant des algorithmes personnalisés dans un conteneur, vous pouvez exécuter presque n'importe quel code de l' SageMaker environnement, quels que soient le langage de programmation, le framework ou les dépendances.

Dans l'exemple de SageMaker bloc-notes fourni, l'image personnalisée du conteneur Docker est stockée dans Amazon Elastic Container Registry (Amazon ECR). Step Functions utilise ensuite le conteneur stocké dans Amazon ECR pour exécuter un script de traitement Python pour SageMaker. Le conteneur exporte ensuite le modèle vers Amazon Simple Storage Service (Amazon S3).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un rôle AWS Identity and Access Management (IAM) pour les utilisateurs disposant SageMaker d'autorisations Amazon S3
- Un rôle IAM pour Step Functions
- Connaissance de Python
- Connaissance du SDK Amazon SageMaker Python
- Connaissance de l'interface de ligne de commande AWS (AWS CLI)
- Connaissance du SDK AWS pour Python (Boto3)
- Connaissance d'Amazon ECR
- Connaissance de Docker

Versions du produit

- SDK AWS Step Functions pour la science des données, version 2.3.0
- Version SageMaker 2.78.0 du SDK Amazon Python

Architecture

Le schéma suivant montre un exemple de flux de travail permettant de créer une image de conteneur Docker pour SageMaker, puis de l'utiliser pour un modèle d'entraînement dans Step Functions :

Le schéma suivant illustre le flux de travail suivant :

1. Un data scientist ou un DevOps ingénieur utilise un SageMaker bloc-notes Amazon pour créer une image de conteneur Docker personnalisée.
2. Un data scientist ou un DevOps ingénieur stocke l'image du conteneur Docker dans un référentiel privé Amazon ECR qui se trouve dans un registre privé.
3. Un data scientist ou un DevOps ingénieur utilise le conteneur Docker pour exécuter une tâche de SageMaker traitement Python dans un flux de travail Step Functions.

Automatisation et mise à l'échelle

Dans ce modèle, l'exemple de SageMaker bloc-notes utilise un type d'instance de `ml.m5.xlarge` bloc-notes. Vous pouvez modifier le type d'instance en fonction de votre cas d'utilisation. Pour plus d'informations sur les types d'instances de SageMaker bloc-notes, consultez Amazon SageMaker Pricing.

Outils

- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon SageMaker est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.
- Le SDK Amazon SageMaker Python est une bibliothèque open source pour la formation et le déploiement de modèles d'apprentissage automatique sur. SageMaker

- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise.
- Le SDK AWS Step Functions Data Science Python est une bibliothèque open source qui vous aide à créer des flux de travail Step Functions qui traitent et publient des modèles d'apprentissage automatique.

Épopées

Créez une image de conteneur Docker personnalisée et stockez-la dans Amazon ECR

Tâche	Description	Compétences requises
Configurez Amazon ECR et créez un nouveau registre privé.	Si ce n'est pas déjà fait, configurez Amazon ECR en suivant les instructions de la section Configuration avec Amazon ECR dans le guide de l'utilisateur Amazon ECR. Chaque compte AWS est associé à un registre Amazon ECR privé par défaut.	DevOps ingénieur
Créez un référentiel privé Amazon ECR.	Suivez les instructions de la section Création d'un référentiel privé dans le guide de l'utilisateur Amazon ECR. **Note** Le référentiel que vous créez est l'endroit où vous stockerez vos images de conteneur Docker personnalisées.	DevOps ingénieur

Tâche	Description	Compétences requises

Créez un Dockerfile qui inclut les spécifications nécessaires à l'exécution de votre tâche de SageMaker traitement.	Créez un Dockerfile qui inclut les spécifications nécessaires pour exécuter votre tâche de SageMaker traitement en configurant un Dockerfile. Pour obtenir des instructions, consultez Adapter votre propre conteneur de formation dans le manuel Amazon SageMaker Developer Guide.
	
	Pour plus d'informations sur Dockerfiles, consultez la référence Dockerfile dans la documentation Docker.
	
	Exemple de cellules de code de bloc-notes Jupyter pour créer un Dockerfile
	
	Cellule 1
	
	`# Make docker folder`
	`!mkdir -p docker`
	
	Cellule 2
	
	`%%writefile docker/Do`
	`ckerfile`
	
	`FROM python:3.7-slim-bu`
	`ster`
	
	`RUN pip3 install`
	` pandas==0.25.3 scikit-`
	`learn==0.21.3`
		DevOps ingénieur

Tâche	Description	Compétences requises

	`ENV PYTHONUNBUFFERED=TRUE`
	
	`ENTRYPOINT ["python3"]`	

Tâche	Description	Compétences requises
Créez votre image de conteneur Docker et envoyez-la vers Amazon ECR.	1. Créez l'image du conteneur à l'aide du Dockerfile que vous avez créé en exécutant la `docker build` commande dans l'AWS CLI. 2. Transférez l'image du conteneur vers Amazon ECR en exécutant la `docker push` commande. Pour plus d'informations, voir Création et enregistrement du conteneur dans Création de votre propre conteneur d'algorithmes sur GitHub. Exemple de cellules de code de bloc-notes Jupyter pour créer et enregistrer une image Docker ⚠ Important Avant d'exécuter les cellules suivantes, assurez-vous d'avoir créé un Dockerfile et de l'avoir stocké dans le répertoire appelé. `docker` Assurez-vous également que vous avez créé un référentiel Amazon ECR et que vous remplacez la	DevOps ingénieur

Tâche	Description	Compétences requises

	`ecr_repository` valeur de la première cellule par le nom de votre référentiel.
	
	Cellule 1
	
	`import boto3`
	`tag = ':latest'`
	`account_id = boto3.client('sts').get_caller_identity().get('Account')`
	`region = boto3.Session().region_name`
	`ecr_repository = 'byoc'`
	
	`image_uri = '{}.dkr.ecr.{}.amazonaws.com/{}'.format(account_id, region, ecr_repository + tag)`
	
	Cellule 2
	
	`# Build docker image`
	`!docker build -t $image_uri docker`
	
	Cellule 3
	
	`# Authenticate to ECR`
	`!aws ecr get-login-password --region {region} | docker login --username AWS --password-stdin`	

Tâche	Description	Compétences requises

	`{account_id}.dkr.ecr.{region}.amazonaws.com`
	
	Cellule 4
	
	`# Push docker image`
	`!docker push $image_uri`
	
	Note
	Vous devez authentifier votre client Docker auprès de votre registre privé afin de pouvoir utiliser les commandes `docker push` et `docker pull`. Ces commandes envoient et extraient des images depuis et vers les référentiels de votre registre.	

Créez un flux de travail Step Functions qui utilise votre image de conteneur Docker personnalisée

Tâche	Description	Compétences requises
Créez un script Python qui inclut votre logique de traitement personnalisé et d'entraînement du modèle.	Rédigez une logique de traitement personnalisée à exécuter dans votre script de traitement des données. Ensuite, enregistrez-le sous	Spécialiste des données

Tâche	Description	Compétences requises

	la forme d'un script Python nommé`training.py` .
	
	Pour plus d'informations, voir Apportez votre propre modèle avec SageMaker le mode Script activé GitHub.
	
	Exemple de script Python incluant un traitement personnalisé et une logique d'entraînement du modèle
	
	`%%writefile training.py`
	`from numpy import empty`
	`import pandas as pd`
	`import os`
	`from sklearn import datasets, svm`
	`from joblib import dump, load`
	
	`if __name__ == '__main__':`
	`digits = datasets.load_digits()`
	`#create classifier object`
	`clf = svm.SVC(gamma=0.001, C=100.)`
	
	`#fit the model`
	`clf.fit(digits.data[:-1], digits.target[:-1])`
	
	`#model output in binary format`	

Tâche	Description	Compétences requises
	`output_path = os.path.join('/opt/ml/processing/model', "model.joblib") dump(clf, output_path)`	

Tâche	Description	Compétences requises

Créez un flux de travail Step Functions qui inclut votre tâche de SageMaker traitement comme l'une des étapes.	Installez et importez le SDK AWS Step Functions Data Science et chargez le fichier training.py sur Amazon S3. Utilisez ensuite le SDK Amazon SageMaker Python pour définir une étape de traitement dans Step Functions.
	
	⚠ Important
	Assurez-vous d'avoir créé un rôle d'exécution IAM pour Step Functions dans votre compte AWS.
	
	Exemple de configuration d'environnement et de script de formation personnalisé à télécharger sur Amazon S3
	
	`!pip install stepfunctions`
	
	`import boto3`
	`import stepfunctions`
	`import sagemaker`
	`import datetime`
	
	`from stepfunctions import steps`
	`from stepfunctions.inputs import ExecutionInput`
		Spécialiste des données

Tâche	Description	Compétences requises

	from stepfunct
	ions.steps import (
	    Chain
	)
	from stepfunct
	ions.workflow import
	 Workflow
	from sagemaker
	.processing import
	 ScriptProcessor,
	 ProcessingInput,
	 ProcessingOutput
	
	sagemaker_session =
	 sagemaker.Session()
	bucket = sagemaker
	_session.default_b
	ucket()
	role = sagemaker
	.get_execution_role()
	prefix = 'byoc-tra
	ining-model'
	
	# See prerequisites
	 section to create this
	 role
	workflow_execution_rol
	e = f"arn:aws:iam::
	{account_id}:role/Ama
	zonSageMaker-StepF
	unctionsWorkflowEx
	ecutionRole"
	
	execution_input =
	 ExecutionInput(
	    schema={
	        "Preproce
	ssingJobName": str})
	
	input_code = sagemaker
	_session.upload_data(	

Tâche	Description	Compétences requises
	`"training.py", bucket=bucket, key_prefix="preprocessing.py", )`	
	Exemple SageMaker de définition d'étape de traitement utilisant une image Amazon ECR personnalisée et un script Python	
	Note Assurez-vous d'utiliser le `execution_input` paramètre pour spécifier le nom de la tâche. La valeur du paramètre doit être unique à chaque exécution de la tâche. De plus, le code du fichier training.py est transmis en tant que `input` paramètre au`ProcessingStep` , ce qui signifie qu'il sera copié dans le conteneur . La destination du `ProcessingInput` code est la même que celle du deuxième argument contenu	

Tâche	Description	Compétences requises

	dans le `container_entrypoint` .
	
	`script_processor = ScriptProcessor(command=['python3'], image_uri=image_uri, role=role, instance_count=1, instance_type='ml.m5.xlarge')`
	
	`processing_step = steps.ProcessingStep( "training-step", processor=script_processor, job_name=execution_input["PreprocessingJobName"], inputs=[ ProcessingInput( source=input_code, destination="/opt/ml/processing/input/code", input_name="code", ), ], outputs=[`	

Tâche	Description	Compétences requises

	<pre>Processin
	gOutput(
	source='/
	opt/ml/processing/
	model',
	destinati
	on="s3://{}/{}".fo
	rmat(bucket, prefix),
	output_na
	me='byoc-example')
	],
	container_entrypoi
	nt=["python3", "/opt/
	ml/processing/input/c
	ode/training.py"],
	)</pre> Exemple de flux de travail Step Functions qui exécute une tâche SageMaker de traitement
	
	Note
	Cet exemple de flux de travail inclut uniquement l'étape de SageMaker traitement, et non un flux de travail Step Functions complet. Pour un exemple complet de flux de travail, consultez Example notebooks SageMaker dans la documentation du SDK AWS	

Tâche	Description	Compétences requises

	Step Functions Data Science.
	
	`workflow_graph = Chain([processing_step])`
	
	`workflow = Workflow( name="ProcessingWorkflow", definition=workflow_graph, role=workflow_execution_role )`
	
	`workflow.create()`
	`# Execute workflow`
	`execution = workflow.execute( inputs={ "PreprocessingJobName": str(datetime.datetime.now().strftime("%Y%m%d%H%M-%SS")), # Each pre processing job (SageMaker processing job) requires a unique name, } )`
	`execution_output = execution.get_output(wait=True)`	

Ressources connexes

- Données de traitement (Amazon SageMaker Developer Guide)
- Adaptation de votre propre conteneur de formation (Amazon SageMaker Developer Guide)

Utilisez les agents Amazon Bedrock pour automatiser la création de contrôles d'accès dans Amazon EKS via des instructions textuelles

Créée par Keshav Ganesh (AWS) et Sudhanshu Saurav (AWS)

Récapitulatif

Organisations rencontrent des difficultés en matière de gestion des contrôles d'accès et de mise à disposition des ressources lorsque plusieurs équipes doivent travailler avec un cluster Amazon Elastic Kubernetes Service (Amazon EKS) partagé. Un service Kubernetes géré tel qu'Amazon EKS a simplifié les opérations de cluster. Cependant, la charge administrative liée à la gestion de l'accès des équipes et des autorisations relatives aux ressources reste complexe et chronophage.

Ce modèle montre comment les agents Amazon Bedrock peuvent vous aider à automatiser la gestion des accès aux clusters Amazon EKS. Cette automatisation permet aux équipes de développement de se concentrer sur le développement de leurs applications principales plutôt que de s'occuper de la configuration et de la gestion du contrôle d'accès. Vous pouvez personnaliser un agent Amazon Bedrock pour effectuer des actions pour une grande variété de tâches à l'aide de simples instructions en langage naturel.

En utilisant AWS Lambda des fonctions sous forme de groupes d'actions, un agent Amazon Bedrock peut gérer des tâches telles que la création d'entrées d'accès utilisateur et la gestion des politiques d'accès. En outre, un agent Amazon Bedrock peut configurer des associations d'identité de pods qui permettent l'accès aux ressources AWS Identity and Access Management (IAM) pour les pods exécutés dans le cluster. Grâce à cette solution, les entreprises peuvent rationaliser l'administration de leur cluster Amazon EKS à l'aide de simples instructions textuelles, réduire les frais manuels et améliorer l'efficacité globale du développement.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Rôles et autorisations IAM établis pour le processus de déploiement. Cela inclut les autorisations pour accéder aux modèles Amazon Bedrock Foundation (FM), créer des fonctions Lambda et toute autre ressource requise sur l'ensemble de la cible. Comptes AWS
- Accès activé en mode actif Compte AWS à ces Amazon Bedrock FMs : Amazon Titan Text Embeddings V2 et Anthropic Claude 3 Haiku.

- AWS Command Line Interface (AWS CLI) version 2.9.11 ou ultérieure, installée et configurée.
- eksctl 0.194.0 ou version ultérieure, installé.

Limites

- Une formation et de la documentation peuvent être nécessaires pour garantir une adoption harmonieuse et une utilisation efficace de ces techniques. L'utilisation d'Amazon Bedrock, Amazon EKS, Lambda, OpenSearch Amazon Service et OpenAPI implique une période d'apprentissage importante pour les développeurs et les équipes. DevOps
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Cette solution exécute les étapes suivantes :

1. L'utilisateur interagit avec l'agent Amazon Bedrock en soumettant une invite ou une requête qui sert de saisie à l'agent pour qu'il puisse traiter et prendre des mesures.
2. Sur la base de l'invite, l'agent Amazon Bedrock vérifie le schéma OpenAPI pour identifier l'API correcte à cibler. Si l'agent Amazon Bedrock trouve le bon appel d'API, la demande est envoyée au groupe d'actions associé à la fonction Lambda qui implémente ces actions.
3. Si aucune API pertinente n'est trouvée, l'agent Amazon Bedrock interroge la OpenSearch collection. La OpenSearch collection utilise le contenu indexé de la base de connaissances provenant du compartiment Amazon S3 qui contient le guide de l'utilisateur Amazon EKS.
4. La OpenSearch collection renvoie des informations contextuelles pertinentes à l'agent Amazon Bedrock.
5. Pour les demandes exploitables (celles qui correspondent à une opération d'API), l'agent Amazon Bedrock s'exécute dans un cloud privé virtuel (VPC) et déclenche la fonction Lambda.
6. La fonction Lambda exécute une action basée sur les entrées de l'utilisateur dans le cluster Amazon EKS.

7. Le compartiment Amazon S3 pour le code Lambda stocke l'artefact dans lequel le code et la logique ont été écrits pour la fonction Lambda.

Outils

Services AWS

- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon OpenSearch Service est un service géré qui vous aide à déployer, exploiter et faire évoluer OpenSearch des clusters dans le AWS Cloud. Sa fonctionnalité de collecte vous aide à organiser vos données et à créer des bases de connaissances complètes que les assistants d'intelligence artificielle tels que les agents Amazon Bedrock peuvent utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- eksctl est un utilitaire de ligne de commande permettant de créer et de gérer des clusters Kubernetes sur Amazon EKS.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub eks-access-controls-bedrock-agent.

Bonnes pratiques

- Maintenez le niveau de sécurité le plus élevé possible lors de la mise en œuvre de ce modèle. Assurez-vous que le cluster Amazon EKS est privé, qu'il dispose d'autorisations d'accès limitées et que toutes les ressources se trouvent dans un cloud privé virtuel (VPC). Pour plus d'informations, consultez les meilleures pratiques en matière de sécurité dans la documentation Amazon EKS.
- Utilisez des clés gérées par le AWS KMS client dans la mesure du possible et accordez-leur des autorisations d'accès limitées.
- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le dépôt de ce modèle, exécutez la commande suivante sur votre station de travail locale : `git clone https://github.com/aws-samples/eks-access-controls-bedrock-agent.git`	AWS DevOps
Obtenez la Compte AWS pièce d'identité.	Pour obtenir l' Compte AWS identifiant, procédez comme suit : 1. Ouvrez un shell dans le dossier racine du dépôt cloné,. `eks-access-`	AWS DevOps

Tâche	Description	Compétences requises

	`controls-bedrock-agent`
	2. Pour obtenir votre Compte AWS identifiant, accédez au répertoire cloné et exécutez la commande suivante :
	`AWS_ACCOUNT=$(aws sts get-caller-identity --query "Account" --output text)`
	Cette commande enregistre votre Compte AWS identifiant dans la `AWS_ACCOUNT` variable.	

Tâche	Description	Compétences requises

Créez le compartiment S3 pour le code Lambda.	Pour implémenter cette solution, vous devez créer trois compartiments Amazon S3 ayant des objectifs différents, comme indiqué dans le schéma d'architecture. Les compartiments S3 sont destinés au code Lambda, à une base de connaissances et au schéma OpenAPI.
	
	Pour créer le bucket de code Lambda, procédez comme suit :
	
	1. Pour créer un compartiment S3 pour le code Lambda, exécutez la commande suivante :
	
	`aws s3 mb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --region us-east-1`
	
	2. Pour installer la dépendance au code Lambda, exécutez la commande suivante :
	
	`cd eks-lambda`
	`npm install`
	`tsc`
	`cd .. && cd opensearch-lambda`
	`npm install`
		AWS DevOps

Tâche	Description	Compétences requises
	``` tsc cd .. ``` 3. Pour empaqueter le code et le télécharger dans le compartiment S3 pour Lambda, exécutez la commande suivante : ``` aws cloudformation package \ --template-file eks- access-controls.yaml \ --s3-bucket bedrock- agent-lambda-artifa cts-${AWS_ACCOUNT} \ --output-template- file eks-access- controls-templat e.yaml \ --region us-east-1 ``` La commande package crée un nouveau CloudForm ation modèle (`eks-acces s-controls-templat e.yaml`) qui contient : • Références au code de fonction Lambda stocké dans votre compartiment S3. • Définitions pour toutes les AWS infrastructures requises, y compris le VPC, les sous-réseaux,	

Tâche	Description	Compétences requises
	l'agent Amazon Bedrock et la collection. OpenSearch Vous pouvez utiliser ce modèle pour déployer la solution complète en utilisant CloudFormation.	

Tâche	Description	Compétences requises

Créez le compartiment S3 pour la base de connaissances.	Pour créer le compartiment Amazon S3 pour la base de connaissances, procédez comme suit :
	1. Pour créer le compartiment Amazon S3 pour la base de connaissances, exécutez la commande suivante :
	`aws s3 mb s3://eks-knowledge-base-${AWS_ACCOUNT} --region us-east-1`
	2. Pour télécharger le guide de l'utilisateur Amazon EKS et le stocker dans un répertoire, exécutez les commandes suivantes :
	`mkdir dataSource`
	`cd dataSource`
	`curl https://docs.aws.amazon.com/pdfs/eks/latest/userguide/eks-ug.pdf -o eks-user-guide.pdf`
	3. Pour télécharger le guide de l'utilisateur dans le compartiment S3 que vous avez créé à l'étape 1, exécutez la commande suivante :
		AWS DevOps

Tâche	Description	Compétences requises
	``` aws s3 cp eks-user-guide.pdf s3://eks-knowledge-base-${AWS_ACCOUNT} \ --region us-east-1 \ ``` 4. Pour revenir au répertoire racine, exécutez la commande suivante : ``` cd .. ```	
Créez le compartiment S3 pour le schéma OpenAPI.	Pour créer le compartiment Amazon S3 pour le schéma OpenAPI, procédez comme suit : 1. Pour créer le compartiment S3, exécutez la commande suivante : ``` aws s3 mb s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1 ``` 2. Pour télécharger le schéma OpenAPI dans le compartiment S3, exécutez la commande suivante : ``` aws s3 cp openapi-schema.yaml s3://eks-openapi-schema-${AWS_ACCOUNT} --region us-east-1 ```	AWS DevOps

Déployez la CloudFormation pile

Tâche	Description	Compétences requises
Déployez la CloudFormation pile.	Pour déployer la CloudFormation pile, utilisez le fichier CloudFormation modèle `eks-access-controls-template.yaml` que vous avez créé précédemment. Pour des instructions plus détaillées, consultez la section Créer une pile à partir de la CloudFormation console dans la CloudFormation documentation. **Note** Le provisionnement de l' OpenSearch index avec le CloudFormation modèle prend environ 10 minutes. Une fois la pile créée, notez les `VPC_ID` et `PRIVATE_SUBNET ID` s.	AWS DevOps
Créez le cluster Amazon EKS.	Pour créer le cluster Amazon EKS au sein du VPC, procédez comme suit : 1. Créez une copie du fichier de `eks-config.yaml` configuration et nommez-	AWS DevOps

Tâche	Description	Compétences requises

	la commeeks-deploy.yaml .
	2. Ouvrez eks-deploy.yaml dans un éditeur de texte. Remplacez ensuite les valeurs d'espace réservé suivantes par des valeurs issues de la pile déployée : VPC_IDPRIVATE_SUBNET1 , et PRIVATE_SUBNET2
	3. Pour créer le cluster à l'aide de l'utilitaire eksctl, exécutez la commande suivante :
	`eksctl create cluster -f eks-deploy.yaml`
	Note
	Ce processus de création de clusters peut prendre jusqu'à 15 à 20 minutes.
	4. Pour vérifier que le cluster a bien été créé, exécutez les commandes suivantes :
	`aws eks describe-cluster --name`	

Tâche	Description	Compétences requises

	`--query "cluster.status"`
	`aws eks update-kubeconfig --name --region`
	`kubectl get nodes`
	
	Les résultats attendus sont les suivants :
	• L'état du cluster est `ACTIVE`.
	• La commande `kubectl get nodes` indique que tous les nœuds sont en `Ready` état.	

Connect la fonction Lambda et le cluster Amazon EKS

Tâche	Description	Compétences requises
Créez une connexion entre le cluster Amazon EKS et la fonction Lambda.	Pour configurer les autorisations réseau et IAM afin de permettre à la fonction Lambda de communiquer avec le cluster Amazon EKS, procédez comme suit : 1. Pour identifier le rôle IAM associé à la fonction Lambda, ouvrez et localisez AWS Management Console la fonction Lambda nommée. `bedrock-agent-eks-access-control` Notez le nom de	AWS DevOps

Tâche	Description	Compétences requises

	ressource Amazon (ARN) du rôle IAM.
	2. Pour créer une entrée d'accès dans le cluster Amazon EKS pour le rôle IAM de la fonction Lambda, exécutez la commande suivante :
	`aws eks create-access-entry --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN>`
	3. Pour attribuer `AmazonEKSClusterAdminPolicy` des autorisations à ce rôle, exécutez la commande suivante :
	`aws eks associate-access-policy --cluster-name eks-testing-cluster --principal-arn <principal-Role-ARN> --policy-arn arn:aws:eks::aws:cluster-access-policy/AmazonEKSClusterAdminPolicy --access-scope type=cluster`
	Pour plus d'informations, consultez Associer les	

Tâche	Description	Compétences requises
	politiques d'accès aux entrées d'accès et Amazon EKSCluster AdminPolicy dans la documentation Amazon EKS. 4. Localisez le groupe de sécurité du cluster Amazon EKS. Ajoutez une règle entrante pour autoriser le trafic réseau entrant de la fonction Lambda vers le cluster Amazon EKS. Utilisez les valeurs suivantes pour la règle de trafic entrant : • Type : HTTPS • Portée de ports : 443 • Source : groupe de sécurité Lambda Pour plus d'informations, consultez Configurer les règles des groupes de sécurité dans la documentation Amazon VPC.	

Tester la solution

Tâche	Description	Compétences requises
Testez l'agent Amazon Bedrock.	Avant de tester l'agent Amazon Bedrock, assurez-	AWS DevOps

Tâche	Description	Compétences requises
	vous de suivre les étapes suivantes : • Testez d'abord avec des rôles non liés à la productio n. • Documentez toutes les modifications apportées à l'accès au cluster. • Établissez un plan pour annuler les modifications si nécessaire. Pour accéder à l'agent Amazon Bedrock, procédez comme suit : 1. Connectez-vous à l' AWS Management Console aide d'un rôle IAM avec les autorisations Amazon Bedrock et ouvrez la console Amazon Bedrock à l'adresse. https://console.aws.amazon.com/bedrock/ 2. Sélectionnez Agents dans le volet de navigation de gauche. Choisissez ensuite votre agent configuré dans la section Agents. 3. Pour tester l'agent, essayez les exemples d'invite suivants dans lesquels vous le remplacez `Principal`	

Tâche	Description	Compétences requises
	`-ARN-OF-ROLE` par un véritable ARN de rôle IAM : • Pour créer une entrée d'accès pour tout rôle IAM auquel vous souhaitez fournir un accès au cluster EKS, utilisez l'invite suivante : `Create an access entry in cluster eks-testing-new for a role whose principal arn is <Principal-ARN-OF-ROLE> with access policy as AmazonEKSAdminPolicy` Résultat attendu : • L'agent doit confirmer la création de l'entrée d'accès. • Pour vérifier, utilisez AWS Management Console ou utilisez l'API Amazon EKS et exécutez la commande suivante : `aws eks list-access-entries --cluster-name ekscluster` • Pour décrire l'entrée d'accès que vous avez créée, utilisez l'invite suivante : `Describe an access`	

Tâche	Description	Compétences requises
	`entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Résultat attendu : • L'agent doit renvoyer les informations relatives à l'entrée d'accès. • Les détails doivent correspondre à ceux que vous avez configuré s précédemment pour l'entrée d'accès. • Pour supprimer l'entrée d'accès que vous avez créée, utilisez l'invite suivante : `Delete the access entry in cluster eks-testing-new whose principal arn is <Principal-ARN-OF-ROLE>` Résultat attendu : • L'agent doit confirmer la suppression de l'entrée d'accès. • Pour vérifier, utilisez AWS Management Console ou utilisez l'API Amazon EKS et exécutez la commande suivante : `aws eks`	

Tâche	Description	Compétences requises
	`list-access-entries --cluster-name ekscluster` Vous pouvez également demander à l'agent d'effectuer des actions pour les associations EKS Pod Identity. Pour plus de détails, consultez la documentation Amazon EKS pour savoir comment EKS Pod Identity autorise l'accès aux Services AWS pods.	

Nettoyage

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour nettoyer les ressources créées par ce modèle, procédez comme suit. Attendez que chaque étape de suppression soit terminée avant de passer à l'étape suivante. ⚠ Warning Cette procédure supprimera définitivement toutes les ressources créées par ces piles. Assurez-vous d'avoir sauvegard	AWS DevOps

Tâche	Description	Compétences requises

	é toutes les données importantes avant de continuer.
	
	1. Pour supprimer le cluster Amazon EKS, exécutez la commande suivante :
	
	`eksctl delete cluster -f eks-deploy.yaml`
	
	Note
	Cette opération peut prendre 15 à 20 minutes.
	
	2. Pour supprimer les compartiments Amazon S3, exécutez les commandes suivantes :
	• Pour vider le compartiment Lambda :
	
	`aws s3 rm s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT} --recursive`
	
	• Pour vider le compartiment de la base de connaissances, procédez comme suit :	

Tâche	Description	Compétences requises

	`aws s3 rm s3://eks-knowledge-base-${AWS_ACCOUNT} –recursive`
	• Pour vider le compartiment du schéma OpenAPI, procédez comme suit :
	`aws s3 rm s3://bedrock-agent-openapi-schema-${AWS_ACCOUNT} –recursive`
	• Pour supprimer les compartiments vides, procédez comme suit :
	`aws s3 rb s3://bedrock-agent-lambda-artifacts-${AWS_ACCOUNT}`
	`aws s3 rb s3://eks-knowledge-base-${AWS_ACCOUNT}`
	`aws s3 rb s3://bedrock-agent-openapi-schema-${AWS_ACCOUNT}`
	3. Pour supprimer la CloudFormation pile, exécutez la commande suivante :
	`aws cloudformation delete-stack \ --stack-name`	

Tâche	Description	Compétences requises

	4. Pour vérifier la suppression du cluster Amazon EKS, exécutez la commande suivante :
	`eksctl get clusters`
	5. Pour vérifier la suppression des compartiments Amazon S3, exécutez les commandes suivantes :
	• Pour vérifier la suppression du bucket Lambda, procédez comme suit :
	`aws s3 ls | grep "bedrock-agent-lambda-artifacts"`
	• Pour vérifier la suppression du bucket de la base de connaissances, procédez comme suit :
	`aws s3 ls | grep "eks-knowledge-base"`
	• Pour vérifier la suppression du bucket de schéma OpenAPI, procédez comme suit :
	`aws s3 ls | grep "bedrock-agent-openapi-schema"`	

Tâche	Description	Compétences requises
	6. Pour vérifier la suppression de la pile, exécutez la commande suivante : `aws cloudformation list-stacks \--query 'StackSummaries[?StackName==``]'` Si la pile ne parvient pas à être supprimée, consultez la section Résolution des problèmes.	

Résolution des problèmes

Problème	Solution
Un code d'erreur différent de zéro est renvoyé lors de la configuration de l'environnement.	Vérifiez que vous utilisez le bon dossier lorsque vous exécutez une commande pour déployer cette solution. Pour plus d'informations, consultez le fichier First_Deploy.md dans le référentiel de ce modèle.
La fonction Lambda n'est pas en mesure d'effectuer cette tâche.	Assurez-vous que la connectivité est correctement configurée entre la fonction Lambda et le cluster Amazon EKS.
Les instructions de l'agent ne reconnaissent pas le APIs.	Redéployez la solution. Pour plus d'informations, consultez le fichier RE_Deploy.md dans le référentiel de ce modèle.
La pile ne parvient pas à être supprimée.	Une première tentative de suppression de la pile peut échouer. Cet échec peut se produire en raison de problèmes de dépendance avec

Problème	Solution
	la ressource personnalisée créée pour la OpenSearch collection qui effectue l'indexation de la base de connaissances. Pour supprimer la pile, réessayez l'opération de suppression en conservant la ressource personnalisée.

Ressources connexes

AWS Blogue

- Présentation approfondie des contrôles de gestion d'accès simplifiés d'Amazon EKS

Documentation Amazon Bedrock

- Automatisez les tâches de votre application à l'aide d'agents d'intelligence artificielle
- Comment fonctionne Amazon Bedrock Agents
- Tester et résoudre les problèmes liés au comportement des agents
- Utilisez des groupes d'actions pour définir les actions à exécuter par votre agent

Documentation Amazon EKS

- Découvrez comment fonctionne le contrôle d'accès dans Amazon EKS

Déployez un cas d'utilisation de RAG AWS en utilisant Terraform et Amazon Bedrock

Créée par Martin Maritsch (AWS), Alice Morano (AWS), Julian Ferdinand Grueber (AWS), Nicolas Jacob Baer (AWS), Olivier Brique (AWS) et Nicola D Orazio (AWS)

Récapitulatif

AWS propose diverses options pour créer vos cas d'utilisation de l'IA générative compatibles avec le Retrieval Augmented Generation (RAG). Ce modèle vous fournit une solution pour une application basée sur RAG basée sur Amazon Aurora PostgreSQL LangChain et compatible avec Amazon Aurora en tant que magasin vectoriel. Vous pouvez déployer directement cette solution avec Terraform dans votre Compte AWS et implémenter le cas d'utilisation simple suivant de RAG :

1. L'utilisateur télécharge manuellement un fichier dans un compartiment Amazon Simple Storage Service (Amazon S3), tel qu'un fichier Microsoft Excel ou un document PDF. (Pour plus d'informations sur les types de fichiers pris en charge, consultez la documentation non structurée.)
2. Le contenu du fichier est extrait et intégré dans une base de connaissances basée sur la compatibilité sans serveur Aurora PostgreSQL, qui prend en charge l'ingestion de documents en temps quasi réel dans le magasin vectoriel. Cette approche permet au modèle RAG d'accéder aux informations pertinentes et de les récupérer pour les cas d'utilisation où les faibles latences sont importantes.
3. Lorsque l'utilisateur utilise le modèle de génération de texte, il améliore l'interaction en récupérant davantage de contenu pertinent à partir des fichiers précédemment téléchargés.

Le modèle utilise Amazon Titan Text Embeddings v2 comme modèle d'intégration et Anthropic Claude 3 Sonnet comme modèle de génération de texte, tous deux disponibles sur Amazon Bedrock.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Command Line Interface (AWS CLI) installé et configuré avec votre Compte AWS. Pour les instructions d'installation, voir Installer ou mettre à jour vers la dernière version AWS CLI de la AWS CLI documentation. Pour vérifier vos AWS informations d'identification et votre accès à votre

compte, consultez la section Configuration et paramètres des fichiers d'identification dans la AWS CLI documentation.

- Accès aux modèles activé pour les grands modèles linguistiques requis (LLMs) dans la console Amazon Bedrock de votre Compte AWS. Ce modèle nécessite les éléments suivants LLMs :
  - `amazon.titan-embed-text-v2:0`
  - `anthropic.claude-3-sonnet-20240229-v1:0`

Limites

- Cet exemple d'architecture n'inclut pas d'interface permettant de répondre aux questions par programmation avec la base de données vectorielle. Si votre cas d'utilisation nécessite une API, pensez à ajouter Amazon API Gateway avec une AWS Lambda fonction qui exécute des tâches de récupération et de réponse aux questions.
- Cet exemple d'architecture n'inclut pas de fonctionnalités de surveillance pour l'infrastructure déployée. Si votre cas d'utilisation nécessite une surveillance, pensez à ajouter AWS des services de surveillance.
- Si vous chargez un grand nombre de documents dans un court laps de temps dans le compartiment Amazon S3, la fonction Lambda peut rencontrer des limites de débit. Comme solution, vous pouvez dissocier la fonction Lambda d'une file d'attente Amazon Simple Queue Service (Amazon SQS) dans laquelle vous pouvez contrôler le taux d'invocations Lambda.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- AWS CLI version 2 ou ultérieure
- Docker version 26.0.0 ou ultérieure
- Poetry version 1.7.1 ou ultérieure
- Python version 3.10 ou ultérieure
- Terraform version 1.8.4 ou ultérieure

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Ce schéma illustre ce qui suit :

1. Lorsqu'un objet est créé dans le compartiment Amazon S3`bedrock-rag-template-<account_id>`, une notification Amazon S3 invoque la fonction `data-ingestion-processor` Lambda.
2. La fonction Lambda `data-ingestion-processor` est basée sur une image Docker stockée dans le référentiel Amazon Elastic Container Registry (Amazon ECR). `bedrock-rag-template`

   La fonction utilise le LangChain S3 FileLoader pour lire le fichier en tant que LangChain document. Ensuite, chaque document LangChain RecursiveCharacterTextSplitterest découpé en un `CHUNK_SIZE` et un `CHUNK_OVERLAP` qui dépendent de la taille maximale du jeton du modèle d'intégration Amazon Titan Text Embedding V2. Ensuite, la fonction Lambda invoque le modèle d'intégration sur Amazon Bedrock pour intégrer les segments dans des représentations vectorielles numériques. Enfin, ces vecteurs sont stockés dans la base de données Aurora PostgreSQL. Pour accéder à la base de données, la fonction Lambda extrait d'abord le nom d'utilisateur et le mot de passe de. AWS Secrets Manager
3. Sur l'instance de bloc-notes Amazon SageMaker AIaws-sample-bedrock-rag-template, l'utilisateur peut rédiger une demande de questions. Le code invoque Claude 3 sur Amazon Bedrock et ajoute les informations de la base de connaissances au contexte de l'invite. Par conséquent, Claude 3 fournit des réponses en utilisant les informations contenues dans les documents.

L'approche de ce modèle en matière de mise en réseau et de sécurité est la suivante :

- La fonction Lambda `data-ingestion-processor` se trouve dans un sous-réseau privé au sein du cloud privé virtuel (VPC). La fonction Lambda n'est pas autorisée à envoyer du trafic vers l'Internet public en raison de son groupe de sécurité. Par conséquent, le trafic vers Amazon S3 et Amazon Bedrock est acheminé uniquement via les points de terminaison VPC. Par conséquent, le trafic ne traverse pas l'Internet public, ce qui réduit la latence et ajoute une couche de sécurité supplémentaire au niveau du réseau.
- Toutes les ressources et données sont chiffrées le cas échéant à l'aide de la clé AWS Key Management Service (AWS KMS) avec l'aliasaws-sample/bedrock-rag-template.

Automatisation et mise à l'échelle

Ce modèle utilise Terraform pour déployer l'infrastructure depuis le référentiel de code dans un. Compte AWS

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL. Dans ce modèle, Aurora PostgreSQL compatible utilise le plugin pgvector comme base de données vectorielle.
- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable. Dans ce modèle, Amazon ECR héberge l'image Docker pour la fonction Lambda`data-ingestion-processor`.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez. Dans ce modèle, Lambda ingère des données dans le magasin vectoriel.
- Amazon SageMaker AI est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS. Le VPC inclut des sous-réseaux et des tables de routage pour contrôler le flux de trafic.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- Poetry est un outil de gestion des dépendances et d'empaquetage en Python.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub terraform-rag-template-using-amazon-bedrock.

Bonnes pratiques

- Bien que cet exemple de code puisse être déployé dans n'importe quel environnement Région AWS, nous vous recommandons d'utiliser l'est des États-Unis (Virginie du Nord) `us-east-1` ou l'ouest des États-Unis (Californie du Nord)`us-west-1`. Cette recommandation est basée sur la disponibilité des modèles de base et d'intégration dans Amazon Bedrock au moment de la publication de ce modèle. Pour obtenir la up-to-date liste des modèles Amazon Bedrock Foundation pris en charge dans Régions AWS, consultez la section Model support by Région AWS dans la documentation Amazon Bedrock. Pour plus d'informations sur le déploiement de cet exemple de code dans d'autres régions, consultez la section Informations supplémentaires.
- Ce modèle fournit uniquement une démonstration proof-of-concept (PoC) ou pilote. Si vous souhaitez mettre le code en production, veillez à suivre les meilleures pratiques suivantes :
  - Activez la journalisation des accès au serveur pour Amazon S3.
  - Configurez la surveillance et les alertes pour la fonction Lambda.
  - Si votre cas d'utilisation nécessite une API, pensez à ajouter Amazon API Gateway avec une fonction Lambda qui exécute des tâches de récupération et de réponse aux questions.

- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Déployez la solution dans un Compte AWS

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le GitHub référentiel fourni avec ce modèle, utilisez la commande suivante : `git clone https://github.com/aws-samples/terraform-rag-template-using-amazon-bedrock`	AWS DevOps
Configurez les variables.	Pour configurer les paramètres de ce modèle, procédez comme suit : 1. Sur votre ordinateur, dans le GitHub référentiel, utilisez la commande suivante pour ouvrir le `terraform` dossier : `cd terraform` 2. Ouvrez le `commons.tfvars` fichier et personnalisez les paramètres en fonction de vos besoins.	AWS DevOps

Tâche	Description	Compétences requises

Déployez la solution.	Pour déployer la solution, procédez comme suit :
	
	1. Dans le `terraform` dossier, utilisez la commande suivante pour exécuter Terraform et transmettre les variables que vous avez personnal isées :
	
	`terraform init`
	`terraform apply -var-file=commons.tfvars`
	
	2. Vérifiez que les ressources indiquées dans le schéma d'architecture ont été déployées avec succès.
	
	Le déploiement de l'infrast ructure fournit une instance d' SageMaker IA au sein du VPC et dispose des autorisat ions nécessaires pour accéder à la base de données Aurora PostgreSQL.
		AWS DevOps

Tester la solution

Tâche	Description	Compétences requises
Lancez la démo.	Une fois le déploiement de l'infrastructure précédent	AWS général

Tâche	Description	Compétences requises
	réussi, suivez les étapes suivantes pour exécuter la démonstration dans un bloc-notes Jupyter : 1. Connectez-vous à l' Compte AWS endroit où AWS Management Console l'infrastructure est déployée. 2. Ouvrez l'instance de bloc-notes SageMaker AIaws-sample-bedrock-rag-template . 3. Déplacez le bloc-note s rag_demo.ipynb Jupyter sur l'instance de bloc-notes SageMaker AI en utilisant le glisser-d époser. 4. Ouvrez rag_demo.ipynb l'instance du bloc-notes SageMaker AI et choisisse z le conda_python3 noyau. 5. Pour exécuter la démonstra tion, exécutez les cellules du bloc-notes. Le bloc-notes Jupyter vous guide tout au long du processus suivant : • Exigences relatives à l'install ation	

Tâche	Description	Compétences requises
	• Définition d'intégration • Connexion de la base de données • Ingestion de données • Récupération et génération de texte augmentée • Demandes relatives aux documents pertinents	

Nettoyer l'infrastructure

Tâche	Description	Compétences requises
Nettoyez l'infrastructure.	Pour supprimer toutes les ressources que vous avez créées lorsqu'elles ne sont plus nécessaires, utilisez la commande suivante : `terraform destroy -var-file=commons.tfvars`	AWS DevOps

Ressources connexes

AWS resources

- Création de fonctions Lambda avec Python
- Paramètres d'inférence pour les modèles de base
- Accès aux modèles de fondations Amazon Bedrock
- Le rôle des bases de données vectorielles dans les applications d'IA générative (AWS Database Blog)
- Utilisation d'Amazon Aurora PostgreSQL

Autres ressources

- documentation pgvector

Informations supplémentaires

Mettre en œuvre une base de données vectorielle

Ce modèle utilise la compatibilité avec Aurora PostgreSQL pour implémenter une base de données vectorielle pour RAG. Comme alternative à Aurora PostgreSQL, il fournit d'autres fonctionnalités et services pour RAG AWS , tels que les bases de connaissances Amazon Bedrock et Amazon Service. OpenSearch Vous pouvez choisir la solution qui répond le mieux à vos besoins spécifiques :

- Amazon OpenSearch Service fournit des moteurs de recherche et d'analyse distribués que vous pouvez utiliser pour stocker et interroger de gros volumes de données.
- Les bases de connaissances Amazon Bedrock sont conçues pour créer et déployer des bases de connaissances sous forme d'abstraction supplémentaire afin de simplifier le processus d'ingestion et de récupération de RAG. Les bases de connaissances Amazon Bedrock peuvent fonctionner à la fois avec Aurora PostgreSQL et Amazon Service. OpenSearch

Déploiement vers d'autres Régions AWS

Comme décrit dans Architecture, nous vous recommandons d'utiliser la région USA Est (Virginie du Nord) `us-east-1` ou USA Ouest (Californie du Nord) `us-west-1` pour déployer cet exemple de code. Cependant, il existe deux manières de déployer cet exemple de code dans des régions autres que `us-east-1` et`us-west-1`. Vous pouvez configurer la région de déploiement dans le `commons.tfvars` fichier. Pour l'accès au modèle de fondation interrégional, considérez les options suivantes :

- Traverser l'Internet public — Si le trafic peut traverser l'Internet public, ajoutez des passerelles Internet au VPC. Ajustez ensuite le groupe de sécurité attribué à la fonction Lambda `data-ingestion-processor` et à l'instance de bloc-notes SageMaker AI pour autoriser le trafic sortant vers l'Internet public.
- Ne pas passer par l'Internet public — Pour déployer cet exemple dans une région autre que `us-east-1` ou`us-west-1`, procédez comme suit :

1. Dans la `us-west-1` région `us-east-1` ou, créez un VPC supplémentaire, y compris un point de terminaison VPC pour. `bedrock-runtime`
2. Créez une connexion d'appairage en utilisant l'appairage VPC ou une passerelle de transit vers le VPC de l'application.
3. Lorsque vous configurez le client `bedrock-runtime` boto3 dans une fonction Lambda en dehors de `us-east-1` ou`us-west-1`, transmettez le nom DNS privé du point de terminaison VPC pour in `bedrock-runtime` ou `us-east-1` us-west-1 au client boto3. `endpoint_url`

Déployez une logique de prétraitement dans un modèle de machine learning sur un seul point de terminaison à l'aide d'un pipeline d'inférence sur Amazon SageMaker

Créée par Mohan Gowda Purushothama (AWS), Gabriel Rodriguez Garcia (AWS) et Mateusz Zaremba (AWS)

Récapitulatif

Ce modèle explique comment déployer plusieurs objets de modèle de pipeline sur un seul point de terminaison à l'aide d'un pipeline d'inférence dans Amazon SageMaker. L'objet du modèle de pipeline représente les différentes étapes du flux de travail d'apprentissage automatique (ML), telles que le prétraitement, l'inférence du modèle et le post-traitement. Pour illustrer le déploiement d'objets de modèle de pipeline connectés en série, ce modèle vous montre comment déployer un conteneur Scikit-learn de prétraitement et un modèle de régression basé sur l'algorithme d'apprentissage linéaire intégré. SageMaker Le déploiement est hébergé derrière un seul point de terminaison dans SageMaker.

> **Note**
>
> Le déploiement dans ce modèle utilise le type d'instance ml.m4.2xlarge. Nous vous recommandons d'utiliser un type d'instance adapté à vos exigences en matière de taille de données et à la complexité de votre flux de travail. Pour plus d'informations, consultez Amazon SageMaker Pricing. Ce modèle utilise des images Docker prédéfinies pour Scikit-learn, mais vous pouvez utiliser vos propres conteneurs Docker et les intégrer dans votre flux de travail.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Python 3.9
- SDK Amazon SageMaker Python et bibliothèque Boto3
- Rôle AWS Identity and Access Management (AWS IAM) avec SageMaker autorisations de base et autorisations Amazon Simple Storage Service (Amazon S3)

Versions du produit

- Kit de développement logiciel Amazon SageMaker Python 2.49.2

Architecture

Pile technologique cible

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon SageMaker
- Amazon SageMaker Studio
- Amazon Simple Storage Service (Amazon S3)
- Point de terminaison d'inférence en temps réel pour Amazon SageMaker

Architecture cible

Le schéma suivant montre l'architecture pour le déploiement d'un objet de modèle de SageMaker pipeline Amazon.

Le schéma suivant illustre le flux de travail suivant :

1. Un SageMaker bloc-notes déploie un modèle de pipeline.
2. Un compartiment S3 stocke les artefacts du modèle.
3. Amazon ECR obtient les images du conteneur source à partir du compartiment S3.

Outils

Outils AWS

- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon SageMaker est un service de machine learning géré qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.

- Amazon SageMaker Studio est un environnement de développement intégré (IDE) basé sur le Web pour le ML qui vous permet de créer, de former, de déboguer, de déployer et de surveiller vos modèles de ML.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

Le code de ce modèle est disponible dans le référentiel GitHub Inference Pipeline with Scikit-learn et Linear Learner.

Épopées

Préparer le jeu de données

Tâche	Description	Compétences requises

Préparez le jeu de données pour votre tâche de régressio n.	Ouvrez un bloc-notes dans Amazon SageMaker Studio.
	
	Pour importer toutes les bibliothèques nécessaires et initialiser votre environnement de travail, utilisez l'exemple de code suivant dans votre bloc-notes :
	
	`import sagemaker`
	`from sagemaker import get_execution_role`
	
	`sagemaker_session = sagemaker.Session()`
	
	`# Get a SageMaker-compatible role used by this Notebook Instance.`
	`role = get_execution_role()`
		Spécialiste des données

Tâche	Description	Compétences requises

	``
	# S3 prefix
	bucket = sagemaker
	_session.default_b
	ucket()
	prefix = "Scikit-L
	inearLearner-pipel
	ine-abalone-example"
	``
	Pour télécharger un exemple de jeu de données, ajoutez le code suivant à votre bloc-notes :
	``
	! mkdir abalone_data
	! aws s3 cp s3://sage
	maker-sample-files
	/datasets/tabular/
	uci_abalone/abalon
	e.csv ./abalone_data
	``
	Note
	L'exemple de ce modèle utilise l'ensemble de données Abalone du référentiel UCI Machine Learning.	

Tâche	Description	Compétences requises

Téléchargez l'ensemble de données dans un compartiment S3.	Dans le bloc-notes dans lequel vous avez préparé votre ensemble de données plus tôt, ajoutez le code suivant pour télécharger vos exemples de données dans un compartiment S3 :
	`WORK_DIRECTORY = "abalone_data"`
	
	`train_input = sagemaker_session.upload_data( path="{}/{}".format(WORK_DIRECTORY, "abalone.csv"), bucket=bucket, key_prefix="{}/{}".format(prefix, "train"), )`
		Spécialiste des données

Créez le préprocesseur de données à l'aide de SKLearn

Tâche	Description	Compétences requises
Préparez le script preprocessor.py.	1. Copiez la logique de prétraitement à partir du fichier Python dans le référentiel GitHub sklearn_abalone_featurizer.py, puis collez le code dans un fichier Python distinct appelé`sklearn_abalone_featurizer.py` . Vous pouvez modifier	Spécialiste des données

Tâche	Description	Compétences requises
	le code pour l'adapter à votre ensemble de données personnalisé et à votre flux de travail personnalisé. 2. Enregistrez le `sklearn_abalone_featurizer.py` fichier dans le répertoire racine de votre projet (c'est-à-dire au même endroit où vous exécutez votre SageMaker bloc-notes).	

Tâche	Description	Compétences requises

Créez l'objet SKLearn préprocesseur.	Pour créer un objet SKLearn préprocesseur (appelé SKLearn Estimator) que vous pouvez intégrer dans votre pipeline d'inférence final, exécutez le code suivant dans votre bloc-notes : SageMaker
	`from sagemaker.sklearn. estimator import SKLearn`
	
	`FRAMEWORK_VERSION = "0.23-1" script_path = "sklearn_abalone_f eaturizer.py"`
	
	`sklearn_preprocessor = SKLearn( entry_point=script _path, role=role, framework_version= FRAMEWORK_VERSION, instance_type="ml. c4.xlarge", sagemaker_session= sagemaker_session, ) sklearn_preproc essor.fit({"train": train_input})`
		Spécialiste des données

Tâche	Description	Compétences requises

Testez l'inférence du préprocesseur.	Pour vérifier que votre préprocesseur est correctem ent défini, lancez une tâche de transformation par lots en saisissant le code suivant dans votre SageMaker bloc-notes :
	
	`# Define a SKLearn Transformer from the trained SKLearn Estimator`
	`transformer = sklearn_preprocessor.transformer(`
	`instance_count=1, instance_type="ml.m5.xlarge", assemble_with="Line", accept="text/csv"`
	`)`
	
	`# Preprocess training input`
	`transformer.transform(train_input, content_type="text/csv")`
	`print("Waiting for transform job: " + transformer.latest_transform_job.job_name)`
	`transformer.wait()`
	`preprocessed_train = transformer.output_path`	

Création d'un modèle d'apprentissage automatique

Tâche	Description	Compétences requises

Créez un objet modèle.	Pour créer un objet modèle basé sur l'algorithme d'apprentissage linéaire, entrez le code suivant dans votre SageMaker bloc-notes :
	`import boto3`
	`from sagemaker`
	`.image_uris import`
	` retrieve`
	
	`ll_image = retrieve(`
	`"linear-learner",`
	` boto3.Session().re`
	`gion_name)`
	`s3_ll_output_key`
	`_prefix = "ll_train`
	`ing_output"`
	`s3_ll_output_location`
	` = "s3://{}/{}/{}/{}"`
	`.format(`
	`  bucket, prefix,`
	` s3_ll_output_key_p`
	`refix, "ll_model"`
	`)`
	
	`ll_estimator =`
	` sagemaker.estimato`
	`r.Estimator(`
	`  ll_image,`
	`  role,`
	`  instance_count=1,`
	`  instance_type="ml.`
	`m4.2xlarge",`
	`  volume_size=20,`
	`  max_run=3600,`
	`  input_mode="File",`
		Spécialiste des données

Tâche	Description	Compétences requises

	<pre> output_path=s3_ll_
	output_location,
	    sagemaker_session=
	sagemaker_session,
	)
	
	ll_estimator.s
	et_hyperparameters
	(feature_dim=10,
	 predictor_type="re
	gressor", mini_batc
	h_size=32)
	
	ll_train_data =
	 sagemaker.inputs.T
	rainingInput(
	    preprocessed_train
	,
	    distribution="Full
	yReplicated",
	    content_type="text
	/csv",
	    s3_data_type="S3Pr
	efix",
	)
	
	data_channels =
	 {"train": ll_train_
	data}
	ll_estimator.fit(inpu
	ts=data_channels,
	 logs=True)</pre> Le code précédent extrait l'image Amazon ECR Docker appropriée du registre Amazon ECR public pour le modèle, crée un objet estimateur, puis utilise cet	

Tâche	Description	Compétences requises
	objet pour entraîner le modèle de régression.	

Déployer le pipeline final

Tâche	Description	Compétences requises

Déployez le modèle de pipeline.	Pour créer un objet de modèle de pipeline (c'est-à-dire un objet préprocesseur) et déployer l'objet, entrez le code suivant dans votre SageMaker bloc-notes :
	`from sagemaker.model import Model`
	`from sagemaker.pipeline import PipelineModel`
	`import boto3`
	`from time import gmtime, strftime`
	
	`timestamp_prefix = strftime("%Y-%m-%d-%H-%M-%S", gmtime())`
	
	`scikit_learn_inferencee_model = sklearn_preprocessor.create_model()`
	`linear_learner_model = ll_estimator.create_model()`
	
	`model_name = "inference-pipeline-" + timestamp_prefix`
		Spécialiste des données

Tâche	Description	Compétences requises
	``` endpoint_name = "inference-pipeline- ep-" + timestamp_prefix sm_model = PipelineM odel(name=model_name, role=role, models= [scikit_learn_infe rencee_model, linear_learner_model]) sm_model.deploy(init ial_instance_count =1, instance_type="ml. c4.xlarge", endpoint_ name=endpoint_name) ``` **Note** Vous pouvez ajuster le type d'instance utilisé dans l'objet du modèle en fonction de vos besoins.	

Tâche	Description	Compétences requises

Testez l'inférence.	Pour vérifier que le point de terminaison fonctionn e correctement, exécutez l'exemple de code d'inférence suivant dans votre SageMaker bloc-notes :
	`from sagemaker.predicto r import Predictor from sagemaker.serializ ers import CSVSerial izer`
	
	`payload = "M, 0.44, 0.365, 0.125, 0.516, 0.2155, 0.114, 0.155" actual_rings = 10 predictor = Predictor( endpoint_name=endp oint_name, sagemaker _session=sagemaker _session, serialize r=CSVSerializer() )`
	
	`print(predictor .predict(payload))`
		Spécialiste des données

Ressources connexes

- Prétraitez les données d'entrée avant de faire des prédictions à l'aide des pipelines SageMaker d'inférence Amazon et de Scikit-learn (AWS Machine Learning Blog)
- Machine Learning de bout en bout avec Amazon SageMaker (GitHub)

Développez des assistants avancés basés sur l'IA générative basés sur le chat en utilisant RAG et des instructions ReAct

Créée par Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS) et Shuai Cao (AWS)

Récapitulatif

Une entreprise typique a 70 % de ses données piégées dans des systèmes cloisonnés. Vous pouvez utiliser des assistants basés sur le chat basés sur l'IA générative pour obtenir des informations et établir des relations entre ces silos de données grâce à des interactions en langage naturel. Pour tirer le meilleur parti de l'IA générative, les résultats doivent être fiables, précis et inclure les données d'entreprise disponibles. Le succès des assistants basés sur le chat dépend des éléments suivants :

- Modèles d'IA génératifs (tels qu'Anthropic Claude 2)
- Vectorisation des sources de données
- Techniques de raisonnement avancées, telles que le ReAct cadre, pour orienter le modèle

Ce modèle propose des approches de récupération de données à partir de sources de données telles que les buckets Amazon Simple Storage Service (Amazon S3), AWS Glue et Amazon Relational Database Service (Amazon RDS). La valeur est obtenue à partir de ces données en entrelacant la génération augmentée de récupération (RAG) avec des méthodes. chain-of-thought Les résultats permettent des conversations d'assistant complexes basées sur le chat qui s'appuient sur l'intégralité des données stockées par votre entreprise.

Ce modèle utilise les SageMaker manuels Amazon et les tableaux de données de tarification comme exemple pour explorer les fonctionnalités d'un assistant génératif basé sur le chat basé sur l'IA. Vous allez créer un assistant basé sur le chat qui aidera les clients à évaluer le SageMaker service en répondant à des questions sur les prix et les fonctionnalités du service. La solution utilise une bibliothèque Streamlit pour créer l'application frontale et le LangChain framework pour développer le backend de l'application basé sur un modèle de langage étendu (LLM).

Les demandes adressées à l'assistant basé sur le chat sont traitées selon une classification d'intention initiale pour être acheminées vers l'un des trois flux de travail possibles. Le flux de travail le plus sophistiqué combine des conseils généraux avec une analyse tarifaire complexe. Vous pouvez adapter le modèle en fonction des cas d'utilisation en entreprise, corporatif et industriel.

Conditions préalables et limitations

Prérequis

- Interface de ligne de commande (AWS CLI) (AWS CLI) installée et configurée
- AWS Cloud Development Kit (AWS CDK) Toolkit 2.114.1 ou version ultérieure installée et configurée
- Connaissance de base de Python et d'AWS CDK
- Git installé
- Docker installé
- Python 3.11 ou version ultérieure installé et configuré (pour plus d'informations, consultez la section Outils)
- Un compte AWS actif démarré à l'aide d'AWS CDK
- Accès aux modèles Amazon Titan et Anthropic Claude activé dans le service Amazon Bedrock
- Informations d'identification de sécurité AWS`AWS_ACCESS_KEY_ID`, y compris celles correctement configurées dans votre environnement de terminal

Limites

- LangChain ne prend pas en charge tous les LLM pour le streaming. Les modèles Anthropic Claude sont pris en charge, mais pas les modèles de AI21 Labs.
- Cette solution est déployée sur un seul compte AWS.
- Cette solution ne peut être déployée que dans les régions AWS où Amazon Bedrock et Amazon Kendra sont disponibles. Pour plus d'informations sur la disponibilité, consultez la documentation d'Amazon Bedrock et d'Amazon Kendra.

Versions du produit

- Python version 3.11 ou ultérieure
- Streamlit version 1.30.0 ou ultérieure
- StreamLit-Chat version 0.1.1 ou ultérieure
- LangChain version 0.1.12 ou ultérieure
- AWS CDK version 2.132.1 ou ultérieure

Architecture

Pile technologique cible

- Amazon Athena
- Amazon Bedrock
- Amazon Elastic Container Service (Amazon ECS)
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon Kendra
- Elastic Load Balancing

Architecture cible

Le code AWS CDK déploiera toutes les ressources nécessaires pour configurer l'application d'assistant basée sur le chat dans un compte AWS. L'application d'assistance basée sur le chat illustrée dans le schéma suivant est conçue pour répondre aux questions SageMaker connexes des utilisateurs. Les utilisateurs se connectent via un Application Load Balancer à un VPC contenant un cluster Amazon ECS hébergeant l'application Streamlit. Une fonction Lambda d'orchestration se connecte à l'application. Les sources de données du compartiment S3 fournissent des données à la fonction Lambda via Amazon Kendra et AWS Glue. La fonction Lambda se connecte à Amazon Bedrock pour répondre aux requêtes (questions) des utilisateurs assistants basés sur le chat.

1. La fonction Lambda d'orchestration envoie la demande d'invite LLM au modèle Amazon Bedrock (Claude 2).
2. Amazon Bedrock renvoie la réponse LLM à la fonction Lambda d'orchestration.

Flux logique au sein de la fonction Lambda d'orchestration

Lorsque les utilisateurs posent une question via l'application Streamlit, celle-ci invoque directement la fonction Lambda d'orchestration. Le schéma suivant montre le flux logique lorsque la fonction Lambda est invoquée.

- Étape 1 — L'entrée `query` (question) est classée dans l'une des trois intentions suivantes :
  - Questions SageMaker d'orientation générales
  - Questions générales SageMaker sur la tarification (formation/inférence)
  - Questions complexes relatives à la tarification SageMaker et à la tarification
- Étape 2 — L'entrée `query` initie l'un des trois services :
  - `RAG Retrieval service`, qui extrait le contexte pertinent de la base de données vectorielle Amazon Kendra et appelle le LLM via Amazon Bedrock pour résumer le contexte extrait sous forme de réponse.
  - `Database Query service`, qui utilise le LLM, les métadonnées de la base de données et des exemples de lignes provenant de tables pertinentes pour convertir l'`query`entrée en requête SQL. Le service Database Query exécute la requête SQL par rapport à la base de données de SageMaker tarification via Amazon Athena et résume les résultats de la requête sous forme de réponse.
  - `In-context ReACT Agent service`, qui décompose la saisie `query` en plusieurs étapes avant de fournir une réponse. L'agent utilise `RAG Retrieval service` et `Database Query service` comme outils pour récupérer les informations pertinentes au cours du processus de raisonnement. Une fois les processus de raisonnement et d'action terminés, l'agent génère la réponse finale en tant que réponse.
- Étape 3 — La réponse de la fonction Lambda d'orchestration est envoyée à l'application Streamlit en sortie.

Outils

Services AWS

- Amazon Athena est un service de requêtes interactif qui vous permet d'analyser les données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du langage SQL standard.
- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données. Ce modèle utilise un robot d'exploration AWS Glue et une table du catalogue de données AWS Glue.
- Amazon Kendra est un service de recherche intelligent qui utilise le traitement du langage naturel et des algorithmes d'apprentissage automatique avancés pour renvoyer des réponses spécifiques aux questions de recherche à partir de vos données.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub genai-bedrock-chatbotréférentiel.

Le référentiel de code contient les fichiers et dossiers suivants :

- `assets`dossier — Les actifs statiques, le schéma d'architecture et le jeu de données public
- `code/lambda-container`dossier — Le code Python exécuté dans la fonction Lambda
- `code/streamlit-app`dossier — Le code Python exécuté en tant qu'image de conteneur dans Amazon ECS
- `tests`dossier — Les fichiers Python exécutés pour tester unitaires les constructions du kit AWS CDK
- `code/code_stack.py`— Le CDK AWS construit des fichiers Python utilisés pour créer des ressources AWS
- `app.py`— Les fichiers Python de pile AWS CDK utilisés pour déployer les ressources AWS dans le compte AWS cible

- `requirements.txt`— La liste de toutes les dépendances Python qui doivent être installées pour AWS CDK
- `requirements-dev.txt`— La liste de toutes les dépendances Python qui doivent être installées pour qu'AWS CDK exécute la suite de tests unitaires
- `cdk.json`— Le fichier d'entrée fournissant les valeurs requises pour faire tourner les ressources

> **Note**
>
> Le code AWS CDK utilise des structures L3 (couche 3) et des politiques AWS Identity and Access Management (IAM) gérées par AWS pour déployer la solution.

Bonnes pratiques

- L'exemple de code fourni ici concerne uniquement une démonstration proof-of-concept (PoC) ou pilote. Si vous souhaitez transférer le code en mode de production, veillez à suivre les meilleures pratiques suivantes :
  - La journalisation des accès Amazon S3 est activée.
  - Les journaux de flux VPC sont activés.
  - L'index Amazon Kendra Enterprise Edition est activé.
- Configurez la surveillance et les alertes pour la fonction Lambda. Pour plus d'informations, consultez la section Surveillance et résolution des problèmes des fonctions Lambda. Pour connaître les meilleures pratiques générales relatives à l'utilisation des fonctions Lambda, consultez la documentation AWS.

Épopées

Configurez les informations d'identification AWS sur votre machine locale

Tâche	Description	Compétences requises
Exportez des variables pour le compte et la région AWS où la pile sera déployée.	Pour fournir des informations d'identification AWS pour AWS CDK à l'aide de variables	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	d'environnement, exécutez les commandes suivantes. `export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number> export CDK_DEFAU LT_REGION=<region>`	
Configurez le profil de la CLI AWS.	Pour configurer le profil de la CLI AWS pour le compte, suivez les instructions de la documentation AWS.	DevOps ingénieur, AWS DevOps

Configuration de votre environnement

Tâche	Description	Compétences requises
Clonez le dépôt sur votre machine locale.	Pour cloner le dépôt, exécutez la commande suivante dans votre terminal. `git clone https://g ithub.com/awslabs/ genai-bedrock-chat bot.git`	DevOps ingénieur, AWS DevOps
Configurez l'environnement virtuel Python et installez les dépendances requises.	Pour configurer l'environ nement virtuel Python, exécutez les commandes suivantes. `cd genai-bedrock-chat bot python3 -m venv .venv`	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises

	`source .venv/bin/activate`
	
	Pour configurer les dépendances requises, exécutez la commande suivante.
	
	`pip3 install -r requirements.txt`	

Configurez l'environnement AWS CDK et synthétisez le code AWS CDK.	1. Pour configurer l'environnement AWS CDK dans votre compte AWS, exécutez la commande suivante. `cdk bootstrap aws://ACCOUNT-NUMBER/REGION` 2. Pour convertir le code en configuration de CloudFormation pile AWS, exécutez la commande`cdk synth`.	DevOps ingénieur, AWS DevOps

Configuration et déploiement de l'application d'assistance basée sur le chat

Tâche	Description	Compétences requises
Fournir un accès au modèle Claude.	Pour activer l'accès au modèle Anthropic Claude pour votre compte AWS, suivez les instructions de la documentation Amazon Bedrock.	AWS DevOps

Tâche	Description	Compétences requises
Déployez des ressources dans le compte.	Pour déployer des ressources dans le compte AWS à l'aide du kit AWS CDK, procédez comme suit : 1. À la racine du référentiel cloné, dans le `cdk.json` fichier, entrez les `logging` paramètres. Les valeurs d'exemple sont `INFO`,`DEBUG`,`WARN`, et`ERROR`. Ces valeurs définissent les messages au niveau du journal pour la fonction Lambda et l'application Streamlit. 2. Le `app.py` fichier situé à la racine du référentiel cloné contient le nom de la CloudFormation pile AWS utilisée pour le déploiement. Le nom de la pile par défaut est`chatbot-stack` . 3. Pour déployer des ressources, exécutez la commande`cdk deploy`. La `cdk deploy` commande utilise des constructions L3 pour créer plusieurs fonctions Lambda permettant de copier des documents et des fichiers	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	de jeux de données CSV dans des compartiments S3. 4. Une fois la commande terminée, connectez-vous à la console de gestion AWS, ouvrez la CloudFormation console et vérifiez que la pile a été déployée avec succès. Une fois le déploiement réussi, vous pouvez accéder à l'application d'assistance basée sur le chat en utilisant l'URL fournie dans la section CloudFormation Sorties.	

Tâche	Description	Compétences requises
Exécutez le robot d'exploration AWS Glue et créez la table du catalogue de données.	Un robot d'exploration AWS Glue est utilisé pour maintenir le schéma de données dynamique. La solution crée et met à jour des partitions dans la table du catalogue de données AWS Glue en exécutant le robot d'exploration à la demande. Une fois les fichiers du jeu de données CSV copiés dans le compartiment S3, exécutez le robot d'exploration AWS Glue et créez le schéma de table du catalogue de données à des fins de test : 1. Accédez à la console AWS Glue. 2. Dans le volet de navigation, sous Catalogue de données, sélectionnez Crawlers. 3. Sélectionnez le crawler avec le suffixe `sagemaker-pricing-crawler` . 4. Lancez le crawler. 5. Une fois le robot d'exploration exécuté avec succès, il crée une table du catalogue de données AWS Glue.	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	Note Le code AWS CDK configure le robot d'exploration AWS Glue pour qu'il s'exécute à la demande, mais vous pouvez également le planifier pour qu'il s'exécute périodiquement.	

Tâche	Description	Compétences requises
Lancez l'indexation des documents.	Une fois les fichiers copiés dans le compartiment S3, utilisez Amazon Kendra pour les explorer et les indexer : 1. Accédez à la console Amazon Kendra. 2. Sélectionnez l'index avec le suffixe`chatbot-index` . 3. Dans le volet de navigation, choisissez Sources de données, puis sélectionnez le connecteur de source de données avec le suffixe`chatbot-index` . 4. Choisissez Synchroniser maintenant pour lancer le processus d'indexation. **Note** Le code AWS CDK configure la synchronisation de l'index Amazon Kendra pour qu'elle s'exécute à la demande, mais vous pouvez également l'exécuter périodiquement à l'aide du paramètre Schedule.	AWS DevOps, DevOps ingénieur

Nettoyez toutes les ressources AWS de la solution

Tâche	Description	Compétences requises
Supprimez les ressources AWS.	Après avoir testé la solution, nettoyez les ressources : 1. Pour supprimer les ressources AWS déployées par la solution, exécutez la commande`cdk destroy`. 2. Supprimez tous les objets des deux compartim ents S3, puis retirez les compartiments. Pour plus d'informations, consultez la section Suppression d'un bucket.	DevOps ingénieur, AWS DevOps

Résolution des problèmes

Problème	Solution
AWS CDK renvoie des erreurs.	Pour obtenir de l'aide concernant les problèmes liés au CDK AWS, consultez la section Résolution des problèmes courants liés au CDK AWS.

Ressources connexes

- Amazon Bedrock :
  - Accès aux modèles
  - Paramètres d'inférence pour les modèles de base
- Création de fonctions Lambda avec Python

- Commencez avec le kit AWS CDK
- Utilisation du kit de développement logiciel AWS en Python
- Générateur d'applications d'IA générative sur AWS
- LangChain documentation
- Documentation simplifiée

Informations supplémentaires

Commandes AWS CDK

Lorsque vous travaillez avec AWS CDK, gardez à l'esprit les commandes utiles suivantes :

- Répertorie toutes les piles de l'application

```
cdk ls
```

- Émet le modèle AWS synthétisé CloudFormation

```
cdk synth
```

- Déploie la pile sur votre compte AWS et votre région par défaut

```
cdk deploy
```

- Compare la pile déployée avec l'état actuel

```
cdk diff
```

- Ouvre la documentation du kit AWS CDK

```
cdk docs
```

- Supprime la CloudFormation pile et retire les ressources déployées par AWS

```
cdk destroy
```

Développez un assistant entièrement automatisé basé sur le chat en utilisant les agents et les bases de connaissances Amazon Bedrock

Créée par Jundong Qiao (AWS), Kara Yang (AWS), Kiowa Jackson (AWS), Noah Hamilton (AWS), Praveen Kumar Jeyarajan (AWS) et Shuai Cao (AWS)

Récapitulatif

De nombreuses entreprises sont confrontées à des défis lorsqu'elles créent un assistant basé sur le chat capable d'orchestrer diverses sources de données afin de proposer des réponses complètes. Ce modèle présente une solution pour développer un assistant basé sur le chat capable de répondre aux requêtes provenant à la fois de la documentation et des bases de données, avec un déploiement simple.

À commencer par Amazon Bedrock, ce service d'intelligence artificielle générative (IA) entièrement géré fournit un large éventail de modèles de base avancés (FMs). Cela facilite la création efficace d'applications d'IA génératives en mettant fortement l'accent sur la confidentialité et la sécurité. Dans le contexte de la récupération de documentation, la génération augmentée de récupération (RAG) est une fonctionnalité essentielle. Il utilise des bases de connaissances pour compléter les instructions FM avec des informations contextuelles pertinentes provenant de sources externes. Un index Amazon OpenSearch Serverless sert de base de données vectorielle à l'origine des bases de connaissances d'Amazon Bedrock. Cette intégration est améliorée grâce à une ingénierie rapide et minutieuse afin de minimiser les inexactitudes et de garantir que les réponses sont ancrées dans une documentation factuelle. Pour les requêtes de base FMs de données, Amazon Bedrock transforme les requêtes textuelles en requêtes SQL structurées, en incorporant des paramètres spécifiques. Cela permet de récupérer avec précision les données des bases de données gérées par les bases de données AWS Glue. Amazon Athena est utilisé pour ces requêtes.

Pour traiter des requêtes plus complexes, l'obtention de réponses complètes nécessite des informations provenant à la fois de la documentation et des bases de données. Agents for Amazon Bedrock est une fonctionnalité d'intelligence artificielle générative qui vous aide à créer des agents autonomes capables de comprendre des tâches complexes et de les décomposer en tâches plus simples à des fins d'orchestration. La combinaison des informations extraites des tâches simplifiées, facilitée par les agents autonomes d'Amazon Bedrock, améliore la synthèse des informations et permet d'obtenir des réponses plus complètes et exhaustives. Ce modèle montre comment créer

un assistant basé sur le chat en utilisant Amazon Bedrock et les services et fonctionnalités d'IA générative associés au sein d'une solution automatisée.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Docker, installé
- AWS Cloud Development Kit (AWS CDK), installé et démarré dans la ou `us-east-1` les régions AWS `us-west-2`
- AWS CDK Toolkit version 2.114.1 ou ultérieure, installé
- Interface de ligne de commande AWS (AWS CLI), installée et configurée
- Python version 3.11 ou ultérieure, installée
- Dans Amazon Bedrock, activez l'accès à Claude 2, Claude 2.1, Claude Instant et Titan Embeddings G1 — Text

Limites

- Cette solution est déployée sur un seul compte AWS.
- Cette solution ne peut être déployée que dans les régions AWS où Amazon Bedrock et Amazon OpenSearch Serverless sont pris en charge. Pour plus d'informations, consultez la documentation d'Amazon Bedrock et d'Amazon OpenSearch Serverless.

Versions du produit

- LLAMA-Index version 0.10.6 ou ultérieure
- Sqlalchemy version 2.0.23 ou ultérieure
- OpenSearch-PY version 2.4.2 ou ultérieure
- Requests_AWS4Auth version 1.2.3 ou ultérieure
- SDK AWS pour Python (Boto3), version 1.34.57 ou ultérieure

Architecture

Pile technologique cible

L'AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel open source permettant de définir l'infrastructure cloud dans le code et de la provisionner via AWS. CloudFormation La pile AWS CDK utilisée dans ce modèle déploie les ressources AWS suivantes :

- AWS Key Management Service (AWS KMS)
- Amazon Simple Storage Service (Amazon S3)
- Catalogue de données AWS Glue, pour le composant de base de données AWS Glue
- AWS Lambda
- AWS Identity and Access Management (IAM)
- Amazon OpenSearch sans serveur
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- AWS Fargate
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer

Architecture cible

Le schéma montre une configuration cloud native complète d'AWS au sein d'une seule région AWS, en utilisant plusieurs services AWS. L'interface principale de l'assistant basé sur le chat est une application Streamlit hébergée sur un cluster Amazon ECS. Un Application Load Balancer gère l'accessibilité. Les requêtes effectuées via cette interface activent la fonction `Invocation` Lambda, qui s'interface ensuite avec les agents d'Amazon Bedrock. Cet agent répond aux demandes des utilisateurs en consultant les bases de connaissances d'Amazon Bedrock ou en invoquant une fonction Lambda`Agent executor`. Cette fonction déclenche un ensemble d'actions associées à l'agent, selon un schéma d'API prédéfini. Les bases de connaissances d'Amazon Bedrock utilisent un index OpenSearch sans serveur comme base de données vectorielle. En outre, la `Agent executor` fonction génère des requêtes SQL qui sont exécutées sur la base de données AWS Glue via Amazon Athena.

Outils

Services AWS

- Amazon Athena est un service de requêtes interactif qui vous permet d'analyser les données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du langage SQL standard.
- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données. Ce modèle utilise un robot d'exploration AWS Glue et une table du catalogue de données AWS Glue.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon OpenSearch Serverless est une configuration sans serveur à la demande pour Amazon OpenSearch Service. Dans ce modèle, un index OpenSearch sans serveur sert de base de données vectorielle pour les bases de connaissances d'Amazon Bedrock.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Streamlit est un framework Python open source permettant de créer des applications de données.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub genai-bedrock-agent-chatbotréférentiel. Le référentiel de code contient les fichiers et dossiers suivants :

- `assets`dossier — Les actifs statiques, tels que le schéma d'architecture et le jeu de données public.
- `code/lambdas/action-lambda`dossier — Le code Python de la fonction Lambda qui agit comme une action pour l'agent Amazon Bedrock.
- `code/lambdas/create-index-lambda`dossier — Le code Python de la fonction Lambda qui crée l'index OpenSearch Serverless.
- `code/lambdas/invoke-lambda`dossier — Le code Python de la fonction Lambda qui appelle l'agent Amazon Bedrock, qui est appelé directement depuis l'application Streamlit.
- `code/lambdas/update-lambda`dossier — Le code Python de la fonction Lambda qui met à jour ou supprime les ressources une fois les ressources AWS déployées via le CDK AWS.
- `code/layers/boto3_layer`dossier — La pile AWS CDK qui crée une couche Boto3 partagée entre toutes les fonctions Lambda.
- `code/layers/opensearch_layer`dossier — La pile AWS CDK qui crée une couche OpenSearch sans serveur qui installe toutes les dépendances pour créer l'index.
- `code/streamlit-app`dossier — Le code Python qui est exécuté en tant qu'image de conteneur dans Amazon ECS
- `code/code_stack.py`— Le kit AWS CDK crée des fichiers Python qui créent des ressources AWS.
- `app.py`— Le kit AWS CDK empile des fichiers Python qui déploient les ressources AWS dans le compte AWS cible.
- `requirements.txt`— La liste de toutes les dépendances Python qui doivent être installées pour le CDK AWS.
- `cdk.json`— Le fichier d'entrée fournissant les valeurs requises pour créer des ressources. De plus, dans les `context/config` champs, vous pouvez personnaliser la solution en conséquence. Pour plus d'informations sur la personnalisation, consultez la section Informations supplémentaires.

Bonnes pratiques

- L'exemple de code fourni ici est uniquement destiné à proof-of-concept (PoC) ou à des fins pilotes. Si vous souhaitez mettre le code en production, veillez à suivre les meilleures pratiques suivantes :
  - Activer la journalisation des accès Amazon S3

  - Activer les journaux de flux VPC
- Configurez la surveillance et les alertes pour les fonctions Lambda. Pour plus d'informations, consultez la section Surveillance et résolution des problèmes des fonctions Lambda. Pour connaître les meilleures pratiques, consultez les meilleures pratiques d'utilisation des fonctions AWS Lambda.

Épopées

Configurez les informations d'identification AWS sur votre station de travail locale

Tâche	Description	Compétences requises

Exportez les variables du compte et de la région.	Pour fournir des informations d'identification AWS pour le CDK AWS à l'aide de variables d'environnement, exécutez les commandes suivantes.
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<Region>`
		AWS DevOps, DevOps ingénieur

Configurez le profil nommé de l'interface de ligne de commande AWS.	Pour configurer le profil nommé de l'interface de ligne de commande AWS pour le compte, suivez les instructions de la section Configuration et paramètres du fichier d'identification.	AWS DevOps, DevOps ingénieur

Configuration de votre environnement

Tâche	Description	Compétences requises
Clonez le dépôt sur votre poste de travail local.	Pour cloner le dépôt, exécutez la commande suivante dans votre terminal. `git clone https://github.com/awslabs/genai-bedrock-agent-chatbot.git`	DevOps ingénieur, AWS DevOps

Configurez l'environnement virtuel Python.	Pour configurer l'environnement virtuel Python, exécutez les commandes suivantes.
	`cd genai-bedrock-agent-chatbot`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Pour configurer les dépendances requises, exécutez la commande suivante.
	`pip3 install -r requirements.txt`
		DevOps ingénieur, AWS DevOps

Configurez l'environnement AWS CDK.	Pour convertir le code en CloudFormation modèle AWS, exécutez la commande`cdk synth`.	AWS DevOps, DevOps ingénieur

Configuration et déploiement de l'application

Tâche	Description	Compétences requises
Déployez des ressources dans le compte.	Pour déployer des ressources dans le compte AWS à l'aide du kit AWS CDK, procédez comme suit : 1. À la racine du référentiel cloné, dans le `cdk.json` fichier, entrez les paramètres de journalisation. Les valeurs d'exemple sont `INFO`,`DEBUG`,`WARN`, et`ERROR`. Ces valeurs définissent les messages au niveau du journal pour les fonctions Lambda et l'application Streamlit. 2. Le `cdk.json` fichier situé à la racine du référentiel cloné contient le nom de la CloudFormation pile AWS utilisée pour le déploiement. Le nom de la pile par défaut est`chatbot-stack` . Le nom de l'agent Amazon Bedrock par défaut est`ChatbotBedrockAgent` , et l'alias de l'agent Amazon Bedrock par défaut est. `Chatbot_Agent`	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	3. Pour déployer des ressources, exécutez la commande`cdk deploy`. La `cdk deploy` commande utilise des structures de couche 3 pour créer plusieurs fonctions Lambda permettant de copier des documents et des fichiers de jeux de données CSV dans des compartiments S3. Il déploie également l'agent Amazon Bedrock, les bases de connaissances et la fonction `Action group` Lambda pour l'agent Amazon Bedrock. 4. Connectez-vous à la console de gestion AWS, puis ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation/. 5. Vérifiez que la pile a été déployée avec succès. Pour obtenir des instructions, consultez la section Révision de votre stack sur la CloudFormation console AWS.	

Tâche	Description	Compétences requises
	Une fois le déploiement réussi, vous pouvez accéder à l'application d'assistance basée sur le chat en utilisant l'URL fournie dans l'onglet Sorties de la CloudFormation console.	

Nettoyez toutes les ressources AWS de la solution

Tâche	Description	Compétences requises
Supprimez les ressources AWS.	Après avoir testé la solution, exécutez la commande pour nettoyer les ressources`cdk destroy`.	AWS DevOps, DevOps ingénieur

Ressources connexes

Documentation AWS

- Ressources Amazon Bedrock :
  - Accès aux modèles
  - Paramètres d'inférence pour les modèles de base
  - Agents pour Amazon Bedrock
  - Bases de connaissances pour Amazon Bedrock
- Création de fonctions Lambda avec Python
- Ressources du kit AWS CDK :
  - Commencez avec le kit AWS CDK
  - Résolution des problèmes courants liés au kit AWS CDK
  - Utilisation du kit de développement logiciel AWS en Python
- Générateur d'applications d'IA générative sur AWS

Autres ressources AWS

- Moteur vectoriel pour Amazon OpenSearch Serverless

Autres ressources

- LlamaIndex documentation
- Documentation simplifiée

Informations supplémentaires

Personnalisez l'assistant basé sur le chat avec vos propres données

Pour intégrer vos données personnalisées dans le cadre du déploiement de la solution, suivez ces directives structurées. Ces étapes sont conçues pour garantir un processus d'intégration fluide et efficace, vous permettant de déployer efficacement la solution avec vos données personnalisées.

Pour l'intégration des données de la base de connaissances

Préparation des données

1. Localisez le `assets/knowledgebase_data_source/` répertoire.
2. Placez votre ensemble de données dans ce dossier.

Ajustements de configuration

1. Ouvrez le fichier `cdk.json`.
2. Accédez au `context/configure/paths/knowledgebase_file_name` champ, puis mettez-le à jour en conséquence.
3. Accédez au `bedrock_instructions/knowledgebase_instruction` champ, puis mettez-le à jour pour refléter avec précision les nuances et le contexte de votre nouveau jeu de données.

Pour l'intégration des données structurelles

Organisation des données

1. Dans le `assets/data_query_data_source/` répertoire, créez un sous-répertoire, tel `quetabular_data`.

2. Placez votre jeu de données structuré (les formats acceptables incluent CSV, JSON, ORC et Parquet) dans ce sous-dossier nouvellement créé.
3. Si vous vous connectez à une base de données existante, mettez à jour la fonction `code/lambda/action-lambda/build_query_engine.py` pour vous connecter `create_sql_engine()` à votre base de données.

Mises à jour de configuration et de code

1. Dans le `cdk.json` fichier, mettez à jour le `context/configure/paths/athena_table_data_prefix` champ pour l'aligner sur le nouveau chemin de données.
2. Révisez `code/lambda/action-lambda/dynamic_examples.csv` en incorporant de nouveaux text-to-SQL exemples correspondant à votre ensemble de données.
3. Révisez `code/lambda/action-lambda/prompt_templates.py` pour refléter les attributs de votre jeu de données structuré.
4. Dans le `cdk.json` fichier, mettez à jour le `context/configure/bedrock_instructions/action_group_description` champ pour expliquer le but et les fonctionnalités de la fonction `Action group` Lambda.
5. Dans le `assets/agent_api_schema/artifacts_schema.json` fichier, expliquez les nouvelles fonctionnalités de votre fonction `Action group` Lambda.

Mise à jour générale

Dans le `cdk.json` fichier, dans la `context/configure/bedrock_instructions/agent_instruction` section, fournissez une description complète des fonctionnalités et de l'objectif de conception prévus de l'agent Amazon Bedrock, en tenant compte des données récemment intégrées.

Documentez les connaissances institutionnelles à partir de saisies vocales à l'aide d'Amazon Bedrock et Amazon Transcribe

Créée par Praveen Kumar Jeyarajan (AWS), Jundong Qiao (AWS), Megan Wu (AWS) et Rajiv Upadhyay (AWS)

Récapitulatif

La saisie des connaissances institutionnelles est essentielle pour garantir le succès et la résilience de l'organisation. Le savoir institutionnel représente la sagesse collective, les connaissances et les expériences accumulées par les employés au fil du temps, souvent tacites et transmises de manière informelle. Cette mine d'informations englobe des approches uniques, des meilleures pratiques et des solutions à des problèmes complexes qui pourraient ne pas être documentés ailleurs. En formalisant et en documentant ces connaissances, les entreprises peuvent préserver la mémoire institutionnelle, favoriser l'innovation, améliorer les processus décisionnels et accélérer les cycles d'apprentissage des nouveaux employés. De plus, il favorise la collaboration, responsabilise les individus et cultive une culture d'amélioration continue. En fin de compte, l'exploitation des connaissances institutionnelles aide les entreprises à utiliser leur atout le plus précieux, à savoir l'intelligence collective de leur personnel, pour relever les défis, stimuler la croissance et conserver un avantage concurrentiel dans des environnements commerciaux dynamiques.

Ce modèle explique comment saisir les connaissances institutionnelles par le biais d'enregistrements vocaux d'employés supérieurs. Il utilise Amazon Transcribe et Amazon Bedrock pour une documentation et une vérification systématiques. En documentant ces connaissances informelles, vous pouvez les conserver et les partager avec les cohortes d'employés suivantes. Cette initiative soutient l'excellence opérationnelle et améliore l'efficacité des programmes de formation grâce à l'incorporation de connaissances pratiques acquises grâce à l'expérience directe.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Docker, installé
- AWS Cloud Development Kit (AWS CDK) version 2.114.1 ou ultérieure, installé et démarré dans la ou les régions AWS `us-east-1` `us-west-2`
- AWS CDK Toolkit version 2.114.1 ou ultérieure, installé

- Interface de ligne de commande AWS (AWS CLI), installée et configurée
- Python version 3.12 ou ultérieure, installée
- Autorisations pour créer des ressources Amazon Transcribe, Amazon Bedrock, Amazon Simple Storage Service (Amazon S3) et AWS Lambda

Limites

- Cette solution est déployée sur un seul compte AWS.
- Cette solution ne peut être déployée que dans les régions AWS où Amazon Bedrock et Amazon Transcribe sont disponibles. Pour plus d'informations sur la disponibilité, consultez la documentation d'Amazon Bedrock et d'Amazon Transcribe.
- Les fichiers audio doivent être dans un format pris en charge par Amazon Transcribe. Pour obtenir la liste des formats pris en charge, consultez la section Formats multimédia de la documentation Transcribe.

Versions du produit

- SDK AWS pour Python (Boto3), version 1.34.57 ou ultérieure
- LangChain version 0.1.12 ou ultérieure

Architecture

L'architecture représente un flux de travail sans serveur sur AWS. AWS Step Functions orchestre les fonctions Lambda pour le traitement audio, l'analyse de texte et la génération de documents. Le schéma suivant montre le flux de travail Step Functions, également connu sous le nom de machine à états.

Chaque étape de la machine à états est gérée par une fonction Lambda distincte. Les étapes du processus de génération de documents sont les suivantes :

1. La fonction `preprocess` Lambda valide l'entrée transmise à Step Functions et répertorie tous les fichiers audio présents dans le chemin du dossier d'URI Amazon S3 fourni. Les fonctions Lambda en aval du flux de travail utilisent la liste de fichiers pour valider, résumer et générer le document.
2. La fonction `transcribe` Lambda utilise Amazon Transcribe pour convertir les fichiers audio en transcriptions de texte. Cette fonction Lambda est chargée de lancer le processus de transcription

et de transformer avec précision la parole en texte, qui est ensuite stocké pour un traitement ultérieur.

3. La fonction `validate` Lambda analyse les transcriptions de texte afin de déterminer la pertinence des réponses aux questions initiales. En utilisant un modèle linguistique étendu (LLM) via Amazon Bedrock, il identifie et sépare les réponses sur le sujet des réponses hors sujet.
4. La fonction `summarize` Lambda utilise Amazon Bedrock pour générer un résumé cohérent et concis des réponses sur le sujet.
5. La fonction `generate` Lambda assemble les résumés dans un document bien structuré. Il peut formater le document selon des modèles prédéfinis et inclure tout contenu ou donnée supplémentaire nécessaire.
6. Si l'une des fonctions Lambda échoue, vous recevez une notification par e-mail via Amazon Simple Notification Service (Amazon SNS).

Tout au long de ce processus, AWS Step Functions s'assure que chaque fonction Lambda est lancée dans le bon ordre. Cette machine à états a la capacité de traiter en parallèle afin d'améliorer l'efficacité. Un compartiment Amazon S3 fait office de référentiel de stockage central et soutient le flux de travail en gérant les différents formats de supports et de documents concernés.

Outils

Services AWS

- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise.

- Amazon Transcribe est un service de reconnaissance vocale automatique qui utilise des modèles d'apprentissage automatique pour convertir le son en texte.

Autres outils

- LangChainest un framework pour développer des applications basées sur de grands modèles de langage (LLMs).

Référentiel de code

Le code de ce modèle est disponible dans le GitHub genai-knowledge-captureréférentiel.

Le référentiel de code contient les fichiers et dossiers suivants :

- `assets`dossier — Les actifs statiques de la solution, tels que le schéma d'architecture et le jeu de données public
- `code/lambdas`dossier — Le code Python pour toutes les fonctions Lambda
  - `code/lambdas/generate`folder - Le code Python qui génère un document à partir des données résumées dans le compartiment S3
  - `code/lambdas/preprocess`dossier - Le code Python qui traite les entrées pour la machine à états Step Functions
  - `code/lambdas/summarize`dossier - Le code Python qui résume les données transcrites à l'aide du service Amazon Bedrock
  - `code/lambdas/transcribe`dossier - Le code Python qui convertit les données vocales (fichier audio) en texte à l'aide d'Amazon Transcribe
  - `code/lambdas/validate`folder - Le code Python qui valide si toutes les réponses concernent le même sujet
- `code/code_stack.py`— Le fichier Python de construction AWS CDK utilisé pour créer des ressources AWS
- `app.py`— Le fichier Python de l'application AWS CDK utilisé pour déployer les ressources AWS dans le compte AWS cible
- `requirements.txt`— La liste de toutes les dépendances Python qui doivent être installées pour le AWS CDK
- `cdk.json`— Le fichier d'entrée fournissant les valeurs requises pour créer des ressources

Bonnes pratiques

L'exemple de code fourni est uniquement destiné à proof-of-concept (PoC) ou à des fins pilotes. Si vous souhaitez appliquer la solution à la production, appliquez les meilleures pratiques suivantes :

- Activer la journalisation des accès Amazon S3
- Activer les journaux de flux VPC

Épopées

Configurer les informations d'identification AWS sur votre station de travail locale

Tâche	Description	Compétences requises

Exportez des variables pour le compte et la région AWS.	Pour fournir des informations d'identification AWS pour le CDK AWS à l'aide de variables d'environnement, exécutez les commandes suivantes.
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<Region>`
		AWS DevOps, DevOps ingénieur

Configurez le profil nommé de la CLI AWS.	Pour configurer le profil nommé de l'interface de ligne de commande AWS pour le compte, suivez les instructions de la section Configuration et paramètres du fichier d'identification.	AWS DevOps, DevOps ingénieur

Configuration de votre environnement

Tâche	Description	Compétences requises
Clonez le dépôt sur votre poste de travail local.	Pour cloner le genai-knowledge-capturedépôt, exécutez la commande suivante dans votre terminal. `git clone https://github.com/aws-samples/genai-knowledge-capture`	AWS DevOps, DevOps ingénieur
(Facultatif) Remplacez les fichiers audio.	Pour personnaliser l'exemple d'application afin d'intégrer vos propres données, procédez comme suit : 1. Accédez au `assets/audio_samples` dossier dans le référentiel cloné. 2. Supprimez les dossiers contenant les exemples de fichiers audio. 3. Créez un dossier pour chaque sujet que vous souhaitez analyser. 4. Transférez vos fichiers audio dans leurs dossiers respectifs.	AWS DevOps, DevOps ingénieur
Configurez l'environnement virtuel Python.	Pour configurer l'environnement virtuel Python, exécutez les commandes suivantes.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	`cd genai-knowledge-capture`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`	

Synthétisez le code AWS CDK.	Pour convertir le code en configuration de CloudFormation pile AWS, exécutez la commande suivante. `cdk synth`	AWS DevOps, DevOps ingénieur

Configuration et déploiement de la solution

Tâche	Description	Compétences requises
Provisionnez l'accès au modèle de base.	Activez l'accès au modèle Anthropic Claude 3 Sonnet pour votre compte AWS. Pour obtenir des instructions, voir Ajouter un accès au modèle dans la documentation de Bedrock.	AWS DevOps
Déployez des ressources dans le compte.	Pour déployer des ressources dans le compte AWS à l'aide du kit AWS CDK, procédez comme suit : 1. (Facultatif) À la racine du référentiel cloné, dans le `app.py` fichier,	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	mettez à jour le nom de la CloudFormation pile AWS. Le nom de la pile par défaut est`genai-knowledge-capture-stack` . 2. Pour déployer des ressources, exécutez la commande`cdk deploy`. La `cdk deploy` commande utilise des structures de couche 3 pour créer un ensemble de fonctions Lambda, un compartiment S3, une rubrique Amazon SNS et une machine d'état Step Functions. Les fichiers audio du `assets/audio_samples` dossier sont copiés dans le compartiment S3 lors du déploiement. 3. Connectez-vous à la console de gestion AWS, puis ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation/. 4. Vérifiez que la pile a été déployée avec succès. Pour obtenir des instructions, consultez la section	

Tâche	Description	Compétences requises
	Révision de votre stack sur la CloudFormation console AWS.	
Abonnez-vous à la rubrique Amazon SNS.	Pour vous abonner à la rubrique Amazon SNS pour recevoir des notifications, procédez comme suit : 1. Dans le volet de navigation de la CloudFormation console, sélectionnez Stacks. 2. Choisissez la `genai-knowledge-capture-stack` pile. 3. Choisissez l'onglet Outputs. 4. Trouvez le nom de la rubrique Amazon SNS avec la clé. `SNSTopicName` 5. Configurez une adresse e-mail pour recevoir des notifications en suivant les instructions de la section Abonner une adresse e-mail à une rubrique Amazon SNS.	AWS général

Tester la solution

Tâche	Description	Compétences requises
Lancez la machine d'état.	1. Ouvrez la console Step Functions.	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	2. Sur la page State machines, choisissez genai-knowledge-capture-stack-state-machine. 3. Choisissez Start execution (Démarrer l'exécution). 4. (Facultatif) Dans le champ Nom, entrez le nom de l'exécution. 5. Dans la zone de saisie, entrez l'objet JSON suivant en remplaçant le texte de l'espace réservé, où : • <Name>est le nom que vous souhaitez donner au document. • <S3 bucket name>est le nom du compartiment Amazon S3 qui contient les fichiers audio. • <Folder path>est le répertoire qui contient les fichiers audio. `{ "documentName": "<Name>", "audioFileFolderUri": "s3://<S3 bucket name>/<Folder path>" }` 6. Choisissez Démarrer une exécution.	

Tâche	Description	Compétences requises
	7. Sur la page des détails de l'exécution, passez en revue les résultats et attendez que l'exécution soit terminée.	

Nettoyez toutes les ressources AWS de la solution

Tâche	Description	Compétences requises
Supprimez les ressources AWS.	Après avoir testé la solution, nettoyez les ressources : 1. Supprimez tous les objets du compartiment S3, puis supprimez le compartiment. Pour plus d'informations, consultez la section Suppression d'un bucket. 2. À partir du référentiel cloné, exécutez la commande `cdk destroy`.	AWS DevOps, DevOps ingénieur

Ressources connexes

Documentation AWS

- Ressources Amazon Bedrock :
  - Accès aux modèles
  - Paramètres d'inférence pour les modèles de base
- Ressources AWS CDK :
  - Commencez avec le kit AWS CDK
  - Utilisation du kit AWS CDK en Python

  - Résolution des problèmes courants liés au kit AWS CDK
  - commandes du kit d'outils
- Ressources AWS Step Functions :
  - Commencer à utiliser AWS Step Functions
  - Dépannage
- Création de fonctions Lambda avec Python
- Générateur d'applications d'IA générative sur AWS

Autres ressources

- LangChain documentation

Générez des recommandations personnalisées et reclassées à l'aide d'Amazon Personalize

Créée par Mason Cahill (AWS), Matthew Chasse (AWS) et Tayo Olajide (AWS)

Récapitulatif

Ce modèle vous montre comment utiliser Amazon Personalize pour générer des recommandations personnalisées, y compris des recommandations reclassées, pour vos utilisateurs sur la base de l'ingestion de données d'interaction utilisateur en temps réel provenant de ces utilisateurs. L'exemple de scénario utilisé dans ce modèle est basé sur un site Web d'adoption d'animaux de compagnie qui génère des recommandations pour ses utilisateurs en fonction de leurs interactions (par exemple, les animaux qu'un utilisateur visite). En suivant cet exemple de scénario, vous apprendrez à utiliser Amazon Kinesis Data Streams pour ingérer les données d'interaction, AWS Lambda pour générer des recommandations et les reclasser, et Amazon Data Firehose pour stocker les données dans un compartiment Amazon Simple Storage Service (Amazon S3). Vous apprendrez également à utiliser AWS Step Functions pour créer une machine à états qui gère la version de la solution (c'est-à-dire un modèle entraîné) qui génère vos recommandations.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec un kit de développement cloud AWS (AWS CDK) amorcé
- Interface de ligne de commande AWS (AWS CLI) avec informations d'identification configurées
- Python 3.9

Versions du produit

- Python 3.9
- AWS CDK 2.23.0 ou version ultérieure
- AWS CLI 2.7.27 ou version ultérieure

Architecture

Pile technologique

- Amazon Data Firehose
- Amazon Kinesis Data Streams
- Amazon Personalize
- Amazon Simple Storage Service (Amazon S3)
- Kit de développement cloud AWS (AWS CDK)
- Interface de ligne de commande AWS (AWS CLI)
- AWS Lambda
- AWS Step Functions

Architecture cible

Le schéma suivant illustre un pipeline permettant d'ingérer des données en temps réel dans Amazon Personalize. Le pipeline utilise ensuite ces données pour générer des recommandations personnalisées et reclassées pour les utilisateurs.

Le schéma suivant illustre le flux de travail suivant :

1. Kinesis Data Streams ingère des données utilisateur en temps réel (par exemple, des événements tels que la visite d'animaux de compagnie) pour les traiter par Lambda et Firehose.
2. Une fonction Lambda traite les enregistrements de Kinesis Data Streams et lance un appel d'API pour ajouter l'interaction utilisateur contenue dans l'enregistrement à un outil de suivi des événements dans Amazon Personalize.
3. Une règle basée sur le temps invoque une machine d'état Step Functions et génère de nouvelles versions de solutions pour les modèles de recommandation et de reclassement en utilisant les événements du suivi des événements d'Amazon Personalize.
4. Les campagnes Amazon Personalize sont mises à jour par le State Machine pour utiliser la nouvelle version de la solution.
5. Lambda reclasse la liste des articles recommandés en lançant la campagne de reclassement Amazon Personalize.
6. Lambda récupère la liste des articles recommandés en appelant la campagne de recommandations Amazon Personalize.
7. Firehose enregistre les événements dans un compartiment S3 où ils sont accessibles sous forme de données historiques.

Outils

Outils AWS

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon Data Firehose vous aide à fournir des données de streaming en temps réel à d'autres services AWS, à des points de terminaison HTTP personnalisés et à des points de terminaison HTTP détenus par des fournisseurs de services tiers pris en charge.
- Amazon Kinesis Data Streams vous aide à collecter et à traiter de grands flux d'enregistrements de données en temps réel.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Personalize est un service d'apprentissage automatique (ML) entièrement géré qui vous aide à générer des recommandations d'articles pour vos utilisateurs en fonction de vos données.
- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise.

Autres outils

- pytest est un framework Python pour écrire de petits tests lisibles.
- Python est un langage de programmation informatique polyvalent.

Code

Le code de ce modèle est disponible dans le référentiel GitHub Animal Recommender. Vous pouvez utiliser le CloudFormation modèle AWS de ce référentiel pour déployer les ressources de l'exemple de solution.

> **Note**
>
> Les versions de la solution Amazon Personalize, le suivi des événements et les campagnes sont soutenus par des ressources personnalisées (au sein de l'infrastructure) qui s'appuient sur CloudFormation des ressources natives.

Épopées

Création de l'infrastructure

Tâche	Description	Compétences requises
Créez un environnement Python isolé.	Configuration Mac/Linux 1. Pour créer manuellement un environnement virtuel, exécutez la `$ python3 -m venv .venv` commande depuis votre terminal. 2. Une fois le processus d'initialisation terminé, exécutez la `$ source .venv/bin/activate` commande pour activer l'environnement virtuel. Configuration de Windows Pour créer manuellement un environnement virtuel, exécutez la `% .venv\Scripts\activate.bat` commande depuis votre terminal.	DevOps ingénieur

Tâche	Description	Compétences requises
Synthétisez le CloudFormation modèle.	1. Pour installer les dépendances requises, exécutez la `$ pip install -r requirements.txt` commande depuis votre terminal. 2. Dans l'AWS CLI, définissez les variables d'environnement suivantes : • `export ACCOUNT_ID=123456789` • `export CDK_DEPLOY_REGION=us-east-1` • `export CDK_ENVIRONMENT=dev` 3. Dans le `config/{env}.yml` fichier, mettez-le à jour `vpcId` pour qu'il corresponde à votre ID de cloud privé virtuel (VPC). 4. Pour synthétiser le CloudFormation modèle de ce code, exécutez la `$ cdk synth` commande. **Note** À l'étape 2, `CDK_ENVIRONMENT` fait référence au	DevOps ingénieur

Tâche	Description	Compétences requises
	`config/{env}.yml` fichier.	
Déployez des ressources et créez une infrastructure.	Pour déployer les ressources de la solution, exécutez la `./deploy.sh` commande depuis votre terminal. Cette commande installe les dépendances Python requises. Un script Python crée un compartiment S3 et une clé AWS Key Management Service (AWS KMS), puis ajoute les données de départ pour les créations de modèles initiales. Enfin, le script s'exécute `cdk deploy` pour créer l'infrastructure restante. **Note** L'entraînement initial du modèle a lieu lors de la création de la pile. La création de la pile peut prendre jusqu'à deux heures.	DevOps ingénieur

Ressources connexes

- Recommandeur pour animaux () GitHub
- Documentation de référence AWS CDK

- Documentation Boto3
- Optimisez les recommandations personnalisées pour un indicateur commercial de votre choix avec Amazon Personalize (AWS Machine Learning Blog)

Informations supplémentaires

Exemples de charges utiles et de réponses

Fonction Lambda de recommandation

Pour récupérer des recommandations, soumettez une demande à la fonction Lambda de recommandation avec une charge utile au format suivant :

```
{
  "userId": "3578196281679609099",
  "limit": 6
}
```

L'exemple de réponse suivant contient une liste de groupes d'animaux :

```
[{"id": "1-domestic short hair-1-1"},
{"id": "1-domestic short hair-3-3"},
{"id": "1-domestic short hair-3-2"},
{"id": "1-domestic short hair-1-2"},
{"id": "1-domestic short hair-3-1"},
{"id": "2-beagle-3-3"},
```

Si vous omettez ce `userId` champ, la fonction renvoie des recommandations générales.

Re-classement de la fonction Lambda

Pour utiliser le reclassement, soumettez une demande à la fonction Lambda de reclassement. La charge utile contient tous `userId` les éléments IDs à reclasser et leurs métadonnées. Les exemples de données suivants utilisent les classes Oxford Pets pour `animal_species_id` (1=cat, 2=dog) et des nombres entiers de 1 à 5 pour et : `animal_age_id` `animal_size_id`

```
{
   "userId":"12345",
   "itemMetadataList":[
      {
```

```
         "itemId":"1",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      },
      {
         "itemId":"2",
         "animalMetadata":{
            "animal_species_id":"1",
            "animal_primary_breed_id":"Egyptian_Mau",
            "animal_size_id":"1",
            "animal_age_id":"1"
         }
      },
      {
         "itemId":"3",
         "animalMetadata":{
            "animal_species_id":"2",
            "animal_primary_breed_id":"Saint_Bernard",
            "animal_size_id":"3",
            "animal_age_id":"2"
         }
      }
   ]
}
```

La fonction Lambda reclasse ces articles, puis renvoie une liste ordonnée qui inclut l'article IDs et la réponse directe d'Amazon Personalize. Il s'agit d'une liste classée des groupes d'animaux auxquels appartiennent les objets et de leur score. Amazon Personalize utilise des recettes de personnalisation utilisateur et de classement personnalisé pour inclure un score pour chaque article dans les recommandations. Ces scores représentent la certitude relative dont dispose Amazon Personalize quant au prochain article que l'utilisateur choisira. Des scores plus élevés représentent une plus grande certitude.

```
{
   "ranking":[
      "1",
      "3",
      "2"
```

```
   ],
   "personalizeResponse":{
      "ResponseMetadata":{
         "RequestId":"a2ec0417-9dcd-4986-8341-a3b3d26cd694",
         "HTTPStatusCode":200,
         "HTTPHeaders":{
            "date":"Thu, 16 Jun 2022 22:23:33 GMT",
            "content-type":"application/json",
            "content-length":"243",
            "connection":"keep-alive",
            "x-amzn-requestid":"a2ec0417-9dcd-4986-8341-a3b3d26cd694"
         },
         "RetryAttempts":0
      },
      "personalizedRanking":[
         {
            "itemId":"2-Saint_Bernard-3-2",
            "score":0.8947961
         },
         {
            "itemId":"1-Siamese-1-1",
            "score":0.105204
         }
      ],
      "recommendationId":"RID-d97c7a87-bd4e-47b5-a89b-ac1d19386aec"
   }
}
```

Charge utile Amazon Kinesis

La charge utile à envoyer à Amazon Kinesis est au format suivant :

```
{
    "Partitionkey": "randomstring",
    "Data": {
        "userId": "12345",
        "sessionId": "sessionId4545454",
        "eventType": "DetailView",
        "animalMetadata": {
            "animal_species_id": "1",
            "animal_primary_breed_id": "Russian_Blue",
            "animal_size_id": "1",
            "animal_age_id": "2"
        },
```

```
        "animal_id": "98765"

    }
}
```

> **Note**
>
> Le `userId` champ est supprimé pour un utilisateur non authentifié.

Rationalisez les flux de travail d'apprentissage automatique, du développement local aux expériences évolutives en utilisant l' SageMaker IA et Hydra

Créée par David Sauerwein (AWS), Julian Ferdinand Grueber (AWS) et Marco Geiger (AWS)

Récapitulatif

Ce modèle fournit une approche unifiée pour configurer et exécuter des algorithmes d'apprentissage automatique (ML), des tests locaux à la production sur Amazon SageMaker AI. Les algorithmes ML sont au centre de ce modèle, mais son approche s'étend à l'ingénierie des fonctionnalités, à l'inférence et aux pipelines ML complets. Ce modèle illustre la transition entre le développement de scripts locaux et les tâches de formation à l' SageMaker IA à travers un exemple de cas d'utilisation.

Un flux de travail ML typique consiste à développer et tester des solutions sur une machine locale, à exécuter des expériences à grande échelle (par exemple, avec différents paramètres) dans le cloud et à déployer la solution approuvée dans le cloud. Ensuite, la solution déployée doit être surveillée et maintenue. Sans approche unifiée de ce flux de travail, les développeurs doivent souvent refactoriser leur code à chaque étape. Si la solution dépend d'un grand nombre de paramètres susceptibles de changer à n'importe quel stade de ce flux de travail, il peut devenir de plus en plus difficile de rester organisé et cohérent.

Ce modèle répond à ces défis. Tout d'abord, il élimine le besoin de refactoriser le code entre les environnements en fournissant un flux de travail unifié qui reste cohérent, qu'il s'exécute sur des machines locales, dans des conteneurs ou sur SageMaker l'IA. Ensuite, il simplifie la gestion des paramètres grâce au système de configuration d'Hydra, où les paramètres sont définis dans des fichiers de configuration distincts qui peuvent être facilement modifiés et combinés, avec enregistrement automatique de la configuration de chaque exécution. Pour plus de détails sur la manière dont ce modèle permet de relever ces défis, voir Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un rôle d'utilisateur AWS Identity and Access Management (IAM) pour le déploiement et le démarrage des tâches de formation à l' SageMaker IA
- AWS Command Line Interface (AWS CLI) version 2.0 ou ultérieure installée et configurée

- Poetry version 1.8 ou ultérieure, mais antérieure à 2.0, installée
- Docker installé
- Version 3.10.x de Python

Limites

- Le code cible actuellement uniquement les postes de formation SageMaker liés à l'IA. Il est simple de l'étendre aux tâches de traitement et à l'ensemble des pipelines d' SageMaker IA.
- Pour une configuration d' SageMaker IA entièrement productive, des détails supplémentaires doivent être mis en place. Il peut s'agir de clés custom AWS Key Management Service (AWS KMS) pour le calcul et le stockage, ou de configurations réseau. Vous pouvez également configurer ces options supplémentaires en utilisant Hydra dans un sous-dossier dédié du `config` dossier.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant décrit l'architecture de la solution.

Le schéma suivant illustre le flux de travail suivant :

1. Le data scientist peut itérer l'algorithme à petite échelle dans un environnement local, ajuster les paramètres et tester rapidement le script d'apprentissage sans avoir besoin de Docker ou SageMaker d'IA. (Pour plus de détails, consultez la tâche « Exécuter localement pour des tests rapides » dans Epics.)
2. Une fois satisfait de l'algorithme, le data scientist crée et envoie l'image Docker vers le référentiel Amazon Elastic Container Registry (Amazon ECR) nommé. `hydra-sm-artifact` (Pour plus de détails, consultez « Exécuter des flux de travail sur l' SageMaker IA » dans Epics.)
3. Le data scientist lance des tâches d'entraînement basées sur l' SageMaker IA ou des tâches d'optimisation des hyperparamètres (HPO) à l'aide de scripts Python. Pour les tâches de formation régulières, la configuration ajustée est écrite dans le bucket Amazon Simple Storage Service (Amazon S3) nommé. `hydra-sample-config` Pour les tâches HPO, le jeu de configuration par défaut situé dans le `config` dossier est appliqué.

4. La tâche de formation basée sur l' SageMaker IA extrait l'image Docker, lit les données d'entrée depuis le compartiment `hydra-sample-data` Amazon S3 et récupère la configuration depuis le compartiment Amazon S3 `hydra-sample-config` ou utilise la configuration par défaut. Après l'entraînement, la tâche enregistre les données de sortie dans le compartiment Amazon S3`hydra-sample-data`.

Automatisation et mise à l'échelle

- Pour une formation, un recyclage ou une inférence automatisés, vous pouvez intégrer le AWS CLI code à des services tels que AWS LambdaAWS CodePipeline, ou Amazon. EventBridge
- La mise à l'échelle peut être réalisée en modifiant les configurations relatives à la taille des instances ou en ajoutant des configurations pour la formation distribuée.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande. Pour ce modèle, le AWS CLI est utile à la fois pour la configuration initiale des ressources et pour les tests.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon SageMaker AI est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production. SageMaker AI Training est un service de ML entièrement géré au sein de l' SageMaker IA qui permet la formation de modèles de ML à grande échelle. L'outil peut gérer efficacement les exigences informatiques des modèles de formation, en utilisant l'évolutivité intégrée et l'intégration avec d'autres modèles. Services AWS SageMaker AI Training prend également en charge des algorithmes et des conteneurs personnalisés, ce qui le rend flexible pour un large éventail de flux de travail ML.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Docker est un ensemble de produits PaaS (plate-forme en tant que service) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs. Il a été utilisé dans ce modèle pour garantir des environnements cohérents à différentes étapes, du développement au déploiement, ainsi que pour garantir la fiabilité des dépendances et du code. La conteneurisation de Docker a facilité le dimensionnement et le contrôle des versions dans l'ensemble du flux de travail.
- Hydra est un outil de gestion de configuration qui offre la flexibilité nécessaire pour gérer plusieurs configurations et une gestion dynamique des ressources. Il joue un rôle essentiel dans la gestion des configurations d'environnement, permettant un déploiement fluide dans différents environnements. Pour plus de détails sur Hydra, voir Informations supplémentaires.
- Python est un langage de programmation informatique polyvalent. Python a été utilisé pour écrire le code ML et le flux de travail de déploiement.
- Poetry est un outil de gestion des dépendances et d'empaquetage en Python.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub configuring-sagemaker-training-jobs-with-hydra.

Bonnes pratiques

- Choisissez un rôle IAM pour le déploiement et le démarrage des tâches de formation à l' SageMaker IA qui respecte le principe du moindre privilège et accorde les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.
- Utilisez des informations d'identification temporaires pour accéder au rôle IAM dans le terminal.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Créez et activez l'environnement virtuel.	Pour créer et activer l'environnement virtuel, exécutez les	AWS général

Tâche	Description	Compétences requises

	commandes suivantes à la racine du référentiel :
	`poetry install`
	`poetry shell`	

Déployez l'infrastructure.	Pour déployer l'infrastructure à l'aide de CloudFormation, exécutez la commande suivante : `aws cloudformation deploy --template-file infra/hydra-sagemaker-setup.yaml --stack-name hydra-sagemaker-setup --capabilities CAPABILITY_NAMED_IAM`	AWS général, DevOps ingénieur
Téléchargez les exemples de données.	Pour télécharger les données d'entrée d'openml sur votre machine locale, exécutez la commande suivante : `python scripts/download_data.py`	AWS général

Tâche	Description	Compétences requises
Exécutez localement pour des tests rapides.	Pour exécuter le code d'entraînement localement à des fins de test, exécutez la commande suivante : `python mypackage/train.py data.train_data_path=data/train.csv evaluation.base_dir_path=data` Les journaux de toutes les exécutions sont stockés par heure d'exécution dans un dossier appelé`outputs`. Pour plus d'informations, consultez la section « Sortie » du GitHub référentiel. Vous pouvez également effectuer plusieurs entraînements en parallèle, avec différents paramètres, en utilisant cette `--multirun` fonctionnalité. Pour plus de détails, consultez la documentation d'Hydra.	Spécialiste des données

Exécutez des flux de travail sur l' SageMaker IA

Tâche	Description	Compétences requises
Définissez les variables d'environnement.	Pour exécuter votre tâche sur l' SageMaker IA, définissez les variables d'environnement	AWS général

Tâche	Description	Compétences requises

	suivantes, en indiquant votre identifiant Région AWS et votre Compte AWS identifiant :
	
	`export ECR_REPO_NAME=hydra-sm-artifact`
	`export image_tag=latest`
	`export AWS_REGION="<your_aws_region>" # for instance, us-east-1`
	`export ACCOUNT_ID="<your_account_id>"`
	`export BUCKET_NAME_DATA=hydra-sample-data-$ACCOUNT_ID`
	`export BUCKET_NAME_CONFIG=hydra-sample-config-$ACCOUNT_ID`
	`export AWS_DEFAULT_REGION=$AWS_REGION`
	`export ROLE_ARN=arn:aws:iam::${ACCOUNT_ID}:role/hydra-sample-sagemaker`
	`export INPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/input/`
	`export OUTPUT_DATA_S3_PATH=s3://$BUCKET_NAME_DATA/hydra-on-sm/output/`	

Tâche	Description	Compétences requises

Créez et publiez une image Docker.	Pour créer l'image Docker et la transférer vers le référentiel Amazon ECR, exécutez la commande suivante :
	`chmod +x scripts/create_and_push_image.sh`
	`scripts/create_and_push_image.sh $ECR_REPO_NAME $image_tag $AWS_REGION $ACCOUNT_ID`
	Cette tâche suppose que vous disposez d'informations d'identification valides dans votre environnement. L'image Docker est envoyée vers le référentiel Amazon ECR spécifié dans la variable d'environnement de la tâche précédente et est utilisée pour activer le conteneur SageMaker AI dans lequel la tâche de formation sera exécutée.
		Ingénieur ML, General AWS

Tâche	Description	Compétences requises
Copiez les données d'entrée sur Amazon S3.	Le poste de formation à l' SageMaker IA doit récupérer les données d'entrée. Pour copier les données d'entrée dans le compartiment Amazon S3 pour les données, exécutez la commande suivante : `aws s3 cp data/train.csv "${INPUT_DATA_S3_PATH}train.csv"`	Ingénieur de données, General AWS

Tâche	Description	Compétences requises
Soumettez des offres de formation en SageMaker IA.	Pour simplifier l'exécution de vos scripts, spécifiez les paramètres de configuration par défaut dans le `default.yaml` fichier. En plus de garantir la cohérence entre les cycles, cette approche offre également la flexibilité nécessaire pour remplacer facilement les paramètres par défaut selon les besoins. Consultez l'exemple suivant: `python scripts/start_sagemaker_training_job.py sagemaker.role_arn=$ROLE_ARN sagemaker.config_s3_bucket=$BUCKET_NAME_CONFIG sagemaker.input_data_s3_path=$INPUT_DATA_S3_PATH sagemaker.output_data_s3_path=$OUTPUT_DATA_S3_PATH`	AWS général, ingénieur ML, scientifique des données

Tâche	Description	Compétences requises
Exécutez le réglage des hyperparamètres de l' SageMaker IA.	L'exécution du réglage des hyperparamètres de l' SageMaker IA est similaire à la soumission d'une tâche de formation SageMaker AII. Cependant, le script d'exécuti on diffère sur certains points importants, comme vous pouvez le voir dans le fichier start_sagemaker_hpo_job.py. Les hyperparamètres à régler doivent être transmis via la charge utile du boto3, et non par un canal vers le poste de formation. Pour démarrer la tâche d'optimisation des hyperpara mètres (HPO), exécutez les commandes suivantes : `python scripts/s tart_sagemaker_hpo _job.py sagemaker .role_arn=$ROLE_AR N sagemaker.config_s 3_bucket=$BUCKET_N AME_CONFIG sagemaker .input_data_s3_path= $INPUT_DATA_S3_PATH sagemaker.output_d ata_s3_path=$OUTPU T_DATA_S3_PATH`	Spécialiste des données

Résolution des problèmes

Problème	Solution
Jeton expiré	Exportez de nouvelles AWS informations d'identification.
Absence d'autorisations IAM	Assurez-vous d'exporter les informations d'identification d'un rôle IAM disposant de toutes les autorisations IAM requises pour déployer le CloudFormation modèle et démarrer les tâches de formation à l' SageMaker IA.

Ressources connexes

- Entraînez un modèle avec Amazon SageMaker AI (AWS documentation)
- Qu'est-ce que le réglage des hyperparamètres ?

Informations supplémentaires

Ce modèle permet de relever les défis suivants :

Cohérence entre le développement local et le déploiement à grande échelle : grâce à ce modèle, les développeurs peuvent utiliser le même flux de travail, qu'ils utilisent des scripts Python locaux, qu'ils exécutent des conteneurs Docker locaux, qu'ils mènent des expériences de grande envergure sur l' SageMaker IA ou qu'ils déploient en production sur SageMaker l'IA. Cette cohérence est importante pour les raisons suivantes :

- Itération plus rapide — Cela permet une expérimentation locale rapide sans nécessiter d'ajustements majeurs lors de la mise à l'échelle.
- Pas de refactorisation : la transition vers des expériences de plus grande envergure sur l' SageMaker IA se fait sans difficulté et ne nécessite aucune refonte de la configuration existante.
- Amélioration continue — Le développement de nouvelles fonctionnalités et l'amélioration continue de l'algorithme sont simples car le code reste le même dans tous les environnements.

Gestion de la configuration : ce modèle utilise Hydra, un outil de gestion de configuration, pour offrir les avantages suivants :

- Les paramètres sont définis dans des fichiers de configuration, distincts du code.
- Les différents ensembles de paramètres peuvent être facilement échangés ou combinés.
- Le suivi des expériences est simplifié car la configuration de chaque exécution est enregistrée automatiquement.
- Les expériences dans le cloud peuvent utiliser la même structure de configuration que les exécutions locales, ce qui garantit la cohérence.

Avec Hydra, vous pouvez gérer efficacement la configuration en activant les fonctionnalités suivantes :

- Divisez les configurations : divisez les configurations de votre projet en éléments plus petits et faciles à gérer qui peuvent être modifiés indépendamment. Cette approche facilite la gestion de projets complexes.
- Ajustez facilement les paramètres par défaut : modifiez rapidement vos configurations de base afin de tester plus facilement de nouvelles idées.
- Alignez les entrées CLI et les fichiers de configuration : combinez facilement les entrées de ligne de commande avec vos fichiers de configuration. Cette approche réduit l'encombrement et la confusion, ce qui rend votre projet plus facile à gérer au fil du temps.

Formez et déployez un modèle de machine learning personnalisé supporté par GPU sur Amazon SageMaker

Créée par Ankur Shukla (AWS)

Récapitulatif

La formation et le déploiement d'un modèle d'apprentissage automatique (ML) supporté par une unité de traitement graphique (GPU) nécessitent une configuration initiale et une initialisation de certaines variables d'environnement pour tirer pleinement parti des avantages de NVIDIA. GPUs Cependant, la configuration de l'environnement et sa compatibilité avec l' SageMaker architecture Amazon sur le cloud Amazon Web Services (AWS) peuvent prendre beaucoup de temps.

Ce modèle vous permet de former et de créer un modèle de machine learning personnalisé supporté par GPU à l'aide d'Amazon. SageMaker Il fournit des étapes pour former et déployer un CatBoost modèle personnalisé basé sur un ensemble de données Amazon Reviews open source. Vous pouvez ensuite comparer ses performances sur une instance `p3.16xlarge` Amazon Elastic Compute Cloud (Amazon EC2).

Ce modèle est utile si votre organisation souhaite déployer des modèles de machine learning existants pris en charge par le GPU sur. SageMaker Vos data scientists peuvent suivre les étapes de ce modèle pour créer des conteneurs compatibles avec le GPU NVIDIA et déployer des modèles de machine learning sur ces conteneurs.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un compartiment source Amazon Simple Storage Service (Amazon S3) pour stocker les artefacts et les prédictions du modèle.
- Compréhension des instances de SageMaker blocs-notes et des blocs-notes Jupyter.
- Comprendre comment créer un rôle AWS Identity and Access Management (IAM) avec des autorisations de rôle de base SageMaker , des autorisations d'accès au compartiment S3 et des autorisations de mise à jour, ainsi que des autorisations supplémentaires pour Amazon Elastic Container Registry (Amazon ECR).

Limites

- Ce modèle est destiné aux charges de travail ML supervisées avec un code d'entraînement et de déploiement écrit en Python.

Architecture

Pile technologique

- SageMaker
- Amazon ECR

Outils

Outils

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs géré par AWS qui est sécurisé, évolutif et fiable.
- Amazon SageMaker — SageMaker est un service de machine learning entièrement géré.
- Docker — Docker est une plate-forme logicielle permettant de créer, de tester et de déployer rapidement des applications.
- Python — Python est un langage de programmation.

Code

Le code de ce modèle est disponible sur la page GitHub Implémentation d'un modèle de classification des révisions avec Catboost et le SageMaker référentiel.

Épopées

Préparation des données

Tâche	Description	Compétences requises
Créez un rôle IAM et associez les politiques requises.	Connectez-vous à l'AWS Management Console, ouvrez la console IAM et créez un nouveau rôle IAM. Attachez les politiques suivantes au rôle IAM : • `AmazonEC2ContainerRegistryFullAccess` • `AmazonS3FullAccess` • `AmazonSageMakerFullAccess` Pour plus d'informations à ce sujet, consultez la section Créer une instance de bloc-notes dans la SageMaker documentation Amazon.	Spécialiste des données
Créez l'instance du SageMaker bloc-notes.	Ouvrez la SageMaker console, choisissez instances de bloc-notes, puis choisissez Créer une instance de bloc-notes. Pour le rôle IAM, choisissez le rôle IAM que vous avez créé précédemment. Configurez l'instance de bloc-notes en fonction de vos besoins, puis choisissez Créer une instance de bloc-notes.	Spécialiste des données

Tâche	Description	Compétences requises
	Pour obtenir des instructions et des étapes détaillées, consultez la section Créer une instance de bloc-notes dans la SageMaker documentation Amazon.	
Pour cloner le référentiel.	Ouvrez le terminal dans l'instance de SageMaker bloc-notes et clonez le GitHub modèle de classification Implementation a review with Catboost et le SageMaker référentiel en exécutant la commande suivante : `git clone https://github.com/aws-samples/review-classification-using-catboost-sagemaker.git`	
Démarrez le bloc-notes Jupyter.	Démarrez le bloc-notes `Review classification model with Catboost and SageMaker.ipynb` Jupyter, qui contient les étapes prédéfinies.	Spécialiste des données

Ingénierie des fonctionnalités

Tâche	Description	Compétences requises
Exécutez des commandes dans le bloc-notes Jupyter.	Ouvrez le bloc-notes Jupyter et exécutez les commandes	Spécialiste des données

Tâche	Description	Compétences requises
	décrites dans les histoires suivantes pour préparer les données nécessaires à l'entraînement de votre modèle de machine learning.	

Lisez les données du compartiment S3.	`import pandas as pd`
	`import csv`
	`fname = 's3://amazon-reviews-pds/tsv/amazon_reviews_us_Digital_Video_Download_v1_00.tsv.gz'`
	`df = pd.read_csv(fname, sep='\t',delimiter='\t',error_bad_lines=False)`
		Spécialiste des données

Tâche	Description	Compétences requises

Prétraitez les données.	`import numpy as np`
	`def pre_process(df):`
	
	`  df.fillna(value={'`
	`review_body': '',`
	`'review_headline':`
	`''}, inplace=True)`
	`df.fillna( value={'v`
	`erified_purchase':`
	`'Unk'}, inplace=True)`
	
	`df.fillna(0,`
	`inplace=True)`
	`return df`
	`df = pre_process(df)`
	`df.review_date =`
	`pd.to_datetime(df.`
	`review_date)`
	`df['target'] =`
	`np.where(df['star_`
	`rating']>=4,1,0)`
	
	Note
	Ce code remplace les valeurs nulles `'review_body'` par une chaîne vide et remplace la `'verified_purchase'` colonne par`'Unk'`, ce qui signifie « inconnu ».
		Spécialiste des données

Tâche	Description	Compétences requises
Divisez les données en ensembles de données d'entraînement, de validation et de test.	Pour que la distribution de l'étiquette cible reste identique dans les ensembles divisés, vous devez stratifier l'échanti llonnage à l'aide de la bibliothè que scikit-learn. `from sklearn.model_sele ction import Stratifie dShuffleSplit sss = Stratifie dShuffleSplit(n_sp lits=2, test_size =0.10, random_state=0) sss.get_n_splits(df, df['target']) for train_index, test_index in sss.split(df, df['target']): X_train_vallid , X_test = df.iloc[t rain_index], df.iloc[t est_index]`  `sss.get_n_splits(X_train_vallid, X_train_vallid['ta rget']) for train_index, test_index in sss.split(X_train_ vallid, X_train_v allid['target']): X_train , X_valid = X_train_vallid.ilo c[train_index],`	Spécialiste des données

Tâche	Description	Compétences requises
	`X_train_vallid.ilo c[test_index]`	

Créez, exécutez et envoyez l'image Docker vers Amazon ECR

Tâche	Description	Compétences requises
Préparez et insérez l'image Docker.	Dans le bloc-notes Jupyter, exécutez les commandes décrites dans les articles suivants pour préparer l'image Docker et la transférer vers Amazon ECR.	Ingénieur ML

Créez un référentiel dans Amazon ECR.	`%%sh`
	
	`algorithm_name=s agemaker-catboost- github-gpu-img`
	
	`chmod +x code/train`
	`chmod +x code/serve`
	
	`account=$(aws sts get- caller-identity -- query Account --output text)`
	
	`# Get the region defined in the current configuration (default to us-west-2 if none defined)`
	`region=$(aws configure get region)`
	`region=${region:-us- east-1}`
		Ingénieur ML

Tâche	Description	Compétences requises

	`fullname="${accou nt}.dkr.ecr.${regi on}.amazonaws.com/ ${algorithm_name}: latest"`
	
	`aws ecr create-re pository --repository- name "${algorithm_name} " > /dev/nul`	

Créez une image Docker localement.	`docker build -t "${algorithm_name}" . docker tag ${algorit hm_name} ${fullname}`	Ingénieur ML
Exécutez l'image Docker et envoyez-la vers Amazon ECR.	`docker push ${fullname}`	Ingénieur ML

Entraînement

Tâche	Description	Compétences requises
Créez une tâche de réglage d' SageMaker hyperparamètres.	Dans le bloc-notes Jupyter, exécutez les commandes décrites dans les histoires suivantes pour créer une tâche de réglage d' SageMaker hyperparamètres à l'aide de votre image Docker.	Spécialiste des données
Créez un SageMaker estimateur.	Créez un SageMaker estimateur en utilisant le nom de l'image Docker.	Spécialiste des données

Tâche	Description	Compétences requises

	`import sagemaker as sage`
	`from time import gmtime,`
	` strftime`
	`sess = sage.Session()`
	`from sagemaker.tuner`
	` import IntegerPa`
	`rameter, Categoric`
	`alParameter, Continuou`
	`sParameter, Hyperpara`
	`meterTuner`
	
	`account = sess.boto`
	`_session.client('s`
	`ts').get_caller_id`
	`entity()['Account']`
	`region = sess.boto`
	`_session.region_name`
	`image = '{}.dkr.e`
	`cr.{}.amazonaws.co`
	`m/sagemaker-catboo`
	`st-github-gpu-img:`
	`latest'.format(acc`
	`ount, region)`
	`tree_hpo = sage.esti`
	`mator.Estimator(im`
	`age,`
	
	` role, 1,`
	
	` 'ml.p3.16xlarge',`
	
	`  train_volume_size =`
	` 100,`
	
	`  output_path="s3://`
	`{}/sagemaker/DEMO-`
	`GPU-Catboost/outpu`
	`t".format(bucket),`	

Tâche	Description	Compétences requises
	<pre> sagemaker_session= sess)</pre>	

Tâche	Description	Compétences requises

Créez une tâche HPO.	Créez une tâche de réglage d'optimisation des hyperparamètres (HPO) avec des plages de paramètres et transmettez le train et les ensembles de validation en tant que paramètres à la fonction.
	
	`hyperparameter_ranges = {'iterations': IntegerParameter(80000, 130000),`
	
	`'max_depth': IntegerParameter(6, 10),`
	
	`'max_ctr_complexity': IntegerParameter(4, 10),`
	
	`'learning_rate': ContinuousParameter(0.01, 0.5)}`
	
	`objective_metric_name = 'auc'`
	`metric_definitions = [{'Name': 'auc',`
	
	`'Regex': 'auc: ([0-9\.]+)'}]`
	
	`tuner = HyperparameterTuner(tree_hpo,`
	
	`objective_metric_name,`
	
	`hyperparameter_ranges,`
		Spécialiste des données

Tâche	Description	Compétences requises

	`metric_definitions,`
	`objective_type='Maximize',`
	`max_jobs=50,`
	`max_parallel_jobs=2)`	

Exécutez le job HPO.	`train_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/train/'`
	`valid_location = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/valid/'`
	`tuner.fit({'train': train_location, 'validation': valid_location})`
		Spécialiste des données

Recevez le poste de formation le plus performant.	`import sagemaker as sage`
	`from time import gmtime, strftime`
	`sess = sage.Session()`
	`best_job =tuner.best_training_job()`
		Spécialiste des données

Transformation par lots

Tâche	Description	Compétences requises
Créez une tâche de transformation SageMaker par lots sur les données de test pour la prédiction du modèle.	Dans le bloc-notes Jupyter, exécutez les commandes décrites dans les articles suivants pour créer le modèle à partir de votre tâche de réglage des SageMaker hyperparamètres et soumettez une tâche de transformation SageMaker par lots sur les données de test pour la prédiction du modèle.	Spécialiste des données

Créez le SageMaker modèle.	Créez un modèle dans un SageMaker modèle en utilisant le meilleur travail de formation.
	`attached_estimator = sage.estimator.Estimator.attach(best_job)`
	`output_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/'`
	`input_path ='s3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test/'`
	`transformer = attached_estimator.transformer(instance_count=1,`
		Spécialiste des données

Tâche	Description	Compétences requises
	`instance_type='ml.p3.16xlarge', assemble_with='Line', accept='text/csv', max_payload=1, output_path=output_path, env = {'SAGEMAKER_MODEL_SERVER_TIMEOUT' : '3600' })`	
Créez une tâche de transformation par lots.	Créez une tâche de transformation par lots sur l'ensemble de données de test. `transformer.transform(input_path, content_type='text/csv', split_type='Line')`	Spécialiste des données

Analyser les résultats

Tâche	Description	Compétences requises
Lisez les résultats et évaluez les performances du modèle.	Dans le bloc-notes Jupyter, exécutez les commandes décrites dans les histoires suivantes pour lire les résultats et évaluer les performances du modèle selon les métriques du modèle Area Under the ROC Curve (ROC-AUC) et Area Under the Precision Recall Curve (PR-AUC). Pour plus d'informations à ce sujet, consultez les concepts clés d'Amazon Machine Learning dans la documentation Amazon Machine Learning (Amazon ML).	Spécialiste des données

Lisez les résultats de la tâche de transformation par lots.	Lisez les résultats du travail de transformation par lots en un bloc de données.
	
	`file_name = 's3://'+bucket+'/sagemaker/DEMO-GPU-Catboost/data/test-predictions/file_1.out'`
	
	`results = pd.read_csv(file_name, names=['review_id','target','score'] ,sep='\t'`
		Spécialiste des données

Tâche	Description	Compétences requises
	,escapechar ='\\' , quoting=csv.QUOTE_NONE, lineterminator='\n',quotechar='"').dropna()	

Tâche	Description	Compétences requises

Évaluez les indicateurs de performance.	Évaluez les performances du modèle sur ROC-AUC et PR-AUC.
	
	`from sklearn import metrics`
	`import matplotlib`
	`import pandas as pd`
	`matplotlib.use('agg', warn=False, force=True)`
	`from matplotlib import pyplot as plt`
	
	`%matplotlib inline`
	
	`def analyze_results(labels, predictions):`
	`precision, recall, thresholds = metrics.precision_recall_curve(labels, predictions)`
	`auc = metrics.auc(recall, precision)`
	
	`fpr, tpr, _ = metrics.roc_curve(labels, predictions)`
	`roc_auc_score = metrics.roc_auc_score(labels, predictions)`
	
	`print('Neural-Nets: ROC auc=%.3f' % ( roc_auc_score))`
	
	`plt.plot(fpr, tpr, label="data 1, auc=" + str(roc_auc_score))`
		Spécialiste des données

Tâche	Description	Compétences requises

	<pre> plt.xlabel('1-Specificity')
	    plt.ylabel('Sensitivity')
	    plt.legend(loc=4)
	    plt.show()
	
	    lr_precision, lr_recall, _ = metrics.precision_recall_curve(labels, predictions)
	    lr_auc = metrics.auc(lr_recall, lr_precision)
	    # summarize scores
	    print('Neural-Nets: PR auc=%.3f' % (lr_auc))
	    # plot the precision-recall curves
	    no_skill = len(labels[labels==1.0]) / len(labels)
	    plt.plot([0, 1], [no_skill, no_skill], linestyle='--', label='No Skill')
	
	    plt.plot(lr_recall, lr_precision, marker='.', label='Neural-Nets')
	    # axis labels
	    plt.xlabel('Recall')
	    plt.ylabel('Precision')
	    # show the legend
	    plt.legend()
	    # show the plot</pre>	

Tâche	Description	Compétences requises

	`plt.show()`
	
	`return auc`
	
	`analyze_results(results['target'].values,results['score'].values)`	

Ressources connexes

- Formez et hébergez des modèles Scikit-Learn sur Amazon en SageMaker créant un conteneur Docker Scikit

Informations supplémentaires

La liste suivante présente les différents éléments du Dockerfile qui sont exécutés lors de la compilation, de l'exécution et du transfert de l'image Docker dans Amazon ECR Epic.

Installez Python avec aws-cli.

```
FROM amazonlinux:1

 RUN yum update -y && yum install -y python36 python36-devel python36-libs python36-
tools python36-pip && \
 yum install gcc tar make wget util-linux kmod man sudo git -y && \
 yum install wget -y && \
 yum install aws-cli -y && \
 yum install nginx -y && \
yum install gcc-c++.noarch -y && yum clean all
```

Installez les packages Python

```
RUN pip-3.6 install --no-cache-dir --upgrade pip && \pip3 install --no-cache-dir --
upgrade setuptools && \
```

```
pip3 install Cython && \
pip3 install --no-cache-dir numpy==1.16.0 scipy==1.4.1 scikit-learn==0.20.3
 pandas==0.24.2 \
flask gevent gunicorn boto3 s3fs  matplotlib joblib catboost==0.20.2
```

Installez CUDA et cuDNN

```
RUN wget https://developer.nvidia.com/compute/cuda/9.0/Prod/local_installers/
cuda_9.0.176_384.81_linux-run \
&& chmod u+x cuda_9.0.176_384.81_linux-run \
&& ./cuda_9.0.176_384.81_linux-run --tmpdir=/data --silent --toolkit --override \
&& wget https://custom-gpu-sagemaker-image.s3.amazonaws.com/installation/cudnn-9.0-
linux-x64-v7.tgz \
&& tar -xvzf cudnn-9.0-linux-x64-v7.tgz \
&& cp /data/cuda/include/cudnn.h /usr/local/cuda/include \
&& cp /data/cuda/lib64/libcudnn* /usr/local/cuda/lib64 \

&& chmod a+r /usr/local/cuda/include/cudnn.h /usr/local/cuda/lib64/libcudnn* \
&&  rm -rf /data/*
```

Créez la structure de répertoire requise pour SageMaker

```
RUN mkdir /opt/ml /opt/ml/input /opt/ml/input/config /opt/ml/input/data /opt/ml/input/
data/training /opt/ml/model /opt/ml/output /opt/program
```

Définissez les variables d'environnement NVIDIA

```
ENV PYTHONPATH=/opt/program
ENV PYTHONUNBUFFERED=TRUE
ENV PYTHONDONTWRITEBYTECODE=TRUE
ENV PATH="/opt/program:${PATH}"

# Set NVIDIA mount environments
ENV LD_LIBRARY_PATH=/usr/local/nvidia/lib:/usr/local/nvidia/lib64:$LD_LIBRARY_PATH
ENV NVIDIA_VISIBLE_DEVICES="all"
ENV NVIDIA_DRIVER_CAPABILITIES="compute,utility"
ENV NVIDIA_REQUIRE_CUDA "cuda>=9.0"
```

Copiez les fichiers d'entraînement et d'inférence dans l'image Docker

```
COPY code/* /opt/program/
```

```
WORKDIR /opt/program
```

Translate le langage naturel en requêtes DSL pour OpenSearch et requêtes Elasticsearch

Créée par Tabby Ward (AWS), Nicholas Switzer (AWS) et Breanne Warner (AWS)

Récapitulatif

Ce modèle montre comment utiliser de grands modèles de langage (LLMs) pour convertir des requêtes en langage naturel en langage spécifique au domaine de requête (requête DSL), ce qui permet aux utilisateurs d'interagir plus facilement avec des services de recherche tels qu' OpenSearch Elasticsearch sans connaissance approfondie du langage de requête. Cette ressource est particulièrement utile pour les développeurs et les scientifiques des données qui souhaitent améliorer les applications basées sur la recherche grâce à des fonctionnalités de requête en langage naturel, améliorant ainsi l'expérience utilisateur et les fonctionnalités de recherche.

Le modèle illustre les techniques d'ingénierie rapide, de raffinement itératif et d'incorporation de connaissances spécialisées, qui sont toutes cruciales pour la génération de données synthétiques. Bien que cette approche se concentre principalement sur la conversion des requêtes, elle démontre implicitement le potentiel d'augmentation des données et de production de données synthétiques évolutives. Cette base pourrait être étendue à des tâches de génération de données synthétiques plus complètes, afin de mettre en évidence le pouvoir de relier les entrées LLMs en langage naturel non structurées aux sorties structurées spécifiques à l'application.

Cette solution n'implique pas d'outils de migration ou de déploiement au sens traditionnel du terme. Il se concentre plutôt sur la démonstration d'une preuve de concept (PoC) pour convertir les requêtes en langage naturel en requêtes DSL en utilisant. LLMs

- Le modèle utilise un bloc-notes Jupyter comme step-by-step guide pour configurer l'environnement et implémenter la text-to-query conversion.
- Il utilise Amazon Bedrock pour y accéder LLMs, ce qui est crucial pour interpréter le langage naturel et générer des requêtes appropriées.
- La solution est conçue pour fonctionner avec Amazon OpenSearch Service. Vous pouvez suivre un processus similaire pour Elasticsearch, et les requêtes générées pourraient éventuellement être adaptées à des moteurs de recherche similaires.

Query DSL est un langage de recherche flexible basé sur JSON qui est utilisé pour créer des requêtes complexes à la fois dans Elasticsearch et. OpenSearch Il vous permet de spécifier des

requêtes dans le paramètre de requête des opérations de recherche et prend en charge différents types de requêtes. Une requête DSL inclut des requêtes foliaires et des requêtes composées. Les requêtes Leaf recherchent des valeurs spécifiques dans certains champs et incluent le texte intégral, le niveau terminologique, les requêtes géographiques, les requêtes de jointure, les requêtes d'envergure et les requêtes spécialisées. Les requêtes composées agissent comme des enveloppes pour plusieurs clauses foliaires ou composées, et combinent leurs résultats ou modifient leur comportement. Query DSL permet de créer des recherches sophistiquées, qu'il s'agisse de simples requêtes assorties de combinaisons ou de requêtes complexes comportant plusieurs clauses qui produisent des résultats très spécifiques. Query DSL est particulièrement utile pour les projets qui nécessitent des fonctionnalités de recherche avancées, une construction de requêtes flexible et des structures de requêtes basées sur le langage JSON.

Ce modèle utilise des techniques telles que les instructions en quelques clics, les instructions système, les sorties structurées, le chaînage des invites, la fourniture de contexte et les instructions spécifiques aux tâches pour la conversion DSL. text-to-query Pour obtenir des définitions et des exemples de ces techniques, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

Pour utiliser efficacement le bloc-notes Jupyter afin de convertir des requêtes en langage naturel en requêtes DSL, vous devez :

- Connaissance des ordinateurs portables Jupyter. Compréhension de base de la navigation et de l'exécution de code dans un environnement de bloc-notes Jupyter.
- Environnement Python. Un environnement Python fonctionnel, de préférence Python 3.x, avec les bibliothèques nécessaires installées.
- Elasticsearch ou Knowledge. OpenSearch Connaissances de base d'Elasticsearch ou OpenSearch, notamment, de son architecture et de la manière d'exécuter des requêtes.
- Compte AWS. Un actif Compte AWS pour accéder à Amazon Bedrock et à d'autres services connexes.
- Bibliothèques et dépendances. Installation des bibliothèques spécifiques mentionnées dans le bloc-notes, par exemple `boto3` pour AWS l'interaction, et de toute autre dépendance requise pour l'intégration du LLM.

- Accès aux modèles dans Amazon Bedrock. Ce modèle utilise trois Claude LLMs d'Anthropic. Ouvrez la console Amazon Bedrock et choisissez Model access. Sur l'écran suivant, choisissez Activer des modèles spécifiques et sélectionnez les trois modèles suivants :
  - Sonnet de Claude III
  - Sonnet de Claude 3.5
  - Haïku Claude 3
- Politiques IAM et rôle IAM appropriés. Pour exécuter le bloc-notes dans un rôle AWS Identity and Access Management (IAM) Compte AWS, vous devez disposer de la `SagemakerFullAccess` politique ainsi que de la stratégie fournie dans la section Informations supplémentaires, que vous pouvez nommer`APGtext2querydslpolicy`. Cette politique inclut l'abonnement aux trois modèles Claude listés.

La mise en place de ces prérequis garantit une expérience fluide lorsque vous travaillez avec l'ordinateur portable et que vous implémentez les text-to-query fonctionnalités.

Limites

- Statut de preuve de concept. Ce projet est principalement conçu comme une preuve de concept (PoC). Il montre le potentiel de l'utilisation LLMs pour convertir des requêtes en langage naturel en requêtes DSL, mais il se peut qu'il ne soit pas entièrement optimisé ou prêt pour la production.
- Limites du modèle :

  Contraintes liées à la fenêtre contextuelle. Lorsque vous utilisez LLMs les fenêtres disponibles sur Amazon Bedrock, tenez compte des limites de la fenêtre contextuelle :

  Modèles Claude (en septembre 2024) :
  - Claude 3 Opus : 200 000 jetons
  - Claude 3 Sonnet : 200 000 jetons
  - Haïku Claude 3 : 200 000 jetons

  D'autres modèles sur Amazon Bedrock peuvent avoir des tailles de fenêtre contextuelles différentes. Consultez toujours la documentation la plus récente pour obtenir les dernières informations.

  Disponibilité du modèle.La disponibilité de certains modèles sur Amazon Bedrock peut varier. Assurez-vous d'avoir accès aux modèles requis avant de mettre en œuvre cette solution.

- Restrictions supplémentaires
  - Complexité des requêtes. L'efficacité du langage naturel pour interroger la conversion DSL peut varier en fonction de la complexité de la requête d'entrée.
  - Compatibilité des versions. La requête DSL générée peut nécessiter des ajustements en fonction de la version spécifique d'Elasticsearch ou de OpenSearch celle que vous utilisez.
  - Rendement. Ce modèle fournit une implémentation PoC, de sorte que la vitesse et la précision de génération des requêtes peuvent ne pas être optimales pour une utilisation en production à grande échelle.
  - Coût. L'utilisation LLMs dans Amazon Bedrock entraîne des frais. Soyez au courant de la structure de prix du modèle que vous avez choisi. Pour plus d'informations, consultez les tarifs d'Amazon Bedrock.
  - Entretien. Des mises à jour régulières des instructions et de la sélection du modèle peuvent être nécessaires pour suivre les avancées de la technologie LLM et les modifications de la syntaxe DSL des requêtes.

Versions du produit

Cette solution a été testée sur Amazon OpenSearch Service. Si vous souhaitez utiliser Elasticsearch, vous devrez peut-être apporter quelques modifications pour reproduire exactement les fonctionnalités de ce modèle.

- OpenSearch compatibilité des versions. OpenSearch maintient la rétrocompatibilité dans les versions majeures. Par exemple :
  - OpenSearch Les clients 1.x sont généralement compatibles avec les clusters OpenSearch 1.x.
  - OpenSearch Les clients 2.x sont généralement compatibles avec les clusters OpenSearch 2.x.

  Cependant, il est toujours préférable d'utiliser la même version mineure pour le client et le cluster lorsque cela est possible.
- OpenSearch Compatibilité avec les API. OpenSearch assure la compatibilité des API avec Elasticsearch OSS 7.10.2 pour la plupart des opérations. Cependant, certaines différences existent, notamment dans les nouvelles versions.
- OpenSearch considérations relatives aux mises à niveau :
  - Les rétrogradations directes ne sont pas prises en charge. Utilisez des instantanés pour revenir en arrière si nécessaire.

- Lors de la mise à niveau, consultez la matrice de compatibilité et les notes de version pour détecter toute modification importante.

Considérations relatives à Elasticsearch

- Version d'Elasticsearch. La version principale d'Elasticsearch que vous utilisez est essentielle, car la syntaxe et les fonctionnalités des requêtes peuvent changer entre les versions principales. Actuellement, la dernière version stable est Elasticsearch 8.x. Assurez-vous que vos requêtes sont compatibles avec votre version spécifique d'Elasticsearch.
- Version de la bibliothèque DSL de requêtes Elasticsearch. Si vous utilisez la bibliothèque Python DSL de requêtes Elasticsearch, assurez-vous que sa version correspond à votre version d'Elasticsearch. Par exemple :
  - Pour Elasticsearch 8.x, utilisez une `elasticsearch-dsl` version supérieure ou égale à 8.0.0 mais inférieure à 9.0.0.
  - Pour Elasticsearch 7.x, utilisez une `elasticsearch-dsl` version supérieure ou égale à 7.0.0 mais inférieure à 8.0.0.
- Version de la bibliothèque cliente. Que vous utilisiez le client Elasticsearch officiel ou un client spécifique à une langue, assurez-vous qu'il est compatible avec votre version d'Elasticsearch.
- Demande la version DSL. Query DSL évolue avec les versions d'Elasticsearch. Certains types de requêtes ou paramètres peuvent être obsolètes ou introduits dans différentes versions.
- Version cartographique. La façon dont vous définissez les mappages pour vos index et passez d'une version à l'autre. Consultez toujours la documentation de mappage correspondant à votre version spécifique d'Elasticsearch.
- Versions des outils d'analyse. Si vous utilisez des analyseurs, des tokeniseurs ou d'autres outils d'analyse de texte, leur comportement ou leur disponibilité peuvent changer d'une version à l'autre.

Architecture

Architecture cible

Le schéma suivant illustre l'architecture de ce modèle.

où :

1. Saisie par l'utilisateur et invite du système avec quelques exemples d'instructions. Le processus commence par un utilisateur qui fournit une requête en langage naturel ou une demande de génération de schéma.
2. Amazon Bedrock. La saisie est envoyée à Amazon Bedrock, qui sert d'interface pour accéder au Claude LLM.
3. Claude 3 Sonnet LLM. Amazon Bedrock utilise le sonnet Claude 3 de la famille Claude 3 LLMs pour traiter les données saisies. Il interprète et génère le DSL Elasticsearch ou OpenSearch de requête approprié. Pour les demandes de schéma, il génère des Elasticsearch synthétiques ou OpenSearch des mappings.
4. Génération de requêtes DSL. Pour les requêtes en langage naturel, l'application prend le résultat du LLM et le formate dans un DSL de requête Elasticsearch ou OpenSearch Service valide.
5. Génération de données synthétiques. L'application utilise également des schémas pour créer un Elasticsearch synthétique ou OpenSearch des données à charger dans une collection OpenSearch sans serveur à des fins de test.
6. OpenSearch ou Elasticsearch. Le Query DSL généré est interrogé par rapport à une collection OpenSearch sans serveur sur tous les index. La sortie JSON contient les données pertinentes et le nombre de connexions provenant des données contenues dans la collection OpenSearch Serverless.

Automatisation et évolutivité

Le code fourni avec ce modèle est conçu strictement à des fins de PoC. La liste suivante fournit quelques suggestions pour automatiser et étendre davantage la solution, ainsi que pour mettre le code en production. Ces améliorations n'entrent pas dans le cadre de ce modèle.

- Conteneurisation :
  - Dockerisez l'application pour garantir la cohérence entre les différents environnements.
  - Utilisez des plateformes d'orchestration de conteneurs telles qu'Amazon Elastic Container Service (Amazon ECS) ou Kubernetes pour des déploiements évolutifs.
- Architecture sans serveur :
  - Convertissez les fonctionnalités de base en AWS Lambda fonctions.
  - Utilisez Amazon API Gateway pour créer des RESTful points de terminaison pour la saisie des requêtes en langage naturel.
- Traitement asynchrone :

  - Implémentez Amazon Simple Queue Service (Amazon SQS) pour mettre en file d'attente les requêtes entrantes.
  - AWS Step Functions À utiliser pour orchestrer le flux de travail de traitement des requêtes et de génération de requêtes DSL.
- Mise en cache :
  - Implémentez un mécanisme pour mettre en cache les invites.
- Surveillance et journalisation :
  - Utilisez Amazon CloudWatch pour la surveillance et les alertes.
  - Mettez en place une journalisation centralisée avec Amazon CloudWatch Logs ou Amazon OpenSearch Service pour l'analyse des journaux.
- Améliorations de sécurité :
  - Implémentez des rôles IAM pour un contrôle d'accès précis.
  - Utilisez-le AWS Secrets Manager pour stocker et gérer en toute sécurité les clés d'API et les informations d'identification.
- Déploiement multirégional :
  - Envisagez de déployer la solution sur plusieurs sites Régions AWS pour améliorer la latence et la reprise après sinistre.
  - Utilisez Amazon Route 53 pour un routage intelligent des demandes.

En mettant en œuvre ces suggestions, vous pouvez transformer ce PoC en une solution robuste, évolutive et prête pour la production. Nous vous recommandons de tester minutieusement chaque composant et l'ensemble du système avant le déploiement complet.

Outils

Outils

- Les blocs-notes Amazon SageMaker AI sont des blocs-notes Jupyter entièrement gérés destinés au développement de l'apprentissage automatique. Ce modèle utilise les blocs-notes comme environnement interactif pour l'exploration des données, le développement de modèles et l'expérimentation dans Amazon SageMaker AI. Les ordinateurs portables offrent une intégration parfaite avec d'autres fonctionnalités de SageMaker l'IA et Services AWS.
- Python est un langage de programmation informatique polyvalent. Ce modèle utilise Python comme langage de base pour implémenter la solution.

- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée. Amazon Bedrock permet d'accéder au LLMs traitement du langage naturel. Ce modèle utilise les modèles Anthropic Claude 3.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python Services AWS, y compris Amazon Bedrock.
- Amazon OpenSearch Service est un service géré qui vous permet de déployer, d'exploiter et de dimensionner des clusters de OpenSearch services dans le cloud AWS. Ce modèle utilise le OpenSearch service comme système cible pour générer le DSL de requête.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Prompt Engineering Text-to-QueryDSL Using Claude 3 Models. L'exemple utilise une application de réseau social de santé qui crée des publications pour les utilisateurs et des profils d'utilisateurs associés à l'application de santé.

Bonnes pratiques

Lorsque vous utilisez cette solution, tenez compte des points suivants :

- Le besoin d' AWS informations d'identification et d'autorisations appropriées pour accéder à Amazon Bedrock
- Coûts potentiels associés à l'utilisation Services AWS et LLMs
- L'importance de comprendre le DSL des requêtes pour valider et éventuellement modifier les requêtes générées

Épopées

Configuration de l'environnement et préparation des données

Tâche	Description	Compétences requises
Configurez l'environnement de développement.	**Note** Pour obtenir des instructions détaillée	Python, pip, kit SDK AWS

Tâche	Description	Compétences requises
	s et le code correspondant à cette étape et aux autres étapes de ce modèle, consultez la procédure détaillée dans le GitHub référentiel. 1. Installez les packages Python requis, y comprisboto3,numpy, awscliopensearch-py , et requests-aws4auth en utilisant pip. 2. Importez les modules nécessaires tels que boto3 jsonos,opensearchpy ,, opensearch RequestsHttpConnection from Opensearchpy opensearchpy.helpers , bulk fromsagemaker ,time, randomre, et AWS4Auth fromrequests_aws4auth .	

Tâche	Description	Compétences requises
Configurez AWS l'accès.	Configurez le client Amazon Bedrock et la session SageMaker AI. Récupérez l'Amazon Resource Name (ARN) pour le rôle d'exécuti on SageMaker AI pour une utilisation ultérieure lors de la création de la collection OpenSearch Serverless.	IAM, AWS CLI, Amazon Bedrock, Amazon SageMaker
Chargez les schémas des applications de santé.	Lisez et analysez les schémas JSON pour les publications de santé et les profils utilisateur à partir de fichiers prédéfinis. Convertissez les schémas en chaînes pour une utilisation ultérieure dans les invites.	DevOps ingénieur, AWS général, Python, JSON

Génération de données synthétiques

Tâche	Description	Compétences requises
Créez un générateur de données basé sur le LLM.	Implémentez la fonction generate_data () pour appeler l'API Amazon Bedrock Converse avec les modèles Claude 3. Modèle de configura tion IDs pour Sonnet, Sonnet 3.5 et Haiku : `model_id_sonnet3_5 = "anthropic.claude-3-5-sonnet-20240620-v1:0"`	Python, API Amazon Bedrock, instructions LLM

Tâche	Description	Compétences requises
	`model_id_sonnet = "anthropic.claude-3-sonnet-20240229-v1:0" model_id_haiku = "anthropic.claude-3-haiku-20240307-v1:0"`	
Créez des postes de santé synthétiques.	Utilisez la fonction generate_data () avec une invite de message spécifique pour créer des entrées de santé synthétiques basées sur le schéma fourni. L'appel de fonction ressemble à ceci : `health_post_data = generate_data(bedrock_rt, model_id_sonnet, system_prompt, message_healthpost, inference_config)`	Python, JSON
Créez des profils utilisateur synthétiques.	Utilisez la fonction generate_data () avec un message d'invite spécifique pour créer des entrées de profil utilisateur synthétiques basées sur le schéma fourni. Ceci est similaire à la génération de postes de santé, mais utilise une invite différente.	Python, JSON

Configuration OpenSearch et ingestion de données

Tâche	Description	Compétences requises
Configurez une collection OpenSearch sans serveur.	Utilisez Boto3 pour créer une collection OpenSearch sans serveur avec des politiques de chiffrement, de réseau et d'accès appropriées. La création de la collection ressemble à ceci : `collection = aoss_client.create_collection(name=es_name, type='SEARCH')` Pour plus d'informations sur OpenSearch Serverless, consultez la AWS documentation.	OpenSearch Sans serveur, IAM
Définissez les OpenSearch index.	Créez des index pour les publications de santé et les profils d'utilisateurs à l'aide du OpenSearch client, sur la base des mappages de schéma prédéfinis. La création de l'index se présente comme suit : `response_health = oss_client.indices.create(healthpost_index, body=healthpost_body)`	OpenSearch, JSON

Tâche	Description	Compétences requises
Chargez les données dans OpenSearch.	Exécutez la fonction ingest_data () pour insérer en bloc les publications de santé synthétiques et les profils utilisateur dans leurs index respectifs. OpenSearch La fonction utilise l'assistant de masse fourni par `opensearch-py` : `success, failed = bulk(oss_client, actions)`	Python, OpenSearch API, opérations de données en masse

Génération et exécution de requêtes

Tâche	Description	Compétences requises
Concevez quelques exemples rapides.	Générez des exemples de requêtes et des questions en langage naturel correspondantes en utilisant les modèles Claude 3 pour servir d'exemples pour la génération de requêtes. L'invite du système inclut les exemples suivants : `system_prompt_query_generation = [{"text": f"""You are an expert query dsl generator. ... Examples: {example_prompt} ..."""}]`	Demande LLM, requête DSL

Tâche	Description	Compétences requises
Créez un convertisseur text-to-query DSL.	Implémentez l'invite du système, qui inclut des schémas, des données et quelques exemples de plans, pour la génération de requêtes. Utilisez l'invite du système pour convertir les requêtes en langage naturel en requêtes DSL. L'appel de fonction ressemble à ceci : `query_response = generate_data(bedrock_rt, model_id, system_prompt_query_generation, query, inference_config)`	Python, API Amazon Bedrock, instructions LLM
Testez la requête DSL sur. OpenSearch	Exécutez la fonction query_oss () pour exécuter la requête DSL générée par rapport à la collection OpenSearch Serverless et renvoyer les résultats. La fonction utilise la méthode de recherche du OpenSearch client : `response = oss_client.search(index="_all", body=temp)`	Python, OpenSearch API, requête DSL

Tester et évaluer

Tâche	Description	Compétences requises
Créez un ensemble de requêtes de test.	Utilisez Claude 3 pour générer un ensemble diversifié de questions de test basées sur les données synthétiques et les schémas : `test_queries = generate_data(bedrock_rt, model_id_sonnet, query_system_prompt, query_prompt, inference_config)`	Invitation au LLM
Évaluez la précision de la conversion DSL des requêtes.	Testez le DSL de requête généré en exécutant des requêtes OpenSearch et en analysant les résultats renvoyés pour en vérifier la pertinence et la précision . Cela implique d'exécuter la requête et d'inspecter les résultats : `output = query_oss(response1) print("Response after running query against Opensearch") print(output)`	Python, analyse de données, requête DSL
Modèles de référence Claude 3.	Comparez les performances de différents modèles Claude 3 (Haiku, Sonnet, Sonnet 3.5) pour la génération de requêtes en termes	Python, analyse comparative des performances

Tâche	Description	Compétences requises
	de précision et de latence. Pour comparer, modifiez le `model_id` moment où vous appelez generate_data () et mesurez le temps d'exécution.	

Nettoyage et documentation

Tâche	Description	Compétences requises
Développez un processus de nettoyage.	Supprimez tous les index de la collection OpenSearch Serverless après utilisation.	Python, kit SDK AWS, API OpenSearch

Ressources connexes

- Requête DSL (OpenSearch documentation)
- Documentation Amazon OpenSearch Service
- OpenSearch Collections sans serveur
- Documentation Amazon Bedrock
- Documentation Amazon SageMaker AI
- AWS SDK pour Python (Boto3) documentation

Informations supplémentaires

Politique IAM

Voici la `APGtext2querydslpolicy` politique applicable au rôle IAM utilisé dans ce modèle :

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Allow",
      "Action": [
```

```
        "bedrock:InvokeModel",
        "bedrock:InvokeModelWithResponseStream"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::sagemaker-*",
        "arn:aws:s3:::sagemaker-*/*"
      ]
    },
    { "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/sagemaker/*"
    },
    { "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aoss:*"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "iam:PassRole",
        "sagemaker:*"
      ],
      "Resource": [
```

```
        "arn:aws:iam::*:role/*", "*"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "sagemaker.amazonaws.com"
          }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "codecommit:GetBranch",
        "codecommit:GetCommit",
        "codecommit:GetRepository",
        "codecommit:ListBranches",
        "codecommit:ListRepositories"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Subscribe"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws-marketplace:ProductId": [
            "prod-6dw3qvchef7zy",
            "prod-m5ilt4siql27k",
            "prod-ozonys2hmmpeu"
          ]
        }
      }
    },
    { "Effect": "Allow",
      "Action": [
        "aws-marketplace:Unsubscribe",
        "aws-marketplace:ViewSubscriptions"
      ],
      "Resource": "*"
    },
    { "Effect": "Allow",
      "Action": "iam:*",
      "Resource": "*"
    }
```

```
  ]
}
```

Techniques rapides avec les modèles Anthropic Claude 3

Ce modèle illustre les techniques d'invite suivantes pour la conversion text-to-query DSL à l'aide des modèles Claude 3.

- Guidage en quelques prises : l'invite en quelques prises est une technique puissante pour améliorer les performances des modèles Claude 3 sur Amazon Bedrock. Cette approche implique de fournir au modèle un petit nombre d'exemples illustrant les input/output behavior before asking it to perform a similar task. When you use Claude 3 models on Amazon Bedrock, few-shot prompting can be particularly effective for tasks that require specific formatting, reasoning patterns, or domain knowledge. To implement this technique, you typically structure your prompt with two main components: the example section and the actual query. The example section contains one or more input/output paires souhaitées illustrant la tâche, et la section de requête présente la nouvelle entrée pour laquelle vous souhaitez une réponse. Cette méthode aide Claude 3 à comprendre le contexte et le format de sortie attendu, et aboutit souvent à une réponse plus précise et cohérente.

  Exemple :

```
"query": {
  "bool": {
    "must": [
      {"match": {"post_type": "recipe"}},
      {"range": {"likes_count": {"gte": 100}}},
      {"exists": {"field": "media_urls"}}
    ]
  }
}
Question: Find all recipe posts that have at least 100 likes and include media URLs.
```

- Instructions du système : en plus des quelques instructions, les modèles Claude 3 sur Amazon Bedrock prennent également en charge l'utilisation des instructions du système. Les instructions système permettent de fournir un contexte général, des instructions ou des directives au modèle avant de le présenter avec des entrées utilisateur spécifiques. Ils sont particulièrement utiles pour donner le ton, définir le rôle du modèle ou établir des contraintes pour l'ensemble de la conversation. Pour utiliser une invite système avec Claude 3 sur Amazon Bedrock, vous devez l'inclure dans le `system` paramètre de votre demande d'API. Ceci est distinct des messages de

l'utilisateur et s'applique à l'ensemble de l'interaction. Des instructions système détaillées sont utilisées pour définir le contexte et fournir des directives pour le modèle.

Exemple :

```
You are an expert query dsl generator. Your task is to take an input question and
 generate a query dsl to answer the question. Use the schemas and data below to
 generate the query.

Schemas: [schema details]
Data: [sample data]
Guidelines:
- Ensure the generated query adheres to DSL query syntax
- Do not create new mappings or other items that aren't included in the provided
 schemas.
```

- Sortie structurée : vous pouvez demander au modèle de fournir une sortie dans des formats spécifiques, tels que JSON ou dans des balises XML.

  Exemple :

  ```
  Put the query in json tags
  ```

- Chainage rapide : le bloc-notes utilise le résultat d'un appel LLM comme entrée pour un autre, par exemple en utilisant des données synthétiques générées pour créer des exemples de questions.
- Fourniture de contexte : le contexte pertinent, y compris les schémas et les exemples de données, est fourni dans les instructions.

  Exemple :

  ```
  Schemas: [schema details]
  Data: [sample data]
  ```

- Invites spécifiques aux tâches : différentes invites sont conçues pour des tâches spécifiques, telles que la génération de données synthétiques, la création d'exemples de questions et la conversion de requêtes en langage naturel en requêtes DSL.

  Exemple de génération de questions de test :

  ```
  Your task is to generate 5 example questions users can ask the health app based on
   provided schemas and data. Only include the questions generated in the response.
  ```

Utilisez Amazon Q Developer comme assistant de codage pour augmenter votre productivité

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Ce modèle utilise un tic-tac-toe jeu pour montrer comment vous pouvez appliquer Amazon Q Developer à un large éventail de tâches de développement. Il génère le code d'un tic-tac-toe jeu sous la forme d'une application monopage (SPA), améliore son interface utilisateur et crée des scripts pour déployer l' AWS application.

Amazon Q Developer fonctionne comme un assistant de codage pour accélérer les flux de travail de développement logiciel et améliorer la productivité des développeurs et des non-développeurs. Quelle que soit votre expertise technique, il vous aide à créer des architectures et à concevoir des solutions aux problèmes commerciaux, à démarrer votre environnement de travail, à implémenter de nouvelles fonctionnalités et à générer des cas de test à des fins de validation. Il utilise des instructions en langage naturel et des fonctionnalités d'intelligence artificielle pour garantir un code cohérent et de haute qualité et pour atténuer les difficultés de codage, quelles que soient vos compétences en programmation.

Le principal avantage d'Amazon Q Developer est sa capacité à vous libérer des tâches de codage répétitives. Lorsque vous utilisez l'`@workspace`annotation, Amazon Q Developer ingère et indexe tous les fichiers de code, les configurations et la structure de projet dans votre environnement de développement intégré (IDE), et fournit des réponses personnalisées pour vous aider à vous concentrer sur la résolution créative des problèmes. Vous pouvez consacrer plus de temps à la conception de solutions innovantes et à l'amélioration de l'expérience utilisateur. Si vous n'êtes pas technicien, vous pouvez utiliser Amazon Q Developer pour rationaliser les flux de travail et collaborer plus efficacement avec l'équipe de développement. La fonctionnalité Amazon Q Developer Explain code propose des instructions détaillées et des résumés, afin que vous puissiez naviguer dans des bases de code complexes.

En outre, Amazon Q Developer propose une approche indépendante de la langue qui aide les développeurs de niveau junior et intermédiaire à développer leurs compétences. Vous pouvez vous concentrer sur les concepts de base et la logique métier plutôt que sur la syntaxe spécifique au langage. Cela réduit la courbe d'apprentissage lorsque vous changez de technologie.

Conditions préalables et limitations

Prérequis

- IDE (par exemple, WebStorm ou Visual Studio Code) avec le plug-in Amazon Q Developer installé. Pour obtenir des instructions, consultez la section Installation de l'extension ou du plugin Amazon Q Developer dans votre IDE dans la documentation Amazon Q Developer.
- Une Compte AWS configuration active avec Amazon Q Developer. Pour obtenir des instructions, consultez Getting started dans la documentation Amazon Q Developer.
- npm installé. Pour obtenir des instructions, consultez la documentation npm. Ce modèle a été testé avec la version 10.8 de npm.
- AWS Command Line Interface (AWS CLI) installé. Pour obtenir des instructions, consultez la AWS CLI documentation.

Limites

- Amazon Q Developer ne peut effectuer qu'une seule tâche de développement à la fois.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Outils

- Ce modèle nécessite un IDE tel que Visual Studio Code ou WebStorm. Pour obtenir la liste des produits pris en charge IDEs, consultez la documentation Amazon Q Developer.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.

Bonnes pratiques

Consultez les meilleures pratiques de codage avec Amazon Q Developer dans les directives AWS prescriptives. En outre :

- Lorsque vous envoyez des instructions à Amazon Q Developer, assurez-vous que vos instructions sont claires et sans ambiguïté. Ajoutez des extraits de code et des annotations, par exemple `@workspace` à l'invite, pour fournir plus de contexte à vos invites.

- Incluez les bibliothèques pertinentes et importez-les pour éviter les conflits ou les suppositions incorrectes du système.
- Si le code généré n'est pas précis ou ne correspond pas aux attentes, utilisez l'option Fournir des commentaires et régénérer. Essayez de diviser les instructions en instructions plus petites.

Épopées

Configuration de l'environnement de travail

Tâche	Description	Compétences requises
Crée un projet.	Pour créer un nouveau projet dans votre environnement de travail, exécutez la commande suivante et acceptez les paramètres par défaut pour toutes les questions : `npx create-next-app@latest`	Développeur d'applications, programmeur, développeur de logiciels
Testez l'application de base.	Exécutez la commande suivante et vérifiez que l'application de base se charge correctement dans le navigateur : `npm run dev`	Développeur d'applications, programmeur, développeur de logiciels
Nettoyez le code de base.	Accédez au `page.tsx` fichier du `src/app` dossier et supprimez le contenu par défaut pour obtenir une page blanche. Après suppression, le fichier doit ressembler à ceci :	Développeur d'applications, programmeur, développeur de logiciels

Tâche	Description	Compétences requises
	`export default function Home() { return (<div></div> ); }`	

Utilisez Amazon Q Developer pour concevoir un projet de tic-tac-toe jeu

Tâche	Description	Compétences requises
Obtenez une vue d'ensemble des étapes.	1. Dans votre IDE, ouvrez votre projet et choisissez l'icône Amazon Q pour ouvrir le panneau de discussion. 2. Dans le panneau de discussion Amazon Q Developer, demandez un aperçu de la création d'une application monopage (SPA). Par exemple : `I would like to create a single-page application involving Next.js React framework for tic-tac-toe game. What are the steps?`	Développeur d'applications, programmeur, développeur de logiciels
Générez du code pour tic-tac-toe.	Dans le panneau de discussion, lancez une tâche de développement à l'aide de la `/dev` commande suivie de la	Développeur d'applications, programmeur, développeur de logiciels

Tâche	Description	Compétences requises

	description de la tâche. Par exemple :
	
	`/dev Create a React-based single-page application written in TypeScript for a tic-tac-toe game with the following specifications:`
	`1. Design an aesthetically pleasing interface with the game grid centered vertically and horizontally on the page.`
	`2. Include a heading and clear instructions on how to play the game.`
	`3. Implement color-coding for X and O marks to distinguish them easily.`
	
	Amazon Q Developer génère du code en fonction de vos instructions.	

Tâche	Description	Compétences requises
Vérifiez et acceptez le code généré.	Inspectez visuellement le code, puis choisissez Accepter le code pour remplacer automatiquement le `page.tsx` fichier. Si vous rencontrez des problèmes, choisissez Fournir des commentaires et régénérer et décrivez le problème que vous avez rencontré.	Développeur d'applications, programmeur, développeur de logiciels
Corrigez les erreurs de charpie.	L'exemple de tic-tac-toe jeu inclut une grille. Le code généré par Amazon Q Developer peut utiliser le type par défaut`any`. Vous pouvez ajouter la sécurité des types en demandant à Amazon Q Developer de la manière suivante : `/dev Ensure proper TypeScript typing for the onSquare Click event handler to resolve any 'any' type issues.`	Développeur d'applications, programmeur, développeur de logiciels

Tâche	Description	Compétences requises

Ajoutez un attrait visuel.	Vous pouvez diviser l'exigence initiale en fragments plus petits. Par exemple, vous pouvez améliorer l'interface utilisateur du jeu en utilisant les instructions suivantes dans les tâches de développement. Cette invite améliore les styles des feuilles de style en cascade (CSS) et exporte l'application pour le déploiement.
	`/dev Debug and fix any CSS issues to correctly display the game grid and overall layout.`
	
	`Simplify the code by removing game history functionality and related components.`
	
	`Implement static file export to an 'out' directory for easy deployment. The solution should be fully functional, visually appealing, and free of typing errors or layout issues.`
		Développeur d'applications, programmeur, développeur de logiciels

Tâche	Description	Compétences requises

Testez à nouveau.	1. Maintenant que vous avez terminé le cycle de développement, testez le code pour vérifier qu'il fonctionne comme prévu. Pour exécuter l'application localement, utilisez la commande suivante :
	`npm run dev`
	2. Si l'application fonctionne comme prévu, utilisez la `build` commande pour exporter l'ensemble de l'application vers le dossier de sortie en vue du déploiement :
	`npm run build`
		Développeur d'applications, programmeur, développeur de logiciels

Déployez l'application sur AWS Cloud

Tâche	Description	Compétences requises
Créez des dossiers et des fichiers pour le déploiement.	Dans le projet, dans votre environnement de travail, créez un dossier de déploiement et deux fichiers qu'il contient : `pushtos3.sh` et `cloudformation.yml` : `mkdir deployment && cd deployment`	Développeur d'applications, programmeur, développeur de logiciels

Tâche	Description	Compétences requises
	`touch pushtos3.sh && chmod +x pushtos3.sh` `touch cloudformation.yml`	

Tâche	Description	Compétences requises
Générez du code d'automatisation.	1. Dans le panneau de discussion d'Amazon Q Developer, saisissez l'invite suivante : `/dev Generate a Cloudformation template that creates two resources: tictactoe artifact bucket and CloudFront. CloudFront should be configured with this bucket as origin. Add cache policy appropriate for Amazon S3 and default root object as index.html. Ensure that origin access control is used and no public bucket is created. Output all the resources and their ARNs.` 2. Vérifiez et acceptez le code généré. Le `cloudformation.yml` fichier que vous avez créé précédemment doit maintenant être rempli avec un AWS CloudFormation script qui crée les ressources pour le AWS Cloud.	Administrateur AWS, AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises
Générez du contenu de script.	Pour créer un script de déploiement, utilisez l'invite suivante : `/dev Modify the pushtos3 shell script so that it can use AWS CLI commands to create a CloudFormation stack named tictactoe-stack if it does not exist already, and use cloudformation.yml as the source template. Wait for the stack to complete and sync the contents from the out folder to the S3 bucket. Perform invalidation of the CloudFront origin.`	Développeur d'applications, programmeur, développeur de logiciels
Déployez l'application sur AWS Cloud.	1. Configurez l'environnement de travail avec des AWS informations d'identification valides. 2. Exécutez le script shell pour déployer le tic-tac-toe jeu entièrement fonctionnel sur AWS Cloud.	Administrateur AWS, AWS DevOps, architecte cloud, développeur d'applications

Résolution des problèmes

Problème	Solution

La version ne crée pas d'application d'une seule page et ne l'exporte pas vers le dossier de sortie.	Regardez le contenu du `next.config.mjs` fichier.
	
	Si le code possède la configuration par défaut suivante :
	
	`const nextConfig = {};`
	
	modifiez-le comme suit :
	
	`const nextConfig = {`
	`  output: 'export',`
	`  distDir: 'out',`
	`};`

Ressources connexes

- Création d'un nouveau projet React (documentation React)
- Présentation d'Amazon Q Developer (AWS documentation)
- Bonnes pratiques pour les développeurs Amazon Q (conseils AWS prescriptifs)
- Installation, configuration et utilisation d'Amazon Q Developer avec JetBrains IDEs (YouTube vidéo)
- Installation d'Amazon Q pour la ligne de commande (AWS documentation)

Utiliser SageMaker le traitement pour l'ingénierie des fonctionnalités distribuées d'ensembles de données ML à l'échelle du téraoctet

Créée par Chris Boomhower (AWS)

Récapitulatif

De nombreux ensembles de données de plusieurs téraoctets ou plus se composent souvent d'une structure de dossiers hiérarchique, et les fichiers du jeu de données partagent parfois des interdépendances. C'est pourquoi les ingénieurs en apprentissage automatique (ML) et les scientifiques des données doivent prendre des décisions de conception réfléchies afin de préparer ces données pour l'entraînement et l'inférence des modèles. Ce modèle montre comment vous pouvez utiliser des techniques manuelles de macrosharding et de microsharding en combinaison avec Amazon SageMaker Processing et la parallélisation des processeurs virtuels (vCPU) pour adapter efficacement les processus d'ingénierie des fonctionnalités aux ensembles de données Big Data ML complexes.

Ce modèle définit le macrosharding comme la division de répertoires de données sur plusieurs machines pour le traitement, et le microsharding comme le partage des données de chaque machine sur plusieurs threads de traitement. Le modèle illustre ces techniques en utilisant Amazon SageMaker avec des exemples d'enregistrements de formes d'onde de séries chronologiques issus du jeu de données PhysioNet MIMIC-III. En mettant en œuvre les techniques de ce modèle, vous pouvez minimiser le temps de traitement et les coûts liés à l'ingénierie des fonctionnalités tout en maximisant l'utilisation des ressources et l'efficacité du débit. Ces optimisations reposent sur le SageMaker traitement distribué sur les instances Amazon Elastic Compute Cloud EC2 (Amazon) et v CPUs pour des ensembles de données volumineux similaires, quel que soit le type de données.

Conditions préalables et limitations

Prérequis

- Accès aux instances de SageMaker bloc-notes ou à SageMaker Studio, si vous souhaitez implémenter ce modèle pour votre propre ensemble de données. Si vous utilisez Amazon SageMaker pour la première fois, consultez la section Commencer avec Amazon SageMaker dans la documentation AWS.

- SageMaker Studio, si vous souhaitez implémenter ce modèle avec les exemples de données PhysioNet MIMIC-III.
- Le modèle utilise le SageMaker traitement, mais ne nécessite aucune expérience dans l'exécution de tâches SageMaker de traitement.

Limites

- Ce modèle convient parfaitement aux ensembles de données ML qui incluent des fichiers interdépendants. Ces interdépendances tirent le meilleur parti du macrosharding manuel et de l'exécution en parallèle de plusieurs SageMaker tâches de traitement en instance unique. Pour les ensembles de données où de telles interdépendances n'existent pas, la `ShardedByS3Key` fonctionnalité de SageMaker Processing peut constituer une meilleure alternative au macrosharding, car elle envoie des données fragmentées à plusieurs instances gérées par la même tâche de traitement. Cependant, vous pouvez implémenter la stratégie de microsharding de ce modèle dans les deux scénarios afin d'utiliser au mieux l'instance v. CPUs

Versions du produit

- Kit de développement logiciel Amazon SageMaker Python version 2

Architecture

Pile technologique cible

- Amazon Simple Storage Service (Amazon S3)
- Amazon SageMaker

Architecture cible

Macrosharding et instances distribuées EC2

Les 10 processus parallèles représentés dans cette architecture reflètent la structure du jeu de données MIMIC-III. (Les processus sont représentés par des ellipses pour simplifier les diagrammes.) Une architecture similaire s'applique à n'importe quel ensemble de données lorsque vous utilisez le macrosharding manuel. Dans le cas de MIMIC-III, vous pouvez utiliser la structure brute de l'ensemble de données à votre avantage en traitant chaque dossier de groupe de patients séparément, avec un minimum d'effort. Dans le schéma suivant, le bloc des groupes

d'enregistrements apparaît sur la gauche (1). Compte tenu de la nature distribuée des données, il est logique de les partager par groupe de patients.

Toutefois, le découpage manuel par groupe de patients signifie qu'une tâche de traitement distincte est requise pour chaque dossier de groupe de patients, comme vous pouvez le voir dans la partie centrale du diagramme (2), au lieu d'une tâche de traitement unique avec plusieurs EC2 instances. Étant donné que les données de MIMIC-III incluent à la fois des fichiers de formes d'onde binaires et des fichiers d'en-tête textuels correspondants, et que l'extraction de données binaires nécessite une dépendance à la bibliothèque wfdb, tous les dossiers d'un patient spécifique doivent être disponibles sur la même instance. La seule façon de s'assurer que le fichier d'en-tête associé à chaque fichier de forme d'onde binaire est également présent est d'implémenter le sharding manuel pour exécuter chaque partition dans le cadre de sa propre tâche de traitement, et de spécifier `s3_data_distribution_type='FullyReplicated'` quand vous définissez l'entrée de la tâche de traitement. Sinon, si toutes les données étaient disponibles dans un seul répertoire et qu'aucune dépendance n'existait entre les fichiers, une option plus appropriée pourrait être de lancer une seule tâche de traitement avec plusieurs EC2 instances `s3_data_distribution_type='ShardedByS3Key'` spécifiées. Spécifier `ShardedByS3Key` comme le type de distribution de données Amazon S3 indique SageMaker de gérer automatiquement le partitionnement des données entre les instances.

Le lancement d'une tâche de traitement pour chaque dossier est un moyen rentable de prétraiter les données, car l'exécution simultanée de plusieurs instances permet de gagner du temps. Pour économiser du temps et des coûts supplémentaires, vous pouvez utiliser le microsharding dans chaque tâche de traitement.

Microsharding et parallel v CPUs

Au sein de chaque tâche de traitement, les données groupées sont ensuite divisées afin de maximiser l'utilisation de tous les v disponibles CPUs sur l' EC2 instance SageMaker entièrement gérée. Les blocs situés dans la partie centrale du diagramme (2) décrivent ce qui se passe dans le cadre de chaque tâche de traitement principale. Le contenu des dossiers des patients est aplati et divisé de manière égale en fonction du nombre de v disponibles CPUs sur l'instance. Une fois le contenu du dossier divisé, l'ensemble de fichiers de taille uniforme est réparti sur tous les v CPUs pour être traité. Une fois le traitement terminé, les résultats de chaque vCPU sont combinés dans un seul fichier de données pour chaque tâche de traitement.

Dans le code joint, ces concepts sont représentés dans la section suivante du `src/feature-engineering-pass1/preprocessing.py` fichier.

```
def chunks(lst, n):
    """
    Yield successive n-sized chunks from lst.

    :param lst: list of elements to be divided
    :param n: number of elements per chunk
    :type lst: list
    :type n: int
    :return: generator comprising evenly sized chunks
    :rtype: class 'generator'
    """
    for i in range(0, len(lst), n):
        yield lst[i:i + n]


# Generate list of data files on machine
data_dir = input_dir
d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]
file_list = []
for ds in d_subs:
    file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))
dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in
 file_list if f[-4:] == '.dat']

# Split list of files into sub-lists
cpu_count = multiprocessing.cpu_count()
splits = int(len(dat_list) / cpu_count)
if splits == 0: splits = 1
dat_chunks = list(chunks(dat_list, splits))

# Parallelize processing of sub-lists across CPUs
ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in
 dat_chunks)

# Compile and pickle patient group dataframe
ws_df_group = pd.concat(ws_df_list)
ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})
ws_df_group.to_json(os.path.join(output_dir, group_data_out))
```

Une fonction est d'abord définie pour consommer une liste donnée en la divisant en morceaux de taille égale `n` et en renvoyant ces résultats sous forme de générateur. `chunks` Ensuite, les données sont aplaties dans les dossiers des patients en compilant une liste de tous les fichiers de formes

d'onde binaires présents. Une fois cela fait, le nombre de v CPUs disponibles sur l' EC2 instance est obtenu. La liste des fichiers de formes d'onde binaires est répartie uniformément sur ces v CPUs par appel`chunks`, puis chaque sous-liste de formes d'onde est traitée sur son propre vCPU en utilisant la classe Parallel de joblib. Les résultats sont automatiquement combinés dans une liste unique de dataframes par la tâche de traitement, qui poursuit SageMaker ensuite le traitement avant de les écrire dans Amazon S3 une fois la tâche terminée. Dans cet exemple, 10 fichiers ont été écrits sur Amazon S3 par les tâches de traitement (un pour chaque tâche).

Lorsque toutes les tâches de traitement initiales sont terminées, une tâche de traitement secondaire, illustrée dans le bloc à droite du diagramme (3), combine les fichiers de sortie produits par chaque tâche de traitement principale et écrit la sortie combinée sur Amazon S3 (4).

Outils

Outils

- Python — L'exemple de code utilisé pour ce modèle est Python (version 3).
- SageMaker Studio — Amazon SageMaker Studio est un environnement de développement intégré (IDE) basé sur le Web pour l'apprentissage automatique qui vous permet de créer, de former, de déboguer, de déployer et de surveiller vos modèles d'apprentissage automatique. Vous exécutez SageMaker des tâches de traitement en utilisant des blocs-notes Jupyter dans Studio. SageMaker
- SageMaker Traitement — Amazon SageMaker Processing fournit un moyen simplifié d'exécuter vos charges de travail de traitement des données. Dans ce modèle, le code d'ingénierie des fonctionnalités est implémenté à grande échelle à l'aide de tâches SageMaker de traitement.

Code

Le fichier .zip joint fournit le code complet de ce modèle. La section suivante décrit les étapes à suivre pour créer l'architecture de ce modèle. Chaque étape est illustrée par un exemple de code extrait de la pièce jointe.

Épopées

Configuration de votre environnement SageMaker Studio

Tâche	Description	Compétences requises
Accédez à Amazon SageMaker Studio.	Accédez à SageMaker Studio depuis votre compte AWS en suivant les instructions fournies dans la SageMaker documentation Amazon.	Scientifique des données, ingénieur ML
Installez l'utilitaire wget.	Installez wget si vous avez intégré une nouvelle configuration de SageMaker Studio ou si vous n'avez jamais utilisé ces utilitaires dans SageMaker Studio auparavant. Pour l'installer, ouvrez une fenêtre de terminal dans la console SageMaker Studio et exécutez la commande suivante : `sudo yum install wget`	Scientifique des données, ingénieur ML
Téléchargez et décompressez l'exemple de code.	Téléchargez le `attachments.zip` fichier dans la section Pièces jointes. Dans une fenêtre de terminal, accédez au dossier dans lequel vous avez téléchargé le fichier et extrayez son contenu : `unzip attachment.zip`	Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises
	Accédez au dossier dans lequel vous avez extrait le fichier .zip et extrayez le contenu du `Scaled-Processing.zip` fichier. `unzip Scaled-Processing.zip`	
Téléchargez l'exemple de jeu de données sur physionet.org et chargez-le sur Amazon S3.	Exécutez le bloc-notes `get_data.ipynb` Jupyter dans le dossier contenant les `Scaled-Processing` fichiers. Ce bloc-notes télécharge un exemple de jeu de données MIMIC-III depuis physionet.org et le charge dans votre SageMaker compartiment de session Studio dans Amazon S3.	Scientifique des données, ingénieur ML

Configuration du premier script de prétraitement

Tâche	Description	Compétences requises
Aplatissez la hiérarchie des fichiers dans tous les sous-répertoires.	Dans les grands ensembles de données tels que MIMIC-III, les fichiers sont souvent répartis dans plusieurs sous-répertoires, même au sein d'un groupe parent logique. Votre script doit être configuré pour aplatir tous les fichiers de groupe dans tous les sous-	Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises

	répertoires, comme le montre le code suivant.
	
	`# Generate list of .dat files on machine`
	`data_dir = input_dir`
	`d_subs = next(os.walk(os.path.join(data_dir, '.')))[1]`
	`file_list = []`
	`for ds in d_subs:`
	`  file_list.extend(os.listdir(os.path.join(data_dir, ds, '.')))`
	`dat_list = [os.path.join(re.split('_|\.', f)[0].replace('n', ''), f[:-4]) for f in file_list if f[-4:] == '.dat']`
	
	Note
	Les exemples d'extraits de code présentés dans cette épopée proviennent du `src/feature-engineering-pass1/preprocessing.py` fichier fourni en pièce jointe.	

Tâche	Description	Compétences requises

Divisez les fichiers en sous-groupes en fonction du nombre de vCPU.	Les fichiers doivent être divisés en sous-groupes ou en morceaux de taille égale, en fonction du nombre de v CPUs présents sur l'instanc e qui exécute le script. Pour cette étape, vous pouvez implémenter un code similaire au suivant.
	`# Split list of files into sub-lists`
	`cpu_count = multiproc essing.cpu_count()`
	`splits = int(len(d at_list) / cpu_count)`
	`if splits == 0: splits = 1`
	`dat_chunks = list(chun ks(dat_list, splits))`
		Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises

Paralléliser le traitement des sous-groupes dans v. CPUs	La logique du script doit être configurée pour traiter tous les sous-groupes en parallèle . Pour ce faire, utilisez la `Parallel` classe et la `delayed` méthode de la bibliothèque Joblib comme suit.
	`# Parallelize processing of sub-lists across CPUs`
	`ws_df_list = Parallel(n_jobs=-1, verbose=0)(delayed(run_process)(dc) for dc in dat_chunks)`
		Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises

Enregistrez la sortie d'un seul groupe de fichiers sur Amazon S3.	Lorsque le traitement parallèle des vCPU est terminé, les résultats de chaque vCPU doivent être combinés et téléchargés dans le chemin du compartiment S3 du groupe de fichiers. Pour cette étape, vous pouvez utiliser un code similaire au suivant.
	`# Compile and pickle patient group dataframe`
	`ws_df_group = pd.concat(ws_df_list)`
	`ws_df_group = ws_df_group.reset_index().rename(columns={'index': 'signal'})`
	`ws_df_group.to_json(os.path.join(output_dir, group_data_out))`
		Scientifique des données, ingénieur ML

Configuration du deuxième script de prétraitement

Tâche	Description	Compétences requises
Combinez les fichiers de données produits dans toutes les tâches de traitement qui ont exécuté le premier script.	Le script précédent génère un fichier unique pour chaque tâche de SageMaker traitement qui traite un groupe de fichiers de l'ensemble de données. Ensuite, vous devez combiner ces fichiers de sortie en un seul objet et écrire un	Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises

	ensemble de données de sortie unique sur Amazon S3. Cela est démontré dans le `src/feature-engineering-pass1p5/preprocessing.py` fichier, qui est fourni en pièce jointe, comme suit.
	
	`def write_parquet(wavs_df, path):`
	`"""`
	`Write waveform summary dataframe to S3 in parquet format.`
	
	`:param wavs_df: waveform summary dataframe`
	`:param path: S3 directory prefix`
	`:type wavs_df: pandas dataframe`
	`:type path: str`
	`:return: None`
	`"""`
	`extra_args = {"ServerSideEncryption": "aws:kms"}`
	`wr.s3.to_parquet(`
	`df=wavs_df,`
	`path=path,`
	`compression='snappy',`
	`s3_additional_kwargs=extra_args)`
	
	`def combine_data():`	

Tâche	Description	Compétences requises

	`"""`
	`Get combined data and write to parquet.`
	
	`:return: waveform summary dataframe`
	`:rtype: pandas dataframe`
	`"""`
	`wavs_df = get_data()`
	`wavs_df = normalize_signal_names(wavs_df)`
	`write_parquet(wavs_df, "s3://{}/{}/{}".format(bucket_xform, dataset_prefix, pass1p5out_data))`
	
	`return wavs_df`
	
	`wavs_df = combine_data()`	

Exécuter des tâches de traitement

Tâche	Description	Compétences requises
Exécutez la première tâche de traitement.	Pour effectuer le macrosharding, exécutez une tâche de traitement distincte pour chaque groupe de fichiers. Le microsharding est effectué dans chaque tâche de traitement, car chaque tâche	Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises

	exécute votre premier script. Le code suivant montre comment lancer une tâche de traitement pour chaque répertoire de groupe de fichiers dans l'extrait suivant (inclus dans `notebooks/FeatExtract_Pass1.ipynb`).
	
	`pat_groups = list(range(30,40))`
	`ts = str(int(time.time()))`
	
	`for group in pat_groups:`
	`  sklearn_processor = SKLearnProcessor(framework_version='0.20.0',`
	
	`  role=role,`
	
	`  instance_type='ml.m5.4xlarge',`
	
	`  instance_count=1,`
	
	`  volume_size_in_gb=5)`
	`  sklearn_processor.run(`
	`  code='../src/feature-engineering-pass1/preprocessing.py',`
	`  job_name='-'.join(['scaled-`	

Tâche	Description	Compétences requises
	processing-p1', str(group), ts]), arguments=["input_path", "/opt/ml/processing/input", "output_path", "/opt/ml/processing/output", "group_data_out", "ws_df_group.json"], inputs= [ProcessingInput(source=f's3://{sess.default_bucket()}/data_inputs/{group}', destination='/opt/ml/processing/input', s3_data_distribution_type='FullyReplicated')], outputs= [ProcessingOutput(source='/opt/ml/processing/output', destination=f's3://{sess.default_bucket()}/data_outputs/{group}'	

Tâche	Description	Compétences requises
	)], wait=False)	

Tâche	Description	Compétences requises
Exécutez le deuxième travail de traitement.	Pour combiner les sorties générées par le premier ensemble de tâches de traitement et effectuer des calculs supplémentaires pour le prétraitement, vous devez exécuter votre deuxième script à l'aide d'une seule tâche de SageMaker traitement. Le code suivant illustre cela (inclus dans`notebooks/FeatExtract_Pass1p5.ipynb`). `ts = str(int(time.time( ))) bucket = sess.defa ult_bucket() sklearn_processor = SKLearnProcessor(f ramework_version=' 0.20.0', role=role, instance_ type='ml.t3.2xlarge', instance_ count=1, volume_si ze_in_gb=5) sklearn_processor.run(code='../src/featu re-engineering-pas s1p5/preprocessing .py',`	Scientifique des données, ingénieur ML

Tâche	Description	Compétences requises
	`job_name='-'.join(['scaled-processing', 'p1p5', ts]), arguments=['bucket', bucket, 'pass1out_prefix', 'data_outputs', 'pass1out_data', 'ws_df_group.json', 'pass1p5out_data', 'waveform_summary.parquet', 'statsdata_name', 'signal_stats.csv'], wait=True )`	

Ressources connexes

- Intégration à Amazon SageMaker Studio à l'aide de Quick Start (SageMaker documentation)
- Données de processus (SageMaker documentation)
- Traitement des données avec scikit-learn (documentation) SageMaker
- Documentation Joblib.parallel
- Moody, B., Moody, G., Villarroel, M., Clifford, G.D., & Silva, I. (2020). Base de données de formes d'onde MIMIC-III (version 1.0). PhysioNet.
- Johnson, A.E.W., Pollard, T.J., Shen, L., Lehman, L.H., Feng, M., Ghassemi, M., Moody, B., Szolovits, P., Celi, L.A., et Mark, R.G. (2016). MIMIC-III, une base de données sur les soins intensifs accessible gratuitement. Données scientifiques, 3, 160035.
- Licence de base de données de formes d'onde MIMIC-III

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Visualisez les résultats du modèle AI/ML à l'aide de Flask et AWS Elastic Beanstalk

Créée par Chris Caudill (AWS) et Durga Sury (AWS)

Récapitulatif

La visualisation des résultats des services d'intelligence artificielle et d'apprentissage automatique (AI/ML) nécessite souvent des appels d'API complexes qui doivent être personnalisés par vos développeurs et ingénieurs. Cela peut s'avérer un inconvénient si vos analystes souhaitent explorer rapidement un nouveau jeu de données.

Vous pouvez améliorer l'accessibilité de vos services et proposer une forme d'analyse de données plus interactive en utilisant une interface utilisateur (UI) Web qui permet aux utilisateurs de télécharger leurs propres données et de visualiser les résultats du modèle dans un tableau de bord.

Ce modèle utilise Flask et Plotly pour intégrer Amazon Comprehend à une application Web personnalisée et visualiser les sentiments et les entités à partir des données fournies par les utilisateurs. Le modèle indique également les étapes à suivre pour déployer une application à l'aide d'AWS Elastic Beanstalk. Vous pouvez adapter l'application en utilisant les services d'intelligence artificielle d'Amazon Web Services (AWS) ou avec un modèle entraîné personnalisé hébergé sur un point de terminaison (par exemple, un point de SageMaker terminaison Amazon).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée sur votre machine locale. Pour plus d'informations à ce sujet, consultez la section Principes de base de la configuration dans la documentation de l'AWS CLI. Vous pouvez également utiliser un environnement de développement intégré (IDE) AWS Cloud9 ; pour plus d'informations à ce sujet, consultez le didacticiel Python pour AWS Cloud9 et la prévisualisation des applications en cours d'exécution dans l'IDE AWS Cloud9 dans la documentation AWS Cloud9.

  Remarque : n' AWS Cloud9 est plus disponible pour les nouveaux clients. Les clients existants de AWS Cloud9 peuvent continuer à utiliser le service normalement. En savoir plus

- Compréhension du framework d'applications Web de Flask. Pour plus d'informations sur Flask, consultez le Quickstart dans la documentation de Flask.
- Python version 3.6 ou ultérieure, installé et configuré. Vous pouvez installer Python en suivant les instructions de la section Configuration de votre environnement de développement Python dans la documentation AWS Elastic Beanstalk.
- Interface de ligne de commande Elastic Beanstalk (EB CLI), installée et configurée. Pour plus d'informations à ce sujet, consultez Installer l'interface de ligne de commande EB et configurer l'interface de ligne de commande EB dans la documentation AWS Elastic Beanstalk.

Limites

- L'application Flask de ce modèle est conçue pour fonctionner avec des fichiers .csv qui utilisent une seule colonne de texte et sont limités à 200 lignes. Le code de l'application peut être adapté pour gérer d'autres types de fichiers et volumes de données.
- L'application ne prend pas en compte la conservation des données et continue d'agréger les fichiers utilisateur téléchargés jusqu'à ce qu'ils soient supprimés manuellement. Vous pouvez intégrer l'application à Amazon Simple Storage Service (Amazon S3) pour le stockage d'objets persistants ou utiliser une base de données telle qu'Amazon DynamoDB pour le stockage clé-valeur sans serveur.
- L'application ne prend en compte que les documents en anglais. Cependant, vous pouvez utiliser Amazon Comprehend pour détecter la langue principale d'un document. Pour plus d'informations sur les langues prises en charge pour chaque action, consultez la référence des API dans la documentation Amazon Comprehend.
- Une liste de résolution des problèmes contenant les erreurs courantes et leurs solutions est disponible dans la section Informations supplémentaires.

Architecture

Architecture d'application Flask

Flask est un framework léger pour développer des applications Web en Python. Il est conçu pour combiner le puissant traitement des données de Python avec une interface utilisateur Web riche. L'application Flask du modèle vous montre comment créer une application Web qui permet aux utilisateurs de télécharger des données, d'envoyer les données à Amazon Comprehend pour inférence, puis de visualiser les résultats. La structure de l'application est la suivante :

- `static`— Contient tous les fichiers statiques compatibles avec l'interface utilisateur Web (par exemple JavaScript, le CSS et les images)
- `templates`— Contient toutes les pages HTML de l'application
- `userData`— Stocke les données utilisateur téléchargées
- `application.py`— Le fichier d'application Flask
- `comprehend_helper.py`— Fonctions permettant de passer des appels d'API à Amazon Comprehend
- `config.py`— Le fichier de configuration de l'application
- `requirements.txt`— Les dépendances Python requises par l'application

Le `application.py` script contient les fonctionnalités de base de l'application Web, qui se composent de quatre routes Flask. Le schéma suivant montre ces itinéraires Flask.

- `/`est la racine de l'application et dirige les utilisateurs vers la `upload.html` page (stockée dans le `templates` répertoire).
- `/saveFile`est une route qui est invoquée après qu'un utilisateur télécharge un fichier. Cette route reçoit une `POST` demande via un formulaire HTML, qui contient le fichier téléchargé par l'utilisateur. Le fichier est enregistré dans le `userData` répertoire et l'itinéraire redirige les utilisateurs vers l'`/dashboard`itinéraire.
- `/dashboard`renvoie les utilisateurs vers la `dashboard.html` page. Dans le code HTML de cette page, il exécute le JavaScript code `static/js/core.js` qui lit les données de l'`/data`itinéraire, puis crée des visualisations pour la page.
- `/data`est une API JSON qui présente les données à visualiser dans le tableau de bord. Cet itinéraire lit les données fournies par l'utilisateur et utilise les fonctions incluses `comprehend_helper.py` pour envoyer les données utilisateur à Amazon Comprehend à des fins d'analyse des sentiments et de reconnaissance d'entités nommées (NER). La réponse d'Amazon Comprehend est formatée et renvoyée sous forme d'objet JSON.

Architecture de déploiement

Considérations relatives à la conception

Pour plus d'informations sur les considérations relatives à la conception des applications déployées à l'aide d'Elastic Beanstalk sur le cloud AWS, consultez la documentation d'AWS Elastic Beanstalk.

Pile technologique

- Amazon Comprehend
- Elastic Beanstalk
- Flask

Automatisation et mise à l'échelle

Les déploiements d'Elastic Beanstalk sont automatiquement configurés avec des équilibreurs de charge et des groupes de dimensionnement automatique. Pour plus d'options de configuration, consultez la section Configuration des environnements Elastic Beanstalk dans la documentation d'AWS Elastic Beanstalk.

Outils

- L'interface de ligne de commande AWS (AWS CLI) est un outil unifié qui fournit une interface cohérente pour interagir avec toutes les parties d'AWS.
- Amazon Comprehend utilise le traitement du langage naturel (NLP) pour extraire des informations sur le contenu des documents sans nécessiter de prétraitement spécial.
- AWS Elastic Beanstalk vous permet de déployer et de gérer rapidement des applications dans le cloud AWS sans avoir à vous renseigner sur l'infrastructure qui exécute ces applications.
- Elastic Beanstalk CLI (EB CLI) est une interface de ligne de commande pour AWS Elastic Beanstalk qui fournit des commandes interactives pour simplifier la création, la mise à jour et la surveillance d'environnements à partir d'un référentiel local.
- Le framework Flask effectue le traitement des données et les appels d'API à l'aide de Python et propose une visualisation Web interactive avec Plotly.

Code

Le code de ce modèle est disponible dans les résultats du modèle GitHub Visualize AI/ML à l'aide de Flask et du référentiel AWS Elastic Beanstalk.

Épopées

Configurer l'application Flask

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Extrayez le code de l'application à partir des résultats du modèle GitHub Visualize AI/ML à l'aide de Flask et du référentiel AWS Elastic Beanstalk en exécutant la commande suivante : `git clone git@github.com:aws-samples/aws-comprehend-elasticbeanstalk-for-flask.git` **Note** Assurez-vous de configurer vos clés SSH avec GitHub.	Developer
Installez les modules Python.	Une fois le dépôt cloné, un nouveau `aws-comprehend-elasticbeanstalk-for-flask` répertoire local est créé. Dans ce répertoire, le `requirements.txt` fichier contient les modules Python et les versions qui exécutent l'application. Utilisez les	Développeur Python

Tâche	Description	Compétences requises

	commandes suivantes pour installer les modules :
	
	`cd aws-comprehend-elasticbeanstalk-for-flask`
	
	`pip install -r requirements.txt`	

Tâche	Description	Compétences requises

Testez l'application localement.	Démarrez le serveur Flask en exécutant la commande suivante :
	
	`python application.py`
	
	Cela renvoie des informations sur le serveur en cours d'exécution. Vous devriez pouvoir accéder à l'application en ouvrant un navigateur et en vous rendant sur http://localhost:5000
	
	Note
	Si vous exécutez l'application dans un IDE AWS Cloud9, vous devez remplacer la `application.run()` commande du `application.py` fichier par la ligne suivante :
	
	`application.run(host=os.getenv('IP', '0.0.0.0'),port=int(os.getenv('PORT', 8080)))`
		Développeur Python

Tâche	Description	Compétences requises
	Vous devez annuler cette modification avant le déploiement.	

Déployez l'application sur Elastic Beanstalk

Tâche	Description	Compétences requises
Lancez l'application Elastic Beanstalk.	Pour lancer votre projet en tant qu'application Elastic Beanstalk, exécutez la commande suivante depuis le répertoire racine de votre application : `eb init -p python-3.6 comprehend_flask --region us-east-1` ⚠ Important • `comprehend_flask` est le nom de l'application Elastic Beanstalk et peut être modifié selon vos besoins. • Vous pouvez remplacer la région AWS par la région de votre choix. La région par défaut dans l'AWS CLI est utilisée si vous ne spécifiez aucune région.	Architecte, développeur

Tâche	Description	Compétences requises
	• L'application a été développée avec la version 3.6 de Python. Vous risquez de rencontrer des erreurs si vous utilisez d'autres versions de Python. Exécutez la `eb init -i` commande pour obtenir d'autres options de configuration de déploiement.	
Déployez l'environnement Elastic Beanstalk.	Exécutez la commande suivante depuis le répertoire racine de l'application : `eb create comprehend-flask-env` **Note** `comprehend-flask-env` est le nom de l'environnement Elastic Beanstalk et peut être modifié selon vos besoins. Le nom ne peut contenir que des lettres, des chiffres et des tirets.	Architecte, développeur

Tâche	Description	Compétences requises
Autorisez votre déploiement à utiliser Amazon Comprehend.	Bien que votre application soit déployée avec succès, vous devez également fournir à votre déploiement un accès à Amazon Comprehend. `ComprehendFullAccess` est une politique gérée par AWS qui fournit à l'application déployée les autorisations nécessaires pour effectuer des appels d'API à Amazon Comprehend. Attachez la `ComprehendFullAccess` politique à `aws-elasticbeanstalk-ec2-role` (ce rôle est automatiquement créé pour les instances Amazon Elastic Compute Cloud (Amazon EC2) de votre déploiement) en exécutant la commande suivante : `aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/ComprehendFullAccess --role-name aws-elasticbeanstalk-ec2-role`	Développeur, architecte de sécurité

Tâche	Description	Compétences requises
	Important `aws-elasticbeanstalk-ec2-role` est créé lors du déploiement de votre application. Vous devez terminer le processus de déploiement avant de pouvoir joindre la politique AWS Identity and Access Management (IAM).	
Accédez à l'application que vous avez déployée.	Une fois votre application déployée avec succès, vous pouvez la visiter en exécutant la `eb open` commande. Vous pouvez également exécuter la `eb status` commande pour recevoir des informations sur votre déploiement. L'URL de déploiement est répertoriée ci-dessous`CNAME`.	Architecte, développeur

(Facultatif) Personnalisez l'application en fonction de votre modèle ML

Tâche	Description	Compétences requises
Autorisez Elastic Beanstalk à accéder au nouveau modèle.	Assurez-vous qu'Elastic Beanstalk dispose des	Développeur, architecte de sécurité

Tâche	Description	Compétences requises
	autorisations d'accès requises pour votre nouveau modèle de point de terminaison. Par exemple, si vous utilisez un point de SageMaker terminais on Amazon, votre déploiement doit être autorisé à appeler le point de terminaison. Pour plus d'informations à ce sujet, consultez InvokeEnd pointla SageMaker documenta tion Amazon.	

Tâche	Description	Compétences requises
Envoyez les données utilisateur vers un nouveau modèle.	Pour modifier le modèle de machine learning sous-jacent dans cette application, vous devez modifier les fichiers suivants : • `comprehend_helper.py` — Il s'agit du script Python qui se connecte à Amazon Comprehend, traite la réponse et renvoie le résultat final à l'application. Dans ce script, vous pouvez soit acheminer les données vers un autre service d'IA sur le cloud AWS, soit envoyer les données vers un point de terminaison de modèle personnalisé. Nous vous recommandons également de formater les résultats dans ce script pour une séparation logique et une réutilisation de ce modèle. • `application.py` — Si vous modifiez le nom du `comprehend_helper.py` script ou des fonctions, vous devez mettre à jour le `application.py` script de l'application pour refléter ces modifications.	Spécialiste des données

Tâche	Description	Compétences requises
Mettez à jour les visualisations du tableau de bord.	Généralement, l'incorporation d'un nouveau modèle de machine learning signifie que les visualisations doivent être mises à jour pour refléter les nouveaux résultats. Ces modifications sont apportées dans les fichiers suivants : • `templates/dashboard.html` — L'application prédéfinie ne prend en compte que deux visualisations de base. La mise en page complète de la page peut être ajustée dans ce fichier. • `static/js/core.js` — Ce script capture la sortie formatée de la `/data` route du serveur Flask et utilise Plotly pour créer des visualisations. Vous pouvez ajouter ou mettre à jour les graphiques de la page.	Développeur Web

(Facultatif) Déployez l'application mise à jour

Tâche	Description	Compétences requises
Mettez à jour le fichier d'exigences de votre application.	Avant d'envoyer des modifications à Elastic Beanstalk, `requirements.txt` mettez à jour le fichier pour	Développeur Python

Tâche	Description	Compétences requises
	qu'il reflète les nouveaux modules Python en exécutant la commande suivante dans le répertoire racine de votre application : `pip freeze > requirements.txt`	
Redéployez l'environnement Elastic Beanstalk.	Pour vous assurer que les modifications apportées à votre application sont reflétées dans votre déploiement d'Elastic Beanstalk, accédez au répertoire racine de votre application et exécutez la commande suivante : `eb deploy` Cela envoie la version la plus récente du code de l'application à votre déploiement Elastic Beanstalk existant.	Administrateur système, architecte

Ressources connexes

- Appelez un point de terminaison SageMaker modèle Amazon à l'aide d'Amazon API Gateway et d'AWS Lambda
- Déploiement d'une application Flask sur Elastic Beanstalk
- Référence de commande EB CLI
- Configuration de votre environnement de développement Python

Informations supplémentaires

Liste de résolution des problèmes

Voici six erreurs courantes et leurs solutions.

Erreur 1

```
Unable to assume role "arn:aws:iam::xxxxxxxxxx:role/aws-elasticbeanstalk-ec2-role".
 Verify that the role exists and is configured correctly.
```

Solution : Si cette erreur se produit lors de l'exécution`eb create`, créez un exemple d'application sur la console Elastic Beanstalk pour créer le profil d'instance par défaut. Pour plus d'informations à ce sujet, consultez la section Création d'un environnement Elastic Beanstalk dans la documentation d'AWS Elastic Beanstalk.

Erreur 2

```
Your WSGIPath refers to a file that does not exist.
```

Solution : Cette erreur se produit dans les journaux de déploiement car Elastic Beanstalk s'attend à ce que le code Flask soit nommé. `application.py` Si vous avez choisi un autre nom, exécutez-le `eb config` et WSGIPath modifiez-le comme indiqué dans l'exemple de code suivant :

```
aws:elasticbeanstalk:container:python:
     NumProcesses: '1'
     NumThreads: '15'
     StaticFiles: /static/=static/
     WSGIPath: application.py
```

Assurez-vous de remplacer par le nom `application.py` de votre fichier.

Vous pouvez également utiliser Gunicorn et un Procfile. Pour plus d'informations sur cette approche, consultez la section Configuration du serveur WSGI avec un Procfile dans la documentation AWS Elastic Beanstalk.

Erreur 3

```
Target WSGI script '/opt/python/current/app/application.py' does not contain WSGI
 application 'application'.
```

Solution : Elastic Beanstalk s'attend à ce que la variable représentant votre application Flask soit nommée. `application` Assurez-vous que le `application.py` fichier utilise `application` comme nom de variable :

```
application = Flask(__name__)
```

Erreur 4

```
The EB CLI cannot find your SSH key file for keyname
```

Solution : utilisez l'interface de ligne de commande EB pour spécifier la paire de clés à utiliser ou pour créer une paire de clés pour les EC2 instances de votre déploiement. Pour résoudre l'erreur, lancez `eb init -i` et l'une des options vous demandera :

```
Do you want to set up SSH for your instances?
```

Répondez par Y pour créer une paire de clés ou pour spécifier une paire de clés existante.

Erreur 5

J'ai mis à jour mon code et je l'ai redéployé, mais mon déploiement ne reflète pas mes modifications.

Solution : Si vous utilisez un dépôt Git pour votre déploiement, assurez-vous d'ajouter et de valider vos modifications avant de redéployer.

Erreur 6

Vous êtes en train de prévisualiser l'application Flask à partir d'un IDE AWS Cloud9 et vous rencontrez des erreurs.

Solution : pour plus d'informations à ce sujet, consultez la section Aperçu des applications en cours d'exécution dans l'IDE AWS Cloud9 dans la documentation AWS Cloud9.

Traitement du langage naturel à l'aide d'Amazon Comprehend

En choisissant d'utiliser Amazon Comprehend, vous pouvez détecter des entités personnalisées dans des documents texte individuels en exécutant une analyse en temps réel ou des tâches par lots

asynchrones. Amazon Comprehend vous permet également de former des modèles personnalisés de reconnaissance d'entités et de classification de texte qui peuvent être utilisés en temps réel en créant un point de terminaison.

Ce modèle utilise des tâches par lots asynchrones pour détecter les sentiments et les entités d'un fichier d'entrée contenant plusieurs documents. L'exemple d'application fourni par ce modèle est conçu pour que les utilisateurs puissent télécharger un fichier .csv contenant une seule colonne avec un document texte par ligne. Le `comprehend_helper.py` fichier contenu dans les résultats du modèle GitHub Visualize AI/ML à l'aide de Flask et du référentiel AWS Elastic Beanstalk lit le fichier d'entrée et l'envoie à Amazon Comprehend pour traitement.

BatchDetectEntities

Amazon Comprehend inspecte le texte d'un lot de documents à la recherche d'entités nommées et renvoie l'entité détectée, l'emplacement, le type d'entité, ainsi qu'un score indiquant le niveau de confiance d'Amazon Comprehend. Un maximum de 25 documents peuvent être envoyés en un seul appel d'API, chaque document ayant une taille inférieure à 5 000 octets. Vous pouvez filtrer les résultats pour n'afficher que certaines entités en fonction du cas d'utilisation. Par exemple, vous pouvez ignorer le type d'`'quantity'` entité et définir un score de seuil pour l'entité détectée (par exemple, 0,75). Nous vous recommandons d'étudier les résultats correspondant à votre cas d'utilisation spécifique avant de choisir une valeur de seuil. Pour plus d'informations à ce sujet, consultez BatchDetectEntitiesla documentation Amazon Comprehend.

BatchDetectSentiment

Amazon Comprehend inspecte un lot de documents entrants et renvoie le sentiment dominant pour chaque document (`POSITIVE`, `NEUTRAL` `MIXED`, ou). `NEGATIVE` Un maximum de 25 documents peuvent être envoyés en un seul appel d'API, chaque document ayant une taille inférieure à 5 000 octets. L'analyse du sentiment est simple et vous choisissez le sentiment ayant le score le plus élevé à afficher dans les résultats finaux. Pour plus d'informations à ce sujet, consultez BatchDetectSentimentla documentation Amazon Comprehend.

Gestion de la configuration des flasques

Les serveurs Flask utilisent une série de variables de configuration pour contrôler le fonctionnement du serveur. Ces variables peuvent contenir des résultats de débogage, des jetons de session ou d'autres paramètres d'application. Vous pouvez également définir des variables personnalisées

accessibles pendant l'exécution de l'application. Il existe plusieurs approches pour définir les variables de configuration.

Dans ce modèle, la configuration est définie `config.py` et héritée dans`application.py`.

- > **Note**
  >
  > `config.py`contient les variables de configuration définies au démarrage de l'application. Dans cette application, une `DEBUG` variable est définie pour indiquer à l'application d'exécuter le serveur en mode débogage. : le mode Debug ne doit pas être utilisé lors de l'exécution d'une application dans un environnement de production. `UPLOAD_FOLDER`Rest une variable personnalisée qui est définie pour être référencée ultérieurement dans l'application et indiquer où les données utilisateur téléchargées doivent être stockées.
- `application.py`lance l'application Flask et hérite des paramètres de configuration définis dans. `config.py` Cela s'effectue à l'aide du code suivant :

```
application = Flask(__name__)
application.config.from_pyfile('config.py')
```

Plus de modèles

- Automatisez AWS les opérations d'infrastructure en utilisant Amazon Bedrock
- Déployez une ChatOps solution pour gérer les résultats du scan SAST en utilisant Amazon Q Developer dans les applications de chat, les actions personnalisées et AWS CloudFormation
- Générez des informations sur les données en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight
- Générez des informations sur les données Db2 z/OS à l'aide d' AWS Mainframe Modernization Amazon Q dans QuickSight
- Donnez aux instances de SageMaker bloc-notes un accès temporaire à un CodeCommit référentiel dans un autre compte AWS
- Gérez AWS Organizations les politiques sous forme de code en utilisant AWS CodePipeline Amazon Bedrock
- Migrez les charges de travail de création, de formation et de déploiement de ML vers Amazon à SageMaker l'aide des outils de développement AWS
- Modernisez l'application CardDemo mainframe en utilisant AWS Transform
- Effectuez des analyses avancées à l'aide d'Amazon Redshift ML
- Simplifiez le développement et le déploiement des robots Amazon Lex à l'aide d'un flux de travail automatisé
- Résoudre les problèmes liés aux états en AWS Step Functions utilisant Amazon Bedrock

Analyse

Rubriques

- Analyser les données Amazon Redshift dans Microsoft SQL Server Analysis Services
- Analysez et visualisez des données JSON imbriquées avec Amazon Athena et Amazon QuickSight
- Automatisez l'ingestion de AWS Data Exchange données depuis Amazon S3
- Automatisez l'application du chiffrement dans AWS Glue à l'aide d'un CloudFormation modèle AWS
- Créez un pipeline de données pour ingérer, transformer et analyser les données Google Analytics à l'aide du kit de AWS DataOps développement
- Créez un pipeline de traitement vidéo à l'aide d'Amazon Kinesis Video Streams et d'AWS Fargate
- Créez un pipeline de services ETL pour charger les données de manière incrémentielle d'Amazon S3 vers Amazon Redshift à l'aide d'AWS Glue
- Créez un maillage de données d'entreprise avec Amazon DataZone AWS CDK, et AWS CloudFormation
- Calculez la valeur à risque (VaR) à l'aide des services AWS
- Configurer l'accès entre comptes à un catalogue de données AWS Glue partagé à l'aide d'Amazon Athena
- Convertir la fonctionnalité temporelle Teradata NORMALIZE en Amazon Redshift SQL
- Convertir la fonctionnalité Teradata RESET WHEN en Amazon Redshift SQL
- Déployez et gérez un lac de données sans serveur sur le cloud AWS en utilisant l'infrastructure sous forme de code
- Appliquer le balisage des clusters Amazon EMR au lancement
- Assurez-vous que la journalisation d'Amazon EMR sur Amazon S3 est activée au lancement
- Génération de données de test à l'aide d'une tâche AWS Glue et de Python
- Ingérez de manière rentable des données IoT directement dans Amazon S3 à l'aide d'AWS IoT Greengrass
- Lancer une tâche Spark dans un cluster EMR transitoire à l'aide d'une fonction Lambda
- Migrez les charges de travail Apache Cassandra vers Amazon Keyspaces à l'aide d'AWS Glue
- Migrez les données Hadoop vers Amazon S3 à l'aide de Migrator WANdisco LiveData
- Migrer Oracle Business Intelligence 12c vers le cloud AWS à partir de serveurs sur site

- Migrez un cluster Apache Kafka sur site vers Amazon MSK en utilisant MirrorMaker
- Migrer une pile ELK vers Elastic Cloud sur AWS
- Migrez les données vers le à AWS Cloud l'aide de Starburst
- Optimisation de l'ingestion ETL de la taille du fichier d'entrée sur AWS
- Orchestrez un pipeline ETL avec validation, transformation et partitionnement à l'aide d'AWS Step Functions
- Effectuez des analyses avancées à l'aide d'Amazon Redshift ML
- Interrogez les tables Amazon DynamoDB avec SQL à l'aide d'Amazon Athena
- Accédez aux tables Amazon DynamoDB, interrogez-les et joignez-les à l'aide d'Athena
- Configurez un espace de données minimum viable pour partager les données entre les organisations
- Configurer un tri spécifique à la langue pour les résultats des requêtes Amazon Redshift à l'aide d'un UDF Python scalaire
- Abonnement d'une fonction Lambda aux notifications d'événements provenant de compartiments S3 dans différentes régions AWS
- Trois types de tâches ETL AWS Glue pour convertir des données vers Apache Parquet
- Visualisez les journaux d'audit d'Amazon Redshift à l'aide d'Amazon Athena et Amazon QuickSight
- Visualisez les rapports d'identification IAM pour tous les comptes AWS à l'aide d'Amazon QuickSight
- Plus de modèles

Analyser les données Amazon Redshift dans Microsoft SQL Server Analysis Services

Créée par Sunil Vora (AWS)

Récapitulatif

Ce modèle décrit comment connecter et analyser les données Amazon Redshift dans Microsoft SQL Server Analysis Services, en utilisant le fournisseur Intellisoft OLE DB ou le fournisseur CData ADO.NET pour accéder à la base de données.

Amazon Redshift est un service d'entrepôt des données entièrement géré dans le cloud. SQL Server Analysis Services est un outil de traitement analytique en ligne (OLAP) que vous pouvez utiliser pour analyser les données provenant de data marts et d'entrepôts de données tels qu'Amazon Redshift. Vous pouvez utiliser SQL Server Analysis Services pour créer des cubes OLAP à partir de vos données pour une analyse rapide et avancée des données.

Conditions préalables et limitations

Hypothèses

- Ce modèle décrit comment configurer SQL Server Analysis Services et le fournisseur Intellisoft OLE DB ou le fournisseur CData ADO.NET pour Amazon Redshift sur une instance Amazon Elastic Compute Cloud (Amazon). EC2 Vous pouvez également installer les deux sur un hôte du centre de données de votre entreprise.

Prérequis

- Un compte AWS actif
- Un cluster Amazon Redshift avec des informations d'identification

Architecture

Pile technologique source

- Un cluster Amazon Redshift

Pile technologique cible

- Services d'analyse Microsoft SQL Server

Architecture source et cible

Outils

- Microsoft Visual Studio 2019 (édition communautaire)
- Fournisseur Intellisoft OLE DB pour Amazon Redshift (version d'essai) CData ou fournisseur ADO.NET pour Amazon Redshift (version d'essai)

Épopées

Analyser les tables

Tâche	Description	Compétences requises
Analysez les tables et les données à importer.	Identifiez les tables Amazon Redshift à importer et leurs tailles.	DBA

Configuration de l' EC2 instance et installation des outils

Tâche	Description	Compétences requises
Configurez une EC2 instance.	Dans votre compte AWS, créez une EC2 instance dans un sous-réseau privé ou public.	Administrateur de systèmes
Installez des outils pour accéder à la base de données.	Téléchargez et installez le fournisseur Intellisoft OLE DB pour Amazon Redshift (CData ou le fournisseur ADO.NET pour Amazon Redshift).	Administrateur de systèmes

Tâche	Description	Compétences requises
Installez Visual Studio.	Téléchargez et installez Visual Studio 2019 (Community Edition).	Administrateur de systèmes
Installez les extensions.	Installez l'extension Microsoft Analysis Services Projects dans Visual Studio.	Administrateur de systèmes
Créez un projet.	Créez un nouveau projet de modèle tabulaire dans Visual Studio pour stocker vos données Amazon Redshift. Dans Visual Studio, choisissez l'option Projet tabulaire Analysis Services lors de la création de votre projet.	DBA

Création d'une source de données et importation de tables

Tâche	Description	Compétences requises
Créez une source de données Amazon Redshift.	Créez une source de données Amazon Redshift à l'aide du fournisseur Intellisoft OLE DB pour Amazon Redshift (ou du CData fournisseur ADO.NET pour Amazon Redshift) et de vos informations d'identification Amazon Redshift.	Amazon Redshift, administrateur de bases de données
Importez des tables.	Sélectionnez et importez des tables et des vues depuis Amazon Redshift dans votre	Amazon Redshift, administrateur de bases de données

Tâche	Description	Compétences requises
	projet SQL Server Analysis Services.	

Nettoyage après la migration

Tâche	Description	Compétences requises
Supprimez l' EC2 instance.	Supprimez l' EC2 instance que vous avez lancée précédemment.	Administrateur de systèmes

Ressources connexes

- Amazon Redshift (documentation AWS)
- Installation de SQL Server Analysis Services (documentation Microsoft)
- Concepteur de modèles tabulaires (documentation Microsoft)
- Présentation des cubes OLAP pour les analyses avancées (documentation Microsoft)
- Microsoft Visual Studio 2019 (édition communautaire)
- Fournisseur Intellisoft OLE DB pour Amazon Redshift (version d'essai)
- CData Fournisseur ADO.NET pour Amazon Redshift (version d'essai)

Analysez et visualisez des données JSON imbriquées avec Amazon Athena et Amazon QuickSight

Créée par Anoop Singh (AWS)

Récapitulatif

Ce modèle explique comment traduire une structure de données imbriquée au format JSON en vue tabulaire à l'aide d'Amazon Athena, puis comment visualiser les données dans Amazon. QuickSight

Vous pouvez utiliser des données au format JSON pour les flux de données alimentés par API provenant de systèmes d'exploitation afin de créer des produits de données. Ces données peuvent également vous aider à mieux comprendre vos clients et leurs interactions avec vos produits, afin que vous puissiez personnaliser l'expérience utilisateur et prévoir les résultats.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un fichier JSON qui représente une structure de données imbriquée (ce modèle fournit un exemple de fichier)

Limites :

- Les fonctionnalités JSON s'intègrent bien aux fonctions orientées SQL existantes dans Athena. Cependant, ils ne sont pas compatibles avec le langage ANSI SQL et le fichier JSON est censé contenir chaque enregistrement sur une ligne distincte. Vous devrez peut-être utiliser la `ignore.malformed.json` propriété dans Athena pour indiquer si les enregistrements JSON mal formés doivent être transformés en caractères nuls ou générer des erreurs. Pour plus d'informations, consultez la section Meilleures pratiques pour lire les données JSON dans la documentation d'Athena.
- Ce modèle ne prend en compte que de simples et petites quantités de données au format JSON. Si vous souhaitez utiliser ces concepts à grande échelle, envisagez d'appliquer un partitionnement des données et de consolider vos données dans des fichiers plus volumineux.

Architecture

Le schéma suivant montre l'architecture et le flux de travail de ce modèle. Les structures de données imbriquées sont stockées dans Amazon Simple Storage Service (Amazon S3) au format JSON. Dans Athena, les données JSON sont mappées à une structure de données Athena. Vous créez ensuite une vue pour analyser les données et visualiser la structure des données dans QuickSight.

Outils

Services AWS

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données. Ce modèle utilise Amazon S3 pour stocker le fichier JSON.
- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard. Ce modèle utilise Athena pour interroger et transformer les données JSON. En effectuant quelques actions AWS Management Console, vous pouvez pointer Athena vers vos données dans Amazon S3 et utiliser le SQL standard pour exécuter des requêtes ponctuelles. Athena fonctionne sans serveur, il n'y a donc aucune infrastructure à configurer ou à gérer, et vous ne payez que pour les requêtes que vous exécutez. Athena évolue automatiquement et exécute des requêtes en parallèle, de sorte que les résultats sont rapides, même avec des ensembles de données volumineux et des requêtes complexes.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données sur un tableau de bord unique. QuickSight vous permet de créer et de publier facilement des tableaux de bord interactifs qui incluent des informations sur le machine learning (ML). Vous pouvez accéder à ces tableaux de bord depuis n'importe quel appareil et les intégrer à vos applications, portails et sites Web.

Exemple de code

Le fichier JSON suivant fournit une structure de données imbriquée que vous pouvez utiliser dans ce modèle.

```
{
  "symbol": "AAPL",
  "financials": [
```

```
    {
      "reportDate": "2017-03-31",
      "grossProfit": 20591000000,
      "costOfRevenue": 32305000000,
      "operatingRevenue": 52896000000,
      "totalRevenue": 52896000000,
      "operatingIncome": 14097000000,
      "netIncome": 11029000000,
      "researchAndDevelopment": 2776000000,
      "operatingExpense": 6494000000,
      "currentAssets": 101990000000,
      "totalAssets": 334532000000,
      "totalLiabilities": 200450000000,
      "currentCash": 15157000000,
      "currentDebt": 13991000000,
      "totalCash": 67101000000,
      "totalDebt": 98522000000,
      "shareholderEquity": 134082000000,
      "cashChange": -1214000000,
      "cashFlow": 12523000000,
      "operatingGainsLosses": null
    }
  ]
}
```


Épopées

Configuration d'un compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	Pour créer un compartiment destiné à stocker le fichier JSON, connectez-vous à la console Amazon S3 AWS Management Console, ouvrez-la, puis choisissez Create bucket. Pour plus d'informations, consultez la section Création d'un compartim	Administrateur de systèmes

Tâche	Description	Compétences requises
	ent dans la documentation Amazon S3.	
Ajoutez les données JSON imbriquées.	Téléchargez votre fichier JSON dans le compartiment S3. Pour un exemple de fichier JSON, reportez-vous à la section précédente. Pour obtenir des instructions, consultez la section Chargement d'objets dans la documentation Amazon S3.	Administrateur de systèmes

Analyser les données dans Athena

Tâche	Description	Compétences requises
Créez une table pour mapper les données JSON.	1. Ouvrez la console Athena. 2. Créez une base de données en suivant les instructions de la documentation d'Athena. 3. Dans le menu Base de données, sélectionnez la base de données que vous avez créée. 4. Dans l'éditeur de requêtes, entrez une `CREATE TABLE` instruction telle que la suivante : `CREATE EXTERNAL TABLE financials_json ( symbol string, financials array<`	Developer

Tâche	Description	Compétences requises

	<pre>struct<re
	portdate: string,
	grossprof
	it: bigint,
	totalreve
	nue: bigint,
	totalcash
	: bigint,
	totaldebt
	: bigint,
	researcha
	nddevelopment:
	bigint>>
	)
	ROW FORMAT SERDE
	'org.openx.data.js
	onserde.JsonSerDe'
	LOCATION 's3://s3b
	ucket-for-athena/'</pre> où `LOCATION` indique l'emplacement du compartiment S3 contenant le fichier JSON.
	5. Choisissez Exécuter pour créer la table.
	
	Pour plus d'informations sur la création de tables, consultez la documentation d'Athena.	

Tâche	Description	Compétences requises
Créez une vue pour l'analyse des données.	1. Ouvrez la console Athena. 2. Créez une base de données en suivant les instructions de la documentation d'Athena. 3. Dans le menu Base de données, sélectionnez la base de données que vous avez créée. 4. Dans l'éditeur de requêtes, entrez une `CREATE VIEW` instruction telle que la suivante : `CREATE OR REPLACE VIEW financial_json_view AS SELECT symbol, financials[1].reportdate one_report_date, -- indexes start with 1 financials[1].totalrevenue one_total_revenue, financials[1].reportdate another_report_date, financials[1].totalrevenue another_total_revenue FROM financials_json where symbol='AAPL' ORDER BY 1`	Developer

Tâche	Description	Compétences requises
	5. Choisissez Run (Exécuter) pour créer la vue. Pour plus d'informations sur la création de vues, consultez la documentation d'Athena.	
Analysez et validez les données.	1. Ouvrez la console Athena. 2. Dans l'éditeur de requêtes, exécutez des requêtes en utilisant la vue que vous avez créée à l'étape précédente. 3. Validez les données par rapport au fichier JSON pour vérifier que les noms de colonnes et les types de données sont correctement mappés.	Developer

Visualisez les données dans QuickSight

Tâche	Description	Compétences requises
Configurez Athena en tant que source de données dans. QuickSight	1. Ouvrez la QuickSight console. 2. Choisissez Jeux de données, Nouveau jeu de données. 3. Choisissez Athena comme source de données.	Administrateur de systèmes

Tâche	Description	Compétences requises
	4. Choisissez la base de données qui inclut la vue que vous avez créée. 5. Choisissez la vue pour laquelle vous souhaitez créer un jeu de données. 6. Sur la page Terminer la création de l'ensemble de données, choisissez Directly query your data. 7. Choisissez Visualize.	
Visualisez les données dans QuickSight.	1. Après avoir visualisé le jeu de données, choisissez les éléments visuels dans le volet de gauche et choisissez les champs pour le jeu de données. Pour plus d'informations, consultez le didacticiel dans la QuickSight documentation. 2. Enregistrez les modifications apportées à l'analyse. 3. Choisissez Publier le tableau de bord pour publier les visuels que vous avez créés.	Analyste des données

Ressources connexes

- Documentation Amazon Athena
- QuickSight Tutoriels Amazon

- Utilisation du JSON imbriqué (article de blog)

Automatisez l'ingestion de AWS Data Exchange données depuis Amazon S3

Créée par Adnan Alvee (AWS) et Manikanta Gona (AWS)

Récapitulatif

Ce modèle fournit un AWS CloudFormation modèle qui vous permet d'ingérer automatiquement des données depuis AWS Data Exchange votre lac de données dans Amazon Simple Storage Service (Amazon S3).

AWS Data Exchange est un service qui facilite l'échange sécurisé d'ensembles de données basés sur des fichiers dans le cloud AWS. AWS Data Exchange les ensembles de données sont basés sur des abonnements. En tant qu'abonné, vous pouvez également accéder aux révisions des ensembles de données lorsque les fournisseurs publient de nouvelles données.

Le AWS CloudFormation modèle crée un événement et une AWS Lambda fonction dans Amazon CloudWatch Events. L'événement surveille toute mise à jour de l'ensemble de données auquel vous êtes abonné. En cas de mise à jour, CloudWatch lance une fonction Lambda qui copie les données dans le compartiment S3 que vous spécifiez. Lorsque les données ont été copiées avec succès, Lambda vous envoie une notification Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Abonnement à un ensemble de données dans AWS Data Exchange

Limites

- Le AWS CloudFormation modèle doit être déployé séparément pour chaque ensemble de données souscrit dans AWS Data Exchange.

Architecture

Pile technologique cible

- AWS Lambda
- Amazon S3
- AWS Data Exchange
- Amazon CloudWatch
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Vous pouvez utiliser le AWS CloudFormation modèle plusieurs fois pour les ensembles de données que vous souhaitez ingérer dans le lac de données.

Outils

- AWS Data Exchangepermet AWS aux clients d'échanger facilement en toute sécurité des ensembles de données basés sur des fichiers dans le AWS Cloud. En tant qu'abonné, vous pouvez trouver et vous abonner à des centaines de produits proposés par des fournisseurs de données qualifiés. Vous pouvez ensuite télécharger rapidement l'ensemble de données ou le copier sur Amazon S3 pour l'utiliser dans divers services d' AWS analyse et d'apprentissage automatique. Toute personne possédant un Compte AWS peut être AWS Data Exchange abonnée.
- AWS Lambda vous permet d'exécuter du code sans avoir à allouer ou gérer des serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous ne payez que pour le temps de calcul que vous consommez ; il n'y a aucun frais lorsque votre code n'est pas en cours d'exécution. Avec Lambda, vous pouvez exécuter du code pour pratiquement n'importe quel type d'application ou de service principal sans aucune administration. Lambda exécute votre code sur une infrastructure informatique à haute disponibilité et gère toutes les ressources de calcul, y compris la maintenance des serveurs et des systèmes d'exploitation, le provisionnement des capacités et le dimensionnement automatique, la surveillance du code et la journalisation.
- Amazon S3 fournit du stockage pour Internet. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources. À l'aide de règles simples que vous pouvez

configurer rapidement, vous pouvez associer des événements et les acheminer vers une ou plusieurs fonctions ou flux cibles. CloudWatch Events prend conscience des changements opérationnels au fur et à mesure qu'ils se produisent. Il répond à ces changements opérationnels et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état. Vous pouvez également utiliser les CloudWatch événements pour planifier des actions automatisées qui se déclenchent automatiquement à certains moments à l'aide d'expressions cron ou rate.

- Amazon Simple Notification Service (Amazon SNS) permet aux applications, aux utilisateurs finaux et aux appareils d'envoyer et de recevoir instantanément des notifications depuis le cloud. Amazon SNS propose des rubriques (canaux de communication) pour la messagerie à haut débit basée sur le push. many-to-many À l'aide des rubriques Amazon SNS, les éditeurs peuvent distribuer des messages à un grand nombre d'abonnés pour un traitement parallèle, notamment les files d'attente Amazon Simple Queue Service (Amazon SQS), les fonctions Lambda et les webhooks HTTP/S. Vous pouvez également utiliser Amazon SNS pour envoyer des notifications aux utilisateurs finaux par push mobile, SMS et e-mail.

Épopées

S'abonner à un ensemble de données

Tâche	Description	Compétences requises
Abonnez-vous à un ensemble de données.	Dans la AWS Data Exchange console, abonnez-vous à un ensemble de données. Pour obtenir des instructi ons, consultez la section Abonnement aux produits de données AWS Data Exchange dans la AWS documentation.	AWS général
Notez les attributs de l'ensemble de données.	Notez l'ID Région AWS, l'ID et l'ID de révision de l'ensemble de données. Vous en aurez besoin pour le AWS	AWS général

Tâche	Description	Compétences requises
	CloudFormation modèle à l'étape suivante.	

Déployer le AWS CloudFormation modèle

Tâche	Description	Compétences requises
Créez un compartiment et un dossier S3.	Si vous possédez déjà un lac de données dans Amazon S3, créez un dossier pour stocker les données à partir AWS Data Exchange desquelles vous souhaitez les ingérer. Si vous déployez le modèle à des fins de test, créez un nouveau compartiment S3 et notez le nom du compartiment et le préfixe de dossier pour l'étape suivante.	AWS général
Déployez le AWS CloudFormation modèle.	Déployez le AWS CloudFormation modèle fourni en pièce jointe à ce modèle. Pour obtenir des instructions, consultez la AWS CloudFormation documentation. Configurez les paramètres suivants pour qu'ils correspondent à vos paramètres Compte AWS, à ceux de votre ensemble de données et à ceux du compartiment S3 : ensemble de données Région AWS, ID du jeu de	AWS général

Tâche	Description	Compétences requises
	données, ID de révision, nom du compartiment S3 (par exemple**DOC-EXAMPLE-BUCKET**), préfixe de dossier (par exemple,**myfolder/**) et e-mail pour les notificat ions SNS. Vous pouvez attribuer n'importe quel nom au paramètre Nom du jeu de données. Lorsque vous déployez le modèle, il exécute une fonction Lambda pour ingérer automatiquement le premier ensemble de données disponible dans le jeu de données. L'ingestion ultérieur e a ensuite lieu automatiq uement, au fur et à mesure que de nouvelles données arrivent dans l'ensemble de données.	

Ressources connexes

- Abonnement à des produits de données sur AWS Data Exchange (AWS Data Exchange documentation)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Automatisez l'application du chiffrement dans AWS Glue à l'aide d'un CloudFormation modèle AWS

Créée par Diogo Guedes (AWS)

Récapitulatif

Ce modèle explique comment configurer et automatiser l'application du chiffrement dans AWS Glue à l'aide d'un CloudFormation modèle AWS. Le modèle crée toutes les configurations et ressources requises pour appliquer le chiffrement. Ces ressources incluent une configuration initiale, un contrôle préventif créé par une EventBridge règle Amazon et une fonction AWS Lambda.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorisations pour déployer le CloudFormation modèle et ses ressources

Limites

Ce contrôle de sécurité est régional. Vous devez déployer le contrôle de sécurité dans chaque région AWS où vous souhaitez configurer l'application du chiffrement dans AWS Glue.

Architecture

Pile technologique cible

- Amazon CloudWatch Logs (depuis AWS Lambda)
- EventBridge Règle Amazon
- CloudFormation pile AWS
- AWS CloudTrail
- Rôle et politique gérés par AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)
- Alias AWS KMS
- Fonction AWS Lambda
- AWS Systems Manager Parameter Store

Architecture cible

Le schéma suivant montre comment automatiser l'application du chiffrement dans AWS Glue.

Le schéma suivant illustre le flux de travail suivant :

1. Un CloudFormation modèle crée toutes les ressources, y compris la configuration initiale et le contrôle de détection pour l'application du chiffrement dans AWS Glue.
2. Une EventBridge règle détecte un changement d'état dans la configuration de chiffrement.
3. Une fonction Lambda est invoquée à des fins d'évaluation et de journalisation via CloudWatch Logs. En cas de détection de non-conformité, le magasin de paramètres est restauré avec un Amazon Resource Name (ARN) pour une clé AWS KMS. L'état de conformité du service est rétabli lorsque le chiffrement est activé.

Automatisation et évolutivité

Si vous utilisez AWS Organizations, vous pouvez utiliser AWS CloudFormation StackSets pour déployer ce modèle sur plusieurs comptes où vous souhaitez activer l'application du chiffrement dans AWS Glue.

Outils

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres comptes AWS.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS vous CloudTrail aide à activer l'audit opérationnel et des risques, la gouvernance et la conformité de votre compte AWS.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.

- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Systems Manager vous aide à gérer vos applications et votre infrastructure exécutées dans le cloud AWS. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos ressources AWS en toute sécurité à grande échelle.

Code

Le code de ce modèle est disponible dans le référentiel GitHub aws-custom-guardrail-event-driven.

Bonnes pratiques

AWS Glue prend en charge le chiffrement des données au repos pour créer des tâches dans AWS Glue et développer des scripts à l'aide de points de terminaison de développement.

Tenez compte des meilleures pratiques suivantes :

- Configurez les tâches ETL et les points de terminaison de développement pour utiliser les clés AWS KMS afin d'écrire des données chiffrées au repos.
- Chiffrez les métadonnées stockées dans le catalogue de données AWS Glue à l'aide de clés que vous gérez via AWS KMS.
- Utilisez les clés AWS KMS pour chiffrer les signets de tâches et les journaux générés par les robots d'exploration et les tâches ETL.

Épopées

Lancez le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Téléchargez le `aws-custom-guardrail-`	Architecte du cloud

Tâche	Description	Compétences requises
	`event-driven.yaml` modèle depuis le GitHub référentiel, puis déployez-le. L'`CREATE_COMPLETE` état indique que votre modèle a été déployé avec succès. **Note** Le modèle ne nécessite aucun paramètre d'entrée.	

Vérifiez les paramètres de chiffrement dans AWS Glue

Tâche	Description	Compétences requises
Vérifiez les configurations clés d'AWS KMS.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la console AWS Glue. 2. Dans le volet de navigation, sous Catalogue de données, sélectionnez Paramètres du catalogue. 3. Vérifiez que les paramètres de chiffrement des métadonnées et de chiffrement des mots de passe de connexion sont marqués et configurés pour être utilisés. `KMSKeyGlue`	Architecte du cloud

Testez l'application du chiffrement

Tâche	Description	Compétences requises
Identifiez le paramètre de chiffrement dans CloudFormation.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la CloudFormation console. 2. Dans le volet de navigation, choisissez Stacks, puis choisissez votre stack. 3. Sélectionnez l'onglet Ressources. 4. Dans le tableau Ressources, recherchez le paramètre de chiffrement par ID logique.	Architecte du cloud
Passez l'infrastructure provisionnée à un état non conforme.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la console AWS Glue. 2. Dans le volet de navigation, sous Catalogue de données, sélectionnez Paramètres du catalogue. 3. Décochez la case Chiffrement des métadonnées. 4. Décochez la case Chiffrer les mots de passe de connexion. 5. Choisissez Enregistrer. 6. Actualisez la console AWS Glue.	Architecte du cloud

Tâche	Description	Compétences requises
	Le garde-corps détecte l'état non conforme dans AWS Glue une fois que vous avez décoché les cases à cocher, puis applique la conformité en corrigeant automatiquement la mauvaise configuration du chiffrement. Par conséquent, les cases de chiffrement doivent à nouveau être cochées après avoir actualisé la page.	

Ressources connexes

- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail (CloudWatch documentation Amazon)
- Configuration du chiffrement dans AWS Glue (documentation AWS Glue)

Créez un pipeline de données pour ingérer, transformer et analyser les données Google Analytics à l'aide du kit de AWS DataOps développement

Créée par Anton Kukushkin (AWS) et Rudy Puig (AWS)

Récapitulatif

Ce modèle décrit comment créer un pipeline de données pour ingérer, transformer et analyser les données de Google Analytics à l'aide du kit de AWS DataOps développement (AWS DDK) et d'autres outils. Services AWS Le AWS DDK est un framework de développement open source qui vous aide à créer des flux de travail de données et une architecture de données moderne. AWS L'un des principaux objectifs du AWS DDK est de vous faire économiser le temps et les efforts généralement consacrés aux tâches de pipeline de données exigeantes en main-d'œuvre, telles que l'orchestration de pipelines, la création d'infrastructures et la création de l' DevOps infrastructure sous-jacente. Vous pouvez déléguer ces tâches fastidieuses à AWS DDK afin de pouvoir vous concentrer sur l'écriture de code et d'autres activités à forte valeur ajoutée.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un AppFlow connecteur Amazon pour Google Analytics, configuré
- Python et pip (le gestionnaire de paquets de Python)
- Git, installé et configuré
- AWS Command Line Interface (AWS CLI), installé et configuré
- AWS Cloud Development Kit (AWS CDK), installé

Versions du produit

- Python 3.7 ou version ultérieure
- pip 9.0.3 ou version ultérieure

Architecture

Pile technologique

- Amazon AppFlow
- Amazon Athena
- Amazon CloudWatch
- Amazon EventBridge
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Queue Service (Amazon SQS)
- AWS DataOps Kit de développement (AWS DDK)
- AWS Lambda

Architecture cible

Le schéma suivant montre le processus piloté par les événements qui ingère, transforme et analyse les données de Google Analytics.

Le schéma suivant illustre le flux de travail suivant :

1. Une règle d'événement CloudWatch planifié d'Amazon invoque Amazon AppFlow.
2. Amazon AppFlow ingère les données de Google Analytics dans un compartiment S3.
3. Une fois les données ingérées par le compartiment S3, les notifications d'événements EventBridge sont générées, capturées par une règle CloudWatch Events, puis placées dans une file d'attente Amazon SQS.
4. Une fonction Lambda consomme les événements de la file d'attente Amazon SQS, lit les objets S3 respectifs, transforme les objets au format Apache Parquet, écrit les objets transformés dans le compartiment S3, puis crée ou met à jour AWS Glue Data Catalog la définition de la table.
5. Une requête Athena s'exécute sur la table.

Outils

AWS outils

- Amazon AppFlow est un service d'intégration entièrement géré qui vous permet d'échanger des données en toute sécurité entre des applications SaaS (Software as a Service).
- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, AWS Lambda des fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Cloud Development Kit (AWS CDK)est un framework permettant de définir l'infrastructure cloud dans le code et de la provisionner via AWS CloudFormation ce dernier.
- AWS DataOps Le kit de développement (AWS DDK) est un framework de développement open source qui vous aide à créer des flux de travail de données et une architecture de données moderne. AWS

Code

Le code de ce modèle est disponible dans le kit de GitHub AWS DataOps développement (AWS DDK) et dans les référentiels d'analyse des données Google Analytics avec Amazon AppFlow, Amazon Athena AWS DataOps et Development Kit.

Épopées

Préparez l'environnement

Tâche	Description	Compétences requises
Clonez le code source.	Pour cloner le code source, exécutez la commande suivante : `git clone https://github.com/aws-samples/aws-ddk-examples.git`	DevOps ingénieur
Créez un environnement virtuel.	Accédez au répertoire du code source, puis exécutez la commande suivante pour créer un environnement virtuel : `cd google-analytics-data-using-appflow/python && python3 -m venv .venv`	DevOps ingénieur
Installez les dépendances.	Pour activer l'environnement virtuel et installer les dépendances, exécutez la commande suivante : `source .venv/bin/activate && pip install -r requirements.txt`	DevOps ingénieur

Déployez l'application qui utilise votre pipeline de données

Tâche	Description	Compétences requises
Démarrez l'environnement.	1. Vérifiez que le AWS CLI est configuré avec des informations d'identification valides pour votre Compte AWS. Pour plus d'informations, consultez la section Utilisation de profils nommés dans la AWS CLI documentation. 2. Exécutez la commande `cdk bootstrap --profile [AWS_PROFILE] .`	DevOps ingénieur
Déployez les données.	Pour déployer le pipeline de données, exécutez la `cdk deploy --profile [AWS_PROFILE]` commande.	DevOps ingénieur

Test du déploiement

Tâche	Description	Compétences requises
Validez l'état de la pile.	1. Ouvrez la AWS CloudFormation console. 2. Sur la page Stacks, vérifiez que le statut de la pile `DdkAppflowAthenaStack estCREATE_COMPLETE .`	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Le déploiement échoue lors de la création d'une `AWS::AppFlow::Flow` ressource et le message d'erreur suivant s'affiche : `Connector Profile with name ga-connection does not exist`	Confirmez que vous avez créé un AppFlow connecteur Amazon pour Google Analytics et que vous l'avez nommé`ga-connection` . Pour obtenir des instructions, consultez Google Analytics dans la AppFlow documentation Amazon.

Ressources connexes

- AWS DataOps Kit de développement (AWS DDK) (GitHub)
- AWS Exemples de SDK () GitHub

Informations supplémentaires

AWS Les pipelines de données DDK sont composés d'une ou de plusieurs étapes. Dans les exemples de code suivants, vous les utilisez `AppFlowIngestionStage` pour ingérer des données provenant de Google Analytics, `SqsToLambdaStage` pour gérer la transformation des données et `AthenaSQLStage` pour exécuter la requête Athena.

Tout d'abord, les étapes de transformation et d'ingestion des données sont créées, comme le montre l'exemple de code suivant :

```
        appflow_stage = AppFlowIngestionStage(
            self,
            id="appflow-stage",
            flow_name=flow.flow_name,
        )
        sqs_lambda_stage = SqsToLambdaStage(
            self,
            id="lambda-stage",
            lambda_function_props={
                "code": Code.from_asset("./ddk_app/lambda_handlers"),
                "handler": "handler.lambda_handler",
```

```
                "layers": [
                    LayerVersion.from_layer_version_arn(
                        self,
                        id="layer",
                        layer_version_arn=f"arn:aws:lambda:
{self.region}:336392948345:layer:AWSDataWrangler-Python39:1",
                    )
                ],
                "runtime": Runtime.PYTHON_3_9,
            },
        )
        # Grant lambda function S3 read & write permissions
        bucket.grant_read_write(sqs_lambda_stage.function)
        # Grant Glue database & table permissions
        sqs_lambda_stage.function.add_to_role_policy(
            self._get_glue_db_iam_policy(database_name=database.database_name)
        )
        athena_stage = AthenaSQLStage(
            self,
            id="athena-sql",
            query_string=[
                (
                    "SELECT year, month, day, device, count(user_count) as cnt "
                    f"FROM {database.database_name}.ga_sample "
                    "GROUP BY year, month, day, device "
                    "ORDER BY cnt DESC "
                    "LIMIT 10; "
                )
            ],
            output_location=Location(
                bucket_name=bucket.bucket_name, object_key="query-results/"
            ),
            additional_role_policy_statements=[
                self._get_glue_db_iam_policy(database_name=database.database_name)
            ],
        )
```

Ensuite, la `DataPipeline` construction est utilisée pour « relier » les étapes entre elles en utilisant des EventBridge règles, comme le montre l'exemple de code suivant :

```
        (
            DataPipeline(self, id="ingestion-pipeline")
            .add_stage(
```

```
                stage=appflow_stage,
                override_rule=Rule(
                    self,
                    "schedule-rule",
                    schedule=Schedule.rate(Duration.hours(1)),
                    targets=appflow_stage.targets,
                ),
            )
            .add_stage(
                stage=sqs_lambda_stage,
                # By default, AppFlowIngestionStage stage emits an event after the flow
run finishes successfully
                # Override rule below changes that behavior to call the the stage when
data lands in the bucket instead
                override_rule=Rule(
                    self,
                    "s3-object-created-rule",
                    event_pattern=EventPattern(
                        source=["aws.s3"],
                        detail={
                            "bucket": {"name": [bucket.bucket_name]},
                            "object": {"key": [{"prefix": "ga-data"}]},
                        },
                        detail_type=["Object Created"],
                    ),
                    targets=sqs_lambda_stage.targets,
                ),
            )
            .add_stage(stage=athena_stage)
        )
```

Pour d'autres exemples de code, consultez le GitHub [référentiel Analyse des données Google Analytics avec Amazon AppFlow, Amazon Athena et AWS DataOps le référentiel Development Kit](#).

Créez un pipeline de traitement vidéo à l'aide d'Amazon Kinesis Video Streams et d'AWS Fargate

Créée par Piotr Chotkowski (AWS) et Pushparaju Thangavel (AWS)

Récapitulatif

Ce modèle montre comment utiliser Amazon Kinesis Video Streams et AWS Fargate pour extraire des images d'un flux vidéo et les stocker sous forme de fichiers image pour un traitement ultérieur dans Amazon Simple Storage Service (Amazon S3).

Le modèle fournit un exemple d'application sous la forme d'un projet Java Maven. Cette application définit l'infrastructure AWS à l'aide du kit AWS Cloud Development Kit (AWS CDK). La logique de traitement des trames et les définitions de l'infrastructure sont écrites dans le langage de programmation Java. Vous pouvez utiliser cet exemple d'application comme base pour développer votre propre pipeline de traitement vidéo en temps réel ou pour créer l'étape de prétraitement vidéo d'un pipeline d'apprentissage automatique.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Kit de développement Java SE (JDK) 11, installé
- Apache Maven, installé
- Kit de développement cloud AWS (AWS CDK), installé
- Interface de ligne de commande AWS (AWS CLI) version 2, installée
- Docker (nécessaire pour créer des images Docker à utiliser dans les définitions de tâches AWS Fargate), installé

Limites

Ce modèle est conçu comme une preuve de concept ou comme base pour un développement ultérieur. Il ne doit pas être utilisé sous sa forme actuelle dans les déploiements de production.

Versions du produit

- Ce modèle a été testé avec la version 1.77.0 d'AWS CDK (voir les versions d'AWS CDK)
- JDK 11
- Version 2 de l'interface de ligne de commande AWS

Architecture

Pile technologique cible

- Amazon Kinesis Video Streams
- Tâche AWS Fargate
- File d'attente Amazon Simple Queue Service (Amazon SQS)
- Compartiment Amazon S3

Architecture cible

L'utilisateur crée un flux vidéo Kinesis, télécharge une vidéo et envoie un message JSON contenant des détails sur le flux vidéo Kinesis d'entrée et le bucket S3 de sortie vers une file d'attente SQS. AWS Fargate, qui exécute l'application principale dans un conteneur, extrait le message de la file d'attente SQS et commence à extraire les cadres. Chaque image est enregistrée dans un fichier image et stockée dans le compartiment S3 cible.

Automatisation et évolutivité

L'exemple d'application peut être redimensionné à la fois horizontalement et verticalement au sein d'une même région AWS. La mise à l'échelle horizontale peut être réalisée en augmentant le nombre de tâches AWS Fargate déployées qui sont lues depuis la file d'attente SQS. La mise à l'échelle verticale peut être réalisée en augmentant le nombre de fils de partage d'images et de publication d'images dans l'application. Ces paramètres sont transmis en tant que variables d'environnement à l'application dans la définition de la QueueProcessingFargateServiceressource dans le CDK AWS. En raison de la nature du déploiement de la pile AWS CDK, vous pouvez déployer cette application dans plusieurs régions et comptes AWS sans effort supplémentaire.

Outils

Outils

- AWS CDK est un framework de développement logiciel permettant de définir votre infrastructure et vos ressources cloud à l'aide de langages de programmation tels que Python TypeScript JavaScript, Java et C#/Net.
- Amazon Kinesis Video Streams est un service AWS entièrement géré que vous pouvez utiliser pour diffuser des vidéos en direct depuis des appareils vers le cloud AWS, ou créer des applications pour le traitement vidéo en temps réel ou l'analyse vidéo par lots.
- AWS Fargate est un moteur de calcul sans serveur pour les conteneurs. Fargate élimine le besoin de provisionner et de gérer des serveurs, et vous permet de vous concentrer sur le développement de vos applications.
- Amazon S3 est un service de stockage d'objets qui offre évolutivité, disponibilité des données, sécurité et performances.
- Amazon SQS est un service de mise en file d'attente de messages entièrement géré qui vous permet de découpler et de dimensionner les microservices, les systèmes distribués et les applications sans serveur.

Code

- Un fichier .zip de l'exemple de projet d'application (`frame-splitter-code.zip`) est joint.

Épopées

Déployer l'infrastructure

Tâche	Description	Compétences requises
Lancez le démon Docker.	Démarrez le daemon Docker sur votre système local. L'AWS CDK utilise Docker pour créer l'image utilisée dans la tâche AWS Fargate. Vous devez exécuter Docker avant de passer à l'étape suivante.	Développeur, DevOps ingénieur
Générez le projet.	Téléchargez l'`frame-splitter-code` exemple	Développeur, DevOps ingénieur

Tâche	Description	Compétences requises
	d'application (ci-joint) et extrayez son contenu dans un dossier sur votre ordinateur local. Avant de déployer l'infrastructure, vous devez créer le projet Java Maven. À l'invite de commande, accédez au répertoire racine du projet et créez le projet en exécutant la commande suivante : `mvn clean install`	
Démarrez le kit AWS CDK.	(Utilisateurs du CDK AWS pour la première fois uniquement) Si c'est la première fois que vous utilisez le kit AWS CDK, vous devrez peut-être démarrer l'environnement en exécutant la commande de la CLI AWS : `cdk bootstrap --profile "$AWS_PROFILE_NAME"` où `$AWS_PROFILE_NAME` contient le nom du profil AWS issu de vos informations d'identification AWS. Vous pouvez également supprimer ce paramètre pour utiliser le profil par défaut. Pour plus d'informations, consultez la documentation AWS CDK.	Développeur, DevOps ingénieur

Tâche	Description	Compétences requises
Déployez la pile AWS CDK.	Au cours de cette étape, vous créez les ressources d'infrastructure requises (file d'attente SQS, compartim ent S3, définition de tâche AWS Fargate) dans votre compte AWS, vous créez l'image Docker requise pour la tâche AWS Fargate et vous déployez l'application. À l'invite de commande, accédez au répertoire racine du projet et exécutez la commande suivante : `cdk deploy --profile "$AWS_PROFILE_NAME" --all` où `$AWS_PROFILE_NAME` contient le nom du profil AWS issu de vos informations d'identification AWS. Vous pouvez également supprimer ce paramètre pour utiliser le profil par défaut. Confirmez le déploiement. Notez les valeurs QueueUrlet Bucket indiquées dans le résultat du déploiement du CDK ; vous en aurez besoin ultérieur ement. Le CDK AWS crée les actifs, les télécharge sur votre compte AWS et crée toutes les ressources de	Développeur, DevOps ingénieur

Tâche	Description	Compétences requises
	l'infrastructure. Vous pouvez observer le processus de création des ressources dans la CloudFormation console AWS. Pour plus d'informations, consultez la CloudFormation documentation AWS et la documentation AWS CDK.	

Tâche	Description	Compétences requises
Créez un flux vidéo.	Au cours de cette étape, vous allez créer un flux vidéo Kinesis qui servira de flux d'entrée pour le traitemen t vidéo. Assurez-vous que la CLI AWS est installée et configurée. Dans l'AWS CLI, exécutez : `aws kinesisvideo --profile "$AWS_PRO FILE_NAME" create-st ream --stream-name "$STREAM_NAME" --data- retention-in-hours "24"` où `$AWS_PROFILE_NAME` contient le nom du profil AWS issu de vos informati ons d'identification AWS (ou supprimez ce paramètre pour utiliser le profil par défaut) et `$STREAM_NAME` est un nom de flux valide. Vous pouvez également créer un flux vidéo à l'aide de la console Kinesis en suivant les étapes décrites dans la documentation Kinesis Video Streams. Notez le nom de ressource AWS (ARN) du flux créé ; vous en aurez besoin ultérieurement.	Développeur, DevOps ingénieur

Exécutez un exemple

Tâche	Description	Compétences requises
Téléchargez la vidéo sur le stream.	Dans le dossier de projet de l'exemple d'`frame-splitter-code` application, ouvrez le `ProcessingTaskTest.java` fichier qui s'y `src/test/java/amazon/awscdk/examples/splitter` trouve. Remplacez les `streamName` variables `profileName` et par les valeurs que vous avez utilisées dans les étapes précédentes. Pour télécharger l'exemple de vidéo dans le flux vidéo Kinesis que vous avez créé à l'étape précédente, exécutez : `amazon.awscdk.examples.splitter.ProcessingTaskTest#testExample test` Vous pouvez également télécharger votre vidéo en utilisant l'une des méthodes décrites dans la documentation de Kinesis Video Streams.	Développeur, DevOps ingénieur
Lancez le traitement vidéo.	Maintenant que vous avez chargé une vidéo dans le flux vidéo Kinesis, vous pouvez	Développeur, DevOps ingénieur

Tâche	Description	Compétences requises

	commencer à la traiter. Pour lancer la logique de traitement, vous devez envoyer un message contenant des informations détaillées à la file d'attente SQS créée par le CDK AWS lors du déploiement. Pour envoyer un message à l'aide de l'AWS CLI, exécutez :
	`aws sqs --profile "$AWS_PROFILE_NAME" send-message --queue-url QUEUE_URL --message-body MESSAGE`
	where `$AWS_PROFILE_NAME` contient le nom du profil AWS issu de vos informations d'identification AWS (supprimez ce paramètre pour utiliser le profil par défaut), `QUEUE_URL` est la QueueUrlvaleur de la sortie du CDK AWS et `MESSAGE` est une chaîne JSON au format suivant :
	`{ "streamARN": "STREAM_ARN", "bucket": "BUCKET_NAME", "s3Directory": "test-output" }`	

Tâche	Description	Compétences requises
	où `STREAM_ARN` est l'ARN du flux vidéo que vous avez créé lors d'une étape précédente et `BUCKET_NAME` la valeur du bucket issue de la sortie AWS CDK. L'envoi de ce message lance le traitement vidéo. Vous pouvez également envoyer un message à l'aide de la console Amazon SQS, comme décrit dans la documentation Amazon SQS.	
Visionnez des images des images vidéo.	Vous pouvez voir les images obtenues dans le compartiment de sortie S3, `s3://BUCKET_NAME/test-output` où se `BUCKET_NAME` trouve la valeur du compartiment provenant de la sortie AWS CDK.	Développeur, DevOps ingénieur

Ressources connexes

- Documentation du kit AWS CDK
- Référence de l'API AWS CDK
- Atelier d'introduction à AWS CDK
- Documentation Amazon Kinesis Video Streams
- Exemple : identification d'objets dans des flux vidéo à l'aide de SageMaker
- Exemple : analyse et rendu de fragments Kinesis Video Streams

- Analysez des vidéos en direct à grande échelle en temps réel à l'aide d'Amazon Kinesis Video Streams et d' SageMakerAmazon (article de blog AWS Machine Learning)
- Mise en route d'AWS Fargate

Informations supplémentaires

Choisir un IDE

Nous vous recommandons d'utiliser votre IDE Java préféré pour créer et explorer ce projet.

Nettoyage

Une fois que vous avez terminé d'exécuter cet exemple, supprimez toutes les ressources déployées pour éviter d'encourir des coûts supplémentaires liés à l'infrastructure AWS.

Pour supprimer l'infrastructure et le flux vidéo, utilisez ces deux commandes dans l'AWS CLI :

```
cdk destroy --profile "$AWS_PROFILE_NAME" --all
```

```
aws kinesisvideo --profile "$AWS_PROFILE_NAME" delete-stream --stream-arn "$STREAM_ARN"
```

Vous pouvez également supprimer les ressources manuellement en utilisant la CloudFormation console AWS pour supprimer la CloudFormation pile AWS et la console Kinesis pour supprimer le flux vidéo Kinesis. Notez que `cdk destroy` cela ne supprime pas le compartiment S3 de sortie ni les images des référentiels Amazon Elastic Container Registry (Amazon ECR) (). `aws-cdk/assets` Vous devez les supprimer manuellement.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez un pipeline de services ETL pour charger les données de manière incrémentielle d'Amazon S3 vers Amazon Redshift à l'aide d'AWS Glue

Créée par Rohan Jamadagni (AWS) et Arunabha Datta (AWS)

Récapitulatif

Ce modèle fournit des conseils sur la façon de configurer Amazon Simple Storage Service (Amazon S3) pour des performances optimales en matière de data lake, puis de charger les modifications de données incrémentielles d'Amazon S3 dans Amazon Redshift à l'aide d'AWS Glue, en effectuant des opérations d'extraction, de transformation et de chargement (ETL).

Les fichiers source d'Amazon S3 peuvent avoir différents formats, notamment des valeurs séparées par des virgules (CSV), des fichiers XML et des fichiers JSON. Ce modèle décrit comment utiliser AWS Glue pour convertir les fichiers source dans un format optimisé en termes de coûts et de performances, tel qu'Apache Parquet. Vous pouvez interroger les fichiers Parquet directement depuis Amazon Athena et Amazon Redshift Spectrum. Vous pouvez également charger des fichiers Parquet dans Amazon Redshift, les agréger et partager les données agrégées avec les consommateurs, ou visualiser les données à l'aide d'Amazon. QuickSight

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un compartiment source S3 doté des privilèges appropriés et contenant des fichiers CSV, XML ou JSON.

Hypothèses

- Les fichiers source CSV, XML ou JSON sont déjà chargés dans Amazon S3 et sont accessibles depuis le compte sur lequel AWS Glue et Amazon Redshift sont configurés.
- Les meilleures pratiques relatives au chargement des fichiers, au fractionnement des fichiers, à la compression et à l'utilisation d'un manifeste sont suivies, comme indiqué dans la documentation Amazon Redshift.
- La structure du fichier source n'est pas modifiée.

- Le système source est capable d'ingérer des données dans Amazon S3 en suivant la structure de dossiers définie dans Amazon S3.
- Le cluster Amazon Redshift couvre une seule zone de disponibilité. (Cette architecture est appropriée car AWS Lambda, AWS Glue et Amazon Athena fonctionnent sans serveur.) Pour une haute disponibilité, les instantanés du cluster sont pris à une fréquence régulière.

Limites

- Les formats de fichiers sont limités à ceux actuellement pris en charge par AWS Glue.
- Les rapports en temps réel en aval ne sont pas pris en charge.

Architecture

Pile technologique source

- Compartiment S3 avec fichiers CSV, XML ou JSON

Pile technologique cible

- Lac de données S3 (avec stockage de fichiers Parquet partitionné)
- Amazon Redshift

Architecture cible

Flux de données

Outils

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif. Amazon S3 peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- AWS Lambda — AWS Lambda vous permet d'exécuter du code sans provisionner ni gérer de serveurs. AWS Lambda est un service piloté par des événements ; vous pouvez configurer votre code pour qu'il soit lancé automatiquement à partir d'autres services AWS.

- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données de plusieurs pétaoctets entièrement géré. Avec Amazon Redshift, vous pouvez interroger des pétaoctets de données structurées et semi-structurées dans votre entrepôt de données et votre lac de données à l'aide du SQL standard.
- AWS Glue — AWS Glue est un service ETL entièrement géré qui facilite la préparation et le chargement des données à des fins d'analyse. AWS Glue découvre vos données et stocke les métadonnées associées (par exemple, les définitions de tables et le schéma) dans le catalogue de données AWS Glue. Vos données cataloguées sont immédiatement consultables, peuvent être consultées et sont disponibles pour l'ETL.
- AWS Secrets Manager — AWS Secrets Manager facilite la protection et la gestion centralisée des secrets nécessaires à l'accès aux applications ou aux services. Le service stocke les informations d'identification de base de données, les clés d'API et d'autres secrets, et élimine le besoin de coder en dur les informations sensibles au format texte brut. Secrets Manager propose également une rotation des clés pour répondre aux besoins de sécurité et de conformité. Il intègre une intégration à Amazon Redshift, Amazon Relational Database Service (Amazon RDS) et Amazon DocumentDB. Vous pouvez stocker et gérer les secrets de manière centralisée à l'aide de la console Secrets Manager, de l'interface de ligne de commande (CLI) ou de l'API Secrets Manager et. SDKs
- Amazon Athena — Amazon Athena est un service de requête interactif qui facilite l'analyse des données stockées dans Amazon S3. Athena fonctionne sans serveur et est intégrée à AWS Glue, ce qui lui permet d'interroger directement les données cataloguées à l'aide d'AWS Glue. Athena est dimensionnée de manière élastique pour fournir des performances de requête interactives.

Épopées

Création des compartiments et de la structure de dossiers S3

Tâche	Description	Compétences requises
Analysez la structure des données et leurs attributs dans les systèmes sources.	Effectuez cette tâche pour chaque source de données qui contribue au lac de données Amazon S3.	Ingénieur de données
Définissez la stratégie de partition et d'accès.	Cette stratégie doit être basée sur la fréquence des captures	Ingénieur de données

Tâche	Description	Compétences requises
	de données, le traitement du delta et les besoins de consommation. Assurez-vous que les compartiments S3 ne sont pas ouverts au public et que l'accès est contrôlé uniquement par des politique s spécifiques basées sur les rôles de service. Pour plus d'informations, consultez la documentation Amazon S3.	
Créez des compartiments S3 distincts pour chaque type de source de données et un compartiment S3 distinct par source pour les données traitées (Parquet).	Créez un compartiment distinct pour chaque source, puis créez une structure de dossiers basée sur la fréquence d'ingestion des données du système source, par exemple,`s3://sour ce-system-name/dat e/hour` . Pour les fichiers traités (convertis au format Parquet), créez une structure similaire ; par exemple,`s3:// source-processed- bucket/date/hour` . Pour plus d'informations sur la création de compartiments S3, consultez la documenta tion Amazon S3.	Ingénieur de données

Création d'un entrepôt de données dans Amazon Redshift

Tâche	Description	Compétences requises
Lancez le cluster Amazon Redshift avec les groupes de paramètres et la stratégie de maintenance et de sauvegarde appropriés.	Utilisez le secret de base de données Secrets Manager pour les informations d'identification des utilisateurs administrateurs lors de la création du cluster Amazon Redshift. Pour plus d'informations sur la création et le dimensionnement d'un cluster Amazon Redshift, consultez la documentation Amazon Redshift et le livre blanc Sizing Cloud Data Warehouses.	Ingénieur de données
Créez et attachez le rôle de service IAM au cluster Amazon Redshift.	Le rôle de service AWS Identity and Access Management (IAM) garantit l'accès à Secrets Manager et aux compartiments S3 source. Pour plus d'informations, consultez la documentation AWS sur l'autorisation et l'ajout d'un rôle.	Ingénieur de données
Créez le schéma de base de données.	Suivez les meilleures pratiques d'Amazon Redshift pour la conception des tables. En fonction du cas d'utilisation, choisissez les clés de tri et de distribution appropriées, ainsi que le meilleur codage de compression possible. Pour connaître les meilleure	Ingénieur de données

Tâche	Description	Compétences requises
	s pratiques, consultez la documentation AWS.	
Configurer la gestion de la charge de travail.	Configurez les files d'attente pour la gestion de la charge de travail (WLM), l'accélération des requêtes courtes (SQA) ou le dimensionnement de la simultanéité, en fonction de vos besoins. Pour plus d'informations, consultez la section Implémentation de la gestion de la charge de travail dans la documentation Amazon Redshift.	Ingénieur de données

Création d'un secret dans Secrets Manager

Tâche	Description	Compétences requises
Créez un nouveau secret pour stocker les informations de connexion Amazon Redshift dans Secrets Manager.	Ce secret stocke les informations d'identification de l'utilisateur administrateur ainsi que celles des utilisateurs individuels du service de base de données. Pour obtenir des instructions, consultez la documentation de Secrets Manager. Choisissez Amazon Redshift Cluster comme type de secret. De plus, sur la page Rotation secrète, activez la rotation. Cela créera l'utilisateur approprié dans le cluster Amazon Redshift et effectuera	Ingénieur de données

Tâche	Description	Compétences requises
	une rotation des secrets clés à des intervalles définis.	
Créez une politique IAM pour restreindre l'accès à Secrets Manager.	Limitez l'accès à Secrets Manager aux seuls administr ateurs Amazon Redshift et à AWS Glue.	Ingénieur de données

Configurer AWS Glue

Tâche	Description	Compétences requises
Dans le catalogue de données AWS Glue, ajoutez une connexion pour Amazon Redshift.	Pour obtenir des instructions, consultez la documentation AWS Glue.	Ingénieur de données
Créez et attachez un rôle de service IAM pour AWS Glue afin d'accéder à Secrets Manager, Amazon Redshift et aux compartiments S3.	Pour plus d'informations, consultez la documentation AWS Glue.	Ingénieur de données
Définissez le catalogue de données AWS Glue pour la source.	Cette étape implique la création d'une base de données et des tables requises dans le catalogue de données AWS Glue. Vous pouvez utiliser un robot pour cataloguer les tables de la base de données AWS Glue ou les définir comme des tables externes Amazon Athena. Vous pouvez également accéder aux tables	Ingénieur de données

Tâche	Description	Compétences requises
	externes définies dans Athena via le catalogue de données AWS Glue. Consultez la documentation AWS pour plus d'informations sur la définition du catalogue de données et la création d'une table externe dans Athena.	
Créez une tâche AWS Glue pour traiter les données sources.	La tâche AWS Glue peut être un shell Python ou servir PySpark à normaliser, dédupliquer et nettoyer les fichiers de données sources. Pour optimiser les performances et éviter d'avoir à interroger l'intégralité du compartiment source S3, partitionnez le compartiment S3 par date, ventilé par année, mois, jour et heure sous forme de prédicat push down pour la tâche AWS Glue. Pour plus d'informations, consultez la documentation AWS Glue. Chargez les données traitées et transformées dans les partitions du bucket S3 traitées au format Parquet. Vous pouvez consulter les dossiers du parquet auprès d'Athéna.	Ingénieur de données

Tâche	Description	Compétences requises
Créez une tâche AWS Glue pour charger des données dans Amazon Redshift.	La tâche AWS Glue peut être un shell Python ou une tâche consistant PySpark à charger les données en les insérant, puis en les actualisant complètement. Pour plus de détails, consultez la documentation d'AWS Glue et la section Informations supplémentaires.	Ingénieur de données
(Facultatif) Planifiez les tâches AWS Glue en utilisant des déclencheurs si nécessaire.	Le chargement de données incrémentiel est principal ement provoqué par un événement Amazon S3 qui amène une fonction AWS Lambda à appeler la tâche AWS Glue. Utilisez la planifica tion basée sur des déclenche urs AWS Glue pour tous les chargements de données nécessitant une planification basée sur le temps plutôt qu'une planification basée sur des événements.	Ingénieur de données

Création d’une fonction Lambda

Tâche	Description	Compétences requises
Créez et attachez un rôle lié à un service IAM pour qu'AWS Lambda accède aux	Créez un rôle lié à un service IAM pour AWS Lambda avec une politique pour lire les objets et les compartiments	Ingénieur de données

Tâche	Description	Compétences requises
compartiments S3 et à la tâche AWS Glue.	Amazon S3, et une politique pour accéder à l'API AWS Glue pour démarrer une tâche AWS Glue. Pour plus d'informations, consultez le centre de connaissances.	
Créez une fonction Lambda pour exécuter la tâche AWS Glue en fonction de l'événement Amazon S3 défini.	La fonction Lambda doit être initiée par la création du fichier manifeste Amazon S3. La fonction Lambda doit transmettre l'emplacement du dossier Amazon S3 (par exemple, source_bucket/year/month/date/hour) à la tâche AWS Glue en tant que paramètre. La tâche AWS Glue utilisera ce paramètre comme prédicat pushdown afin d'optimiser l'accès aux fichiers et les performances de traitement des tâches. Pour plus d'informations, consultez la documentation AWS Glue.	Ingénieur de données

Tâche	Description	Compétences requises
Créez un événement d'objet Amazon S3 PUT pour détecter la création d'un objet et appelez la fonction Lambda correspondante.	L'événement d'objet Amazon S3 PUT ne doit être initié que par la création du fichier manifeste. Le fichier manifeste contrôle la simultanéité de la fonction Lambda et de la tâche AWS Glue, et traite le chargement par lots au lieu de traiter les fichiers individuels qui arrivent dans une partition spécifique du compartiment source S3. Pour plus d'informations, consultez la documentation Lambda.	Ingénieur de données

Ressources connexes

- Documentation Amazon S3
- Documentation d'AWS Glue
- Documentation Amazon Redshift
- AWS Lambda
- Amazon Athena
- AWS Secrets Manager

Informations supplémentaires

Approche détaillée pour l'amélioration et l'actualisation complète

Upsert : Cela concerne les ensembles de données qui nécessitent une agrégation historique, selon le cas d'utilisation métier. Suivez l'une des approches décrites dans la section Mise à jour et insertion de nouvelles données (documentation Amazon Redshift) en fonction des besoins de votre entreprise.

Actualisation complète : cela concerne les petits ensembles de données qui ne nécessitent pas d'agrégations historiques. Suivez l'une des approches suivantes :

1. Tronquez le tableau Amazon Redshift.
2. Charger la partition actuelle depuis la zone de transit

ou :

1. Créez une table temporaire avec les données de partition actuelles.
2. Supprimez la table Amazon Redshift cible.
3. Renommez la table temporaire en table cible.

Créez un maillage de données d'entreprise avec Amazon DataZone AWS CDK, et AWS CloudFormation

Créée par Dhrubajyoti Mukherjee (AWS), Adjoa Taylor (AWS), Ravi Kumar (AWS) et Weizhou Sun (AWS)

Récapitulatif

Sur Amazon Web Services (AWS), les clients savent que les données sont essentielles pour accélérer l'innovation et créer de la valeur commerciale pour leur entreprise. Pour gérer ces données massives, vous pouvez adopter une architecture décentralisée telle que le maillage de données. Une architecture de maillage de données facilite la réflexion sur les produits, un état d'esprit qui prend en compte les clients, les objectifs et le marché. Le maillage des données permet également d'établir un modèle de gouvernance fédéré qui fournit un accès rapide et sécurisé à vos données.

Stratégies pour créer une solution d'entreprise basée sur le maillage de données AWS explique comment utiliser le cadre de stratégie de maillage de données pour formuler et mettre en œuvre une stratégie de maillage de données pour votre organisation. En utilisant le Data Mesh Strategy Framework, vous pouvez optimiser l'organisation des équipes et leurs interactions afin d'accélérer votre parcours vers le maillage des données.

Ce document fournit des conseils sur la manière de créer un maillage de données d'entreprise avec Amazon DataZone. Amazon DataZone est un service de gestion des données destiné au catalogage, à la découverte, au partage et à la gestion des données stockées auprès de sources tierces AWS, sur site ou auprès de sources tierces. Le modèle inclut des artefacts de code qui vous aident à déployer l'infrastructure de solution de données basée sur un maillage de données à l'aide de et. AWS Cloud Development Kit (AWS CDK) AWS CloudFormation Ce modèle est destiné aux architectes et DevOps ingénieurs du cloud.

Pour plus d'informations sur les objectifs de ce modèle et l'étendue de la solution, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Au moins deux actifs Comptes AWS : un pour le compte de gouvernance central et un autre pour le compte membre

- AWS informations d'identification d'administrateur pour le compte de gouvernance central de votre environnement de développement
- AWS Command Line Interface (AWS CLI) installé pour gérer votre Services AWS depuis la ligne de commande
- Node.js et Node Package Manager (npm) installés pour gérer les applications AWS CDK
- AWS CDK Boîte à outils installée globalement dans votre environnement de développement à l'aide de npm, pour synthétiser et déployer des applications AWS CDK

```
npm install -g aws-cdk
```

- Python version 3.12 installé dans votre environnement de développement
- TypeScript installé dans votre environnement de développement ou installé globalement à l'aide du compilateur npm :

```
npm install -g typescript
```

- Docker installé dans votre environnement de développement
- Un système de contrôle de version tel que Git pour maintenir le code source de la solution (recommandé)
- Un environnement de développement intégré (IDE) ou un éditeur de texte compatible avec Python et TypeScript (fortement recommandé)

Limites

- La solution a été testée uniquement sur des machines exécutant Linux ou macOS.
- Dans la version actuelle, la solution ne prend pas en charge l'intégration d'Amazon DataZone et AWS IAM Identity Center par défaut. Toutefois, vous pouvez le configurer pour prendre en charge cette intégration.

Versions du produit

- Version 3.12 de Python

Architecture

Le schéma suivant montre une architecture de référence de maillage de données. L'architecture est basée sur Amazon DataZone et utilise Amazon Simple Storage Service (Amazon S3) AWS Glue Data Catalog et comme source de données. La méthode Services AWS que vous utilisez avec Amazon DataZone dans le cadre de la mise en œuvre de votre maillage de données peut varier en fonction des exigences de votre organisation.

1. Dans les comptes des producteurs, les données brutes sont soit adaptées à la consommation sous leur forme actuelle, soit transformées pour la consommation par utilisation AWS Glue. Les métadonnées techniques des données sont stockées dans Amazon S3 et sont évaluées à l'aide d'un explorateur de AWS Glue données. La qualité des données est mesurée à l'aide de la qualitéAWS Glue des données. La base de données source du catalogue de données est enregistrée en tant que ressource dans le DataZone catalogue Amazon. Le DataZone catalogue Amazon est hébergé dans le compte de gouvernance central à l'aide des tâches de source de DataZone données Amazon.
2. Le compte de gouvernance central héberge le DataZone domaine Amazon et le portail de DataZone données Amazon. Les producteurs Comptes AWS de données et les consommateurs sont associés au DataZone domaine Amazon. Les DataZone projets Amazon des producteurs et des consommateurs de données sont organisés dans les unités de DataZone domaine Amazon correspondantes.
3. Les utilisateurs finaux des actifs de données se connectent au portail de DataZone données Amazon à l'aide de leurs informations d'identification AWS Identity and Access Management (IAM) ou de leur authentification unique (avec intégration via IAM Identity Center). Ils recherchent, filtrent et consultent les informations sur les actifs (par exemple, les informations sur la qualité des données ou les métadonnées commerciales et techniques) dans le catalogue de DataZone données Amazon.
4. Une fois qu'un utilisateur final a trouvé la ressource de données qu'il souhaite, il utilise la fonctionnalité DataZone d'abonnement Amazon pour demander l'accès. Le propriétaire des données de l'équipe de production reçoit une notification et évalue la demande d'abonnement sur le portail de DataZone données Amazon. Le propriétaire des données approuve ou rejette la demande d'abonnement en fonction de sa validité.
5. Une fois la demande d'abonnement acceptée et traitée, l'actif est accessible sur le compte du consommateur pour les activités suivantes :
   - Développement de modèles AI/ML à l'aide d'Amazon AI SageMaker

- Analyses et rapports à l'aide d'Amazon Athena et Amazon QuickSight

Outils

Services AWS

- Amazon Athena est un service de requêtes interactif qui vous permet d'analyser les données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du langage SQL standard.
- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- Amazon DataZone est un service de gestion des données qui vous permet de cataloguer, de découvrir, de partager et de gérer les données stockées dans des sources tierces AWS, sur site et dans des sources tierces.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique.
- Amazon SageMaker AI est un service géré d'apprentissage automatique (ML) qui vous aide à créer et à former des modèles de machine learning, puis à les déployer dans un environnement hébergé prêt pour la production.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

La solution est disponible dans le référentiel GitHub data-mesh-datazone-cdk-cloudformation.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le dépôt, exécutez la commande suivante dans votre environnement de développement local (Linux ou macOS) : `git clone https://github.com/aws-samples/data-mesh-datazone-cdk-cloudformation`	Architecte cloud, DevOps ingénieur

Création de l'environnement	Pour créer l'environnement virtuel Python, exécutez les commandes suivantes :
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip install -r requirements.txt`
		Architecte cloud, DevOps ingénieur

Démarrez le compte.	Pour démarrer le compte de gouvernance central à l'aide de AWS CDK, exécutez la commande suivante : `cdk bootstrap aws://<GOVERNANCE_ACCOUNT_ID>/<AWS_REGION>`	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	Connectez-vous au AWS Management Console, ouvrez la console centrale du compte de gouvernance et obtenez le nom de ressource Amazon (ARN) du rôle AWS CDK d'exécution.	
Construisez le `DzDataMeshMemberStackSet.yaml` fichier.	Pour créer le `DzDataMeshMemberStackSet.yaml` fichier, à partir du répertoire racine du dépôt, lancez le script bash suivant : `./lib/scripts/create_dz_data_mesh_member_stack_set.sh`	Architecte cloud, DevOps ingénieur
Confirmez la création du modèle.	Assurez-vous que le fichier AWS CloudFormation modèle est créé à cet `lib/cfn-templates/DzDataMeshMemberStackSet.yaml` emplacement.	Architecte cloud, DevOps ingénieur

Déployer des ressources dans le compte de gouvernance central

Tâche	Description	Compétences requises
Modifiez la configuration.	Dans le `config/Config.ts` fichier, modifiez les paramètres suivants :	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

	`DZ_APPLICATION_NAME - Name of the application.`
	`DZ_STAGE_NAME - Name of the stage.`
	`DZ_DOMAIN_NAME - Name of the Amazon DataZone domain`
	`DZ_DOMAIN_DESCRIPTION - Description of the Amazon DataZone domain`
	`DZ_DOMAIN_TAG - Tag of the Amazon DataZone domain`
	`DZ_ADMIN_PROJECT_NAME - Name of the Amazon DataZone project for administrators`
	`DZ_ADMIN_PROJECT_DESCRIPTION - Description of the Amazon DataZone project for administrators`
	`CDK_EXEC_ROLE_ARN - ARN of the cdk execution role`
	`DZ_ADMIN_ROLE_ARN - ARN of the administrator role`
	
	Laissez les paramètres restants vides.	

Tâche	Description	Compétences requises
Mettez à jour la configuration du DataZone glossaire Amazon.	Pour mettre à jour la configuration du DataZone glossaire Amazon dans le `lib/utils/glossary_config.json` fichier, utilisez l'exemple de configuration suivant : `{ "GlossaryName": "PII Data", "GlossaryDescription": "If data source contains PII attributes", "GlossaryTerms": [{ "Name": "Yes", "ShortDescription": "Yes", "LongDescription": "Yes Glossary Term" }, { "Name": "No", "ShortDescription": "No", "LongDescription": "No Glossary Term" } ] }`	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
Mettez à jour la configuration du formulaire de DataZone métadonnées Amazon.	Pour mettre à jour la configuration du formulaire de DataZone métadonnées Amazon dans le`lib/utils/metadata_form_config.json file` , utilisez l'exemple de configuration suivant : `{ "FormName": "ScheduleDataRefresh", "FormDescription": "Form for data refresh schedule", "FormSmithyModel": "@amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\nstructure ScheduleDataRefresh {\n @documentation(\"Schedule of Data Refresh\")\n @required\n @amazon.datazone#searchable\n @amazon.datazone#displayname(defaultName: \"Data Refresh Schedule\")\n data_refresh_schedule: String\n}" }`	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

Exportez les AWS informations d'identification.	Pour exporter les AWS informations d'identification vers votre environnement de développement pour le rôle IAM avec des autorisations administratives, utilisez le format suivant :
	`export AWS_ACCESS_KEY_ID=`
	`export AWS_SECRET_ACCESS_KEY=`
	`export AWS_SESSION_TOKEN=`
		Architecte cloud, DevOps ingénieur

Synthétisez le modèle.	Pour synthétiser le AWS CloudFormation modèle, exécutez la commande suivante : `npx cdk synth`	Architecte cloud, DevOps ingénieur
Déployez la solution.	Pour déployer la solution, exécutez la commande suivante : `npx cdk deploy --all`	Architecte cloud, DevOps ingénieur

Configurer les nouveaux comptes de membres

Tâche	Description	Compétences requises
Déployez le modèle.	Déployez le AWS CloudFormation modèle situé `lib/cfn-`	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	`templates/DzDataMeshCfnStackSetExecutionRole.yaml` dans le compte du membre avec les paramètres d'entrée suivants : • `GovernanceAccountID` – Identifiant du compte de gouvernance • `DataZoneKMSKeyID` – ID de la clé AWS Key Management Service (AWS KMS) qui chiffre les métadonnées Amazon DataZone • `NotificationQueueName` – Nom de la file d'attente de notifications Amazon SQS dans le compte de gouvernance	
Mettez à jour le ARNs.	Pour mettre à jour la liste des rôles AWS CloudFormation StackSet d'exécution ARNs pour les comptes membres, utilisez le code suivant : `DZ_MEMBER_STACK_SET_EXEC_ROLE_LIST - List of Stack set execution role arns for the member accounts.`	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

Synthétisez et déployez.	Pour synthétiser le AWS CloudFormation modèle et déployer la solution, exécutez les commandes suivantes :
	`npx cdk synth`
	`npx cdk deploy --all`
		Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
Associez le compte du membre.	Pour associer le compte membre au compte de gouvernance central, procédez comme suit : 1. Connectez-vous à la console du compte de gouvernance central et ouvrez la DataZone console Amazon à l'adresse https://console.aws.amazon.com/datazone/. 2. Choisissez le domaine que vous avez créé. 3. Accédez à l'onglet Comptes associés, puis sélectionnez Request Association. 4. Indiquez l'ID du compte AWS et choisissez-le AWSRAMPermissionDataZonePortalReadWritecomme politique de RAM. 5. Choisissez Request Association. 6. Attendez de recevoir une notification par e-mail indiquant que votre compte a été correctement démarré.	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
Mettez à jour les paramètres.	Pour mettre à jour les paramètres spécifiques au compte membre dans le fichier de configuration à l'adresse `config/Config.ts` , utilisez le format suivant : `export const DZ_MEMBER_ACCOUNT_CONFIG: memberAccountConfig = { '123456789012' : { PROJECT_NAME: 'TEST-PROJECT-123456789012', PROJECT_DESCRIPTION: 'TEST-PROJECT-123456789012', PROJECT_EMAIL: 'user@xyz.com' } }`	Architecte cloud, DevOps ingénieur

Synthétisez et déployez le modèle.	Pour synthétiser le AWS CloudFormation modèle et déployer la solution, exécutez les commandes suivantes :
	`npx cdk synth`
	`npx cdk deploy --all`
		Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
Ajoutez des comptes de membres.	Pour créer et configurer des comptes membres supplémentaires dans la solution de données, répétez les étapes précédentes pour chaque compte membre. Cette solution ne fait pas de différence entre les producteurs de données et les consommateurs.	Architecte cloud, DevOps ingénieur

Nettoyage

Tâche	Description	Compétences requises
Dissociez les comptes des membres.	Pour dissocier les comptes, procédez comme suit : 1. Connectez-vous à la console et ouvrez la DataZone console Amazon. 2. Choisissez Afficher les domaines. 3. Sélectionnez le domaine que vous avez créé. 4. Choisissez l'onglet Associations de comptes. 5. Sélectionnez le compte de membre que vous souhaitez dissocier. 6. Choisissez Dissocier, puis entrez `disassociate` pour confirmer.	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	7. Répétez les étapes 3 à 6 pour tous les comptes membres.	

Tâche	Description	Compétences requises
Supprimez les instances de la pile.	Pour supprimer les instances de AWS CloudFormation pile, procédez comme suit : 1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation/. 2. Dans le panneau de navigation, sélectionnez StackSets. 3. Choisissez l'ensemble de piles nommé StackSet-DataZone - DataMesh - Member, puis cliquez sur l'onglet Stack instances. 4. Copiez l' Compte AWS identifiant du compte membre que vous souhaitez supprimer de l'adhésion. 5. Choisissez Actions, choisissez Supprimer les piles de StackSet et conservez les options par défaut. 6. Dans le champ Numéros de compte, entrez l'identifiant du compte. 7. Dans la liste déroulante Spécifier les régions, sélectionnez le Région AWS.	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	8. Choisissez Suivant, puis Soumettre. 9. Dans l'onglet Opérations, vérifiez que l'opération a réussi. La suppression de la pile peut prendre un certain temps. 10. Répétez les étapes 2 à 9 pour tous les comptes membres.	
Détruisez toutes les ressources.	Pour détruire des ressources, mettez en œuvre les étapes suivantes dans votre environnement de développement local (Linux ou macOS) : 1. Accédez au répertoire racine de votre dépôt. 2. Exportez les AWS informations d'identification du rôle IAM que vous avez utilisé pour créer la AWS CDK pile. 3. Pour détruire les ressources du cloud, exécutez la commande suivante : `npx cdk destroy --all`	Architecte cloud, DevOps ingénieur

Ressources connexes

- Amazon DataZone Quickstart avec des données AWS Glue

- Tutoriel : Créez votre première AWS CDK application
- Commencer avec AWS CloudFormation
- Stratégies pour créer une solution d'entreprise basée sur un maillage de données sur AWS

Informations supplémentaires

Objectifs

La mise en œuvre de ce modèle permet d'obtenir les résultats suivants :

- Propriété décentralisée des données – Transférez la propriété des données d'une équipe centrale à des équipes représentant les systèmes sources, les unités commerciales ou les cas d'utilisation de votre organisation.
- Pensée produit – Adoptez un état d'esprit axé sur le produit qui inclut les clients, le marché et d'autres facteurs lorsque vous considérez les actifs de données de votre organisation.
- Gouvernance fédérée – Améliorez les garde-fous de sécurité, les contrôles et la conformité des produits de données de votre entreprise.
- Support multi-comptes et multi-projets – Soutenez un partage de données et une collaboration efficaces et sécurisés entre les unités commerciales ou les projets de votre organisation.
- Surveillance et notifications centralisées – Surveillez les ressources cloud de votre maillage de données à l'aide d'Amazon CloudWatch, et informez les utilisateurs lorsqu'un nouveau compte membre est associé.
- Évolutivité et extensibilité – Ajoutez de nouveaux cas d'utilisation au maillage de données au fur et à mesure de l'évolution de votre organisation.

Portée de la solution

Lorsque vous utilisez cette solution, vous pouvez commencer à petite échelle et évoluer au fur et à mesure que vous progressez dans votre parcours vers le maillage des données. Souvent, lorsqu'un compte membre adopte la solution de données, celle-ci contient des configurations de compte spécifiques à l'organisation, au projet ou à l'unité commerciale. Cette solution s'adapte à ces diverses Compte AWS configurations en prenant en charge les fonctionnalités suivantes :

- Le catalogue de données AWS Glue en tant que source de données pour Amazon DataZone
- Gestion du domaine de DataZone données Amazon et du portail de données associé

- Gestion de l'ajout de comptes membres dans la solution de données basée sur le maillage de données
- Gestion des DataZone projets et des environnements Amazon
- Gestion des DataZone glossaires et des formulaires de métadonnées Amazon
- Gestion des rôles IAM correspondant aux utilisateurs de solutions de données basées sur le maillage de données
- Notification des utilisateurs de solutions de données basées sur un maillage de données
- Surveillance de l'infrastructure cloud provisionnée

  Cette solution utilise AWS CDK et AWS CloudFormation déploie l'infrastructure cloud. Il permet AWS CloudFormation d'effectuer les opérations suivantes :

  - Définissez et déployez les ressources cloud à un niveau d'abstraction inférieur.
  - Déployez des ressources cloud à partir du AWS Management Console. En utilisant cette approche, vous pouvez déployer une infrastructure sans environnement de développement.

  La solution de maillage de données permet AWS CDK de définir les ressources à un niveau d'abstraction supérieur. Par conséquent, la solution propose une approche découplée, modulaire et évolutive en choisissant l'outil approprié pour déployer les ressources du cloud.

Étapes suivantes

Vous pouvez contacter des AWSexperts pour obtenir des conseils sur la création d'un maillage de données avec Amazon DataZone.

La nature modulaire de cette solution permet de créer des solutions de gestion des données avec différentes architectures, telles que Data Fabric et Data Lakes. En outre, en fonction des besoins de votre organisation, vous pouvez étendre la solution à d'autres sources de DataZone données Amazon.

Calculez la valeur à risque (VaR) à l'aide des services AWS

Créée par Sumon Samanta (AWS)

Récapitulatif

Ce modèle décrit comment implémenter un système de calcul de la valeur à risque (VaR) à l'aide des services AWS. Dans un environnement sur site, la plupart des systèmes VaR utilisent une vaste infrastructure dédiée et un logiciel de planification de réseau interne ou commercial pour exécuter les processus par lots. Ce modèle présente une architecture simple, fiable et évolutive pour gérer le traitement de la VaR dans le cloud AWS. Il construit une architecture sans serveur qui utilise Amazon Kinesis Data Streams comme service de streaming, Amazon Simple Queue Service (Amazon SQS) comme service de file d'attente géré, ElastiCache Amazon comme service de mise en cache et AWS Lambda pour traiter les commandes et calculer les risques.

La VaR est une mesure statistique que les traders et les gestionnaires de risques utilisent pour estimer les pertes potentielles de leur portefeuille au-delà d'un certain niveau de confiance. La plupart des systèmes VaR impliquent l'exécution d'un grand nombre de calculs mathématiques et statistiques et le stockage des résultats. Ces calculs nécessitent des ressources de calcul importantes, de sorte que les processus par lots VaR doivent être divisés en de plus petits ensembles de tâches de calcul. Il est possible de diviser un lot important en tâches plus petites car ces tâches sont pour la plupart indépendantes (c'est-à-dire que les calculs d'une tâche ne dépendent pas des autres tâches).

Une autre exigence importante pour une architecture VaR est l'évolutivité du calcul. Ce modèle utilise une architecture sans serveur qui évolue automatiquement en entrée ou en sortie en fonction de la charge de calcul. La demande de calcul par lots ou en ligne étant difficile à prévoir, une mise à l'échelle dynamique est nécessaire pour terminer le processus dans les délais imposés par un accord de niveau de service (SLA). En outre, une architecture optimisée en termes de coûts doit être capable de réduire chaque ressource de calcul dès que les tâches associées à cette ressource sont terminées.

Les services AWS sont parfaitement adaptés aux calculs de la VaR car ils offrent des capacités de calcul et de stockage évolutives, des services d'analyse pour un traitement optimisé en termes de coûts et différents types de planificateurs pour exécuter vos flux de travail de gestion des risques. De plus, vous ne payez que pour les ressources de calcul et de stockage que vous utilisez sur AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Fichiers d'entrée, qui dépendent des besoins de votre entreprise. Un cas d'utilisation typique implique les fichiers d'entrée suivants :
  - Fichier de données de marché (entrée dans le moteur de calcul de la VaR)
  - Fichier de données commerciales (sauf si les données commerciales proviennent d'un flux).
  - Fichier de données de configuration (modèle et autres données de configuration statiques)
  - Fichiers de modèles de moteurs de calcul (bibliothèques quantitatives)
  - Fichier de données de séries chronologiques (pour les données historiques telles que le cours des actions des cinq dernières années)
- Si les données de marché ou d'autres entrées arrivent par le biais d'un flux, Amazon Kinesis Data Streams est configuré et les autorisations Amazon Identity and Access Management (IAM) sont configurées pour écrire dans le flux.

Ce modèle crée une architecture dans laquelle les données commerciales sont écrites depuis un système de trading vers un flux de données Kinesis. Au lieu d'utiliser un service de streaming, vous pouvez enregistrer vos données commerciales dans de petits fichiers par lots, les stocker dans un bucket Amazon Simple Storage Service (Amazon S3) et invoquer un événement pour commencer à traiter les données.

Limites

- Le séquençage des flux de données Kinesis est garanti sur chaque partition. Il n'est donc pas garanti que les ordres de transaction écrits sur plusieurs partitions soient livrés dans le même ordre que les opérations d'écriture.
- La limite d'exécution d'AWS Lambda est actuellement de 15 minutes. (Pour plus d'informations, consultez la FAQ Lambda.)

Architecture

Architecture cible

Le schéma d'architecture suivant présente les services et les flux de travail AWS pour le système d'évaluation des risques.

Le diagramme illustre les éléments suivants :

1. Les transactions sont effectuées depuis le système de gestion des commandes.
2. La fonction Lambda de compensation de la position du ticket traite les commandes et écrit des messages consolidés pour chaque ticker dans une file d'attente des risques dans Amazon SQS.
3. La fonction Lambda du moteur de calcul des risques traite les messages provenant d'Amazon SQS, effectue des calculs de risques et met à jour les informations de profits et pertes (PnL) vAR dans le cache des risques d'Amazon. ElastiCache
4. La fonction Lambda de lecture ElastiCache des données extrait les résultats des risques ElastiCache et les stocke dans une base de données et un compartiment S3.

Pour plus d'informations sur ces services et ces étapes, consultez la section Epics.

Automatisation et mise à l'échelle

Vous pouvez déployer l'architecture complète à l'aide de l'AWS Cloud Development Kit (AWS CDK) ou de CloudFormation modèles AWS. L'architecture peut prendre en charge à la fois le traitement par lots et le traitement intrajournalier (en temps réel).

La mise à l'échelle est intégrée à l'architecture. Au fur et à mesure que de nouvelles transactions sont enregistrées dans le flux de données Kinesis et attendent d'être traitées, des fonctions Lambda supplémentaires peuvent être invoquées pour traiter ces transactions, puis peuvent être réduites une fois le traitement terminé. Le traitement via plusieurs files d'attente de calcul des risques Amazon SQS est également une option. Si un ordre ou une consolidation stricts sont requis entre les files d'attente, le traitement ne peut pas être parallélisé. Toutefois, pour un end-of-the-day lot ou un mini-lot intrajournalier, les fonctions Lambda peuvent traiter en parallèle et enregistrer les résultats finaux. ElastiCache

Outils

Services AWS

- Amazon Aurora MySQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible avec MySQL qui vous aide à configurer, exploiter et dimensionner les déploiements MySQL. Ce modèle utilise MySQL comme exemple, mais vous pouvez utiliser n'importe quel système RDBMS pour stocker des données.
- Amazon vous ElastiCache aide à configurer, gérer et faire évoluer des environnements de cache en mémoire distribués dans le cloud AWS.

- Amazon Kinesis Data Streams vous aide à collecter et à traiter de grands flux d'enregistrements de données en temps réel.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

Ce modèle fournit un exemple d'architecture pour un système VaR dans le cloud AWS et décrit comment utiliser les fonctions Lambda pour les calculs VaR. Pour créer vos fonctions Lambda, consultez les exemples de code dans la documentation Lambda. Pour obtenir de l'aide, contactez AWS Professional Services.

Bonnes pratiques

- Faites en sorte que chaque tâche de calcul VaR soit aussi petite et légère que possible. Testez différents nombres de transactions dans chaque tâche de calcul pour déterminer laquelle est la plus optimisée en termes de temps et de coût de calcul.
- Stockez des objets réutilisables sur Amazon ElastiCache. Utilisez un framework tel qu'Apache Arrow pour réduire la sérialisation et la désérialisation.
- Tenez compte de la limite de temps de Lambda. Si vous pensez que vos tâches de calcul peuvent dépasser 15 minutes, essayez de les diviser en tâches plus petites pour éviter le délai Lambda. Si cela n'est pas possible, vous pouvez envisager une solution d'orchestration de conteneurs avec AWS Fargate, Amazon Elastic Container Service (Amazon ECS) et Amazon Elastic Kubernetes Service (Amazon EKS).

Épopées

Système de gestion des flux commerciaux par rapport au risque

Tâche	Description	Compétences requises
Commencez à écrire des transactions.	Les transactions nouvelles , réglées ou partiellement réglées sont enregistrées depuis le système de gestion des ordres dans un flux de risques. Ce modèle utilise Amazon Kinesis comme service de streaming géré. Le hachage du ticker des ordres de transaction est utilisé pour placer les ordres de transacti on sur plusieurs partitions.	Amazon Kinesis

Exécuter les fonctions Lambda pour le traitement des commandes

Tâche	Description	Compétences requises
Commencez le traitement des risques avec Lambda.	Exécutez une fonction AWS Lambda pour les nouvelles commandes. En fonction du nombre d'ordres commerciaux en attente, Lambda évoluera automatiquement. Chaque instance Lambda reçoit une ou plusieurs commandes et récupère la dernière position pour chaque ticker sur Amazon. ElastiCache (Vous pouvez utiliser un identifiant CUSIP, un nom de courbe ou	Amazon Kinesis, AWS Lambda, Amazon ElastiCache

Tâche	Description	Compétences requises
	un nom d'indice pour d'autres produits financiers dérivés comme clé pour stocker et récupérer des données ElasticCache.) Dans ElastiCache, la position totale (quantité) et la paire clé-valeur < ticker, position nette >, où la position nette est le facteur d'échelle, sont mises à jour une fois pour chaque ticker.	

Écrire des messages pour chaque ticker dans la file d'attente

Tâche	Description	Compétences requises
Écrivez des messages consolidés dans la file d'attente des risques.	Ecrivez le message dans une file d'attente. Ce modèle utilise Amazon SQS comme service de file d'attente géré. Une seule instance Lambda peut recevoir un mini-lot d'ordres de transaction à tout moment, mais elle n'écrit qu'un seul message pour chaque ticker sur Amazon SQS. Un facteur d'échelle est calculé : (ancienne position nette + position actuelle)/ancienne position nette.	Amazon SQS, AWS Lambda

Invoquer le moteur de risque

Tâche	Description	Compétences requises
Commencez à calculer les risques.	La fonction Lambda pour le moteur de gestion des risques lambda est invoquée. Chaque position est traitée par une seule fonction Lambda. Toutefois, à des fins d'optimisation, chaque fonction Lambda peut traiter plusieurs messages provenant d'Amazon SQS.	Amazon SQS, AWS Lambda

Extraire les résultats des risques depuis le cache

Tâche	Description	Compétences requises
Récupérez et mettez à jour le cache des risques.	Lambda extrait la position nette actuelle de chaque ticker à partir de. ElastiCac he Il récupère également un tableau des profits et pertes vAR (PnL) pour chaque ticker à partir de. ElastiCache Si le tableau PnL existe déjà, la fonction Lambda met à jour le tableau et le VaR avec une échelle, qui provient du message Amazon SQS écrit par la fonction Lambda de netting. Si le tableau PnL n'y figure pas ElasticCache, un nouveau PnL et un nouveau	Amazon SQS, AWS Lambda, Amazon ElastiCache

Tâche	Description	Compétences requises
	VaR sont calculés à l'aide de données de séries de prix simulées.	

Mettre à jour les données dans Elastic Cache et les stocker dans la base de données

Tâche	Description	Compétences requises
Conservez les résultats relatifs aux risques.	Une fois les numéros VaR et PnL mis à jour ElastiCache, une nouvelle fonction Lambda est invoquée toutes les cinq minutes. Cette fonction lit toutes les données stockées ElastiCache et les stocke dans une base de données compatible Aurora MySQL et dans un compartiment S3.	AWS Lambda, Amazon ElastiCache

Ressources connexes

- Cadre VaR de Bâle

Configurer l'accès entre comptes à un catalogue de données AWS Glue partagé à l'aide d'Amazon Athena

Créée par Denis Avdonin (AWS)

Récapitulatif

Ce modèle fournit des step-by-step instructions, notamment des exemples de politique AWS Identity and Access Management (IAM), pour configurer le partage entre comptes d'un ensemble de données stocké dans un bucket Amazon Simple Storage Service (Amazon S3) à l'aide du catalogue de données AWS Glue. Vous pouvez stocker l'ensemble de données dans un compartiment S3. Les métadonnées sont collectées par un robot d'exploration AWS Glue et intégrées au catalogue de données AWS Glue. Le compartiment S3 et le catalogue de données AWS Glue se trouvent dans un compte AWS appelé compte de données. Vous pouvez fournir l'accès aux principaux IAM via un autre compte AWS appelé compte consommateur. Les utilisateurs peuvent interroger les données du compte client à l'aide du moteur de requête sans serveur Amazon Athena.

Conditions préalables et limitations

Prérequis

- Deux comptes AWS actifs
- Un compartiment S3 dans l'un des comptes AWS
- Moteur Athena version 2
- Interface de ligne de commande AWS (AWS CLI), installée et configurée (ou AWS CloudShell pour exécuter des commandes de l'interface de ligne de commande AWS)

Versions du produit

Ce modèle fonctionne uniquement avec la version 2 du moteur Athena et la version 3 du moteur Athena. Nous vous recommandons de passer à la version 3 du moteur Athena. Si vous ne parvenez pas à passer de la version 1 du moteur Athena à la version 3 du moteur Athena, suivez l'approche décrite dans la section Accès au catalogue de données AWS Glue entre comptes avec Amazon Athena sur le blog AWS Big Data.

Architecture

Pile technologique cible

- Amazon Athena
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Key Management Service (AWS KMS)

Le schéma suivant montre une architecture qui utilise les autorisations IAM pour partager les données d'un compartiment S3 d'un compte AWS (compte de données) avec un autre compte AWS (compte consommateur) via le catalogue de données AWS Glue.

Le schéma suivant illustre le flux de travail suivant :

1. La politique relative au compartiment S3 du compte de données accorde des autorisations à un rôle IAM dans le compte client et au rôle de service d'exploration AWS Glue dans le compte de données.
2. La politique clé d'AWS KMS relative au compte de données accorde des autorisations au rôle IAM dans le compte consommateur et au rôle de service d'exploration AWS Glue dans le compte de données.
3. Le robot d'exploration AWS Glue du compte de données découvre le schéma des données stockées dans le compartiment S3.
4. La politique de ressources du catalogue de données AWS Glue dans le compte de données autorise l'accès au rôle IAM dans le compte client.
5. Un utilisateur crée une référence de catalogue nommée dans le compte client à l'aide d'une commande AWS CLI.
6. Une politique IAM accorde à un rôle IAM dans le compte client l'accès aux ressources du compte de données. La politique de confiance du rôle IAM permet aux utilisateurs du compte client d'assumer le rôle IAM.
7. Un utilisateur du compte consommateur assume le rôle IAM et accède aux objets du catalogue de données à l'aide de requêtes SQL.
8. Le moteur sans serveur Athena exécute les requêtes SQL.

> **Note**
>
> Les meilleures pratiques IAM recommandent d'accorder des autorisations à un rôle IAM et d'utiliser la fédération d'identité.

Outils

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.

Épopées

Configurer les autorisations dans le compte de données

Tâche	Description	Compétences requises
Accordez l'accès aux données du compartiment S3.	Créez une politique de compartiment S3 basée sur le modèle suivant et attribuez-la au compartiment dans lequel les données sont stockées. `{ "Version": "2012-10-17", "Statement": [`	Administrateur du cloud

Tâche	Description	Compétences requises

	<pre>{
	"Effect":
	"Allow",
	"Principa
	l": {
	"AWS": [
	
	"arn:aws:iam::<con
	sumer account id>:role/
	<role name>",
	
	"arn:aws:iam::<dat
	a account id>:role/
	service-role/AWSGl
	ueServiceRole-data-
	bucket-crawler"
	]
	},
	"Action":
	"s3:GetObject",
	"Resource":
	"arn:aws:s3:::data-
	bucket/*"
	},
	{
	"Effect":
	"Allow",
	"Principa
	l": {
	"AWS": [
	
	"arn:aws:iam::<con
	sumer account id>:role/
	<role name>",
	
	"arn:aws:iam::<dat
	a account id>:role/
	service-role/AWSGl
	ueServiceRole-data-
	bucket-crawler"
	]
	},</pre>	

Tâche	Description	Compétences requises

	<pre>"Action":
	"s3:ListBucket",
	"Resource":
	"arn:aws:s3:::data-
	bucket"
	}
	]
	}</pre>
	La politique du bucket accorde des autorisations au rôle IAM dans le compte client et au rôle de service d'exploration AWS Glue dans le compte de données.	

Tâche	Description	Compétences requises
(Si nécessaire) Accordez l'accès à la clé de chiffrement des données.	Si le compartiment S3 est chiffré par une clé AWS KMS, accordez l'`kms:Decrypt` autorisation sur la clé au rôle IAM dans le compte client et au rôle de service d'exploration AWS Glue dans le compte de données. Mettez à jour la politique clé avec la déclaration suivante : `{ "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrateur du cloud

Tâche	Description	Compétences requises

Accordez au robot d'exploration l'accès aux données.	Associez la politique IAM suivante au rôle de service du robot d'exploration :
	
	{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow",
	"Action": "s3:GetObject",
	"Resource": "arn:aws:s3:::data-bucket/*"
	},
	{
	"Effect": "Allow",
	"Action": "s3:ListBucket",
	"Resource": "arn:aws:s3:::data-bucket"
	}
	]
	}
		Administrateur du cloud

Tâche	Description	Compétences requises
(Si nécessaire) Accordez au robot d'exploration l'accès à la clé de chiffrement des données.	Si le compartiment S3 est chiffré par une clé AWS KMS, accordez une `kms:Decrypt` autorisation sur la clé au rôle de service du robot d'exploration en y associant la politique suivante : `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrateur du cloud

Tâche	Description	Compétences requises
Accordez au rôle IAM dans le compte client et au robot d'exploration l'accès au catalogue de données.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Glue. 2. Dans le volet de navigation, sous Catalogue de données, sélectionnez Paramètres. 3. Dans la section Autorisations, ajoutez l'instruction suivante, puis choisissez Enregistrer. `{ "Version" : "2012-10-17", "Statement" : [ { "Effect" : "Allow", "Principal" : { "AWS" : [ "arn:aws:iam::<consumer account id>:role/<role name>", "arn:aws:iam::<data account id>:role/service-role/AWSGlueServiceRole-data-bucket-crawler" ] }, ...`	Administrateur du cloud

Tâche	Description	Compétences requises
	<pre>"Action" : "glue:*", "Resource" : ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] }</pre> Cette politique autorise toutes les actions AWS Glue sur toutes les bases de données et tables du compte de données. Vous pouvez personnaliser la politique pour n'accorder que les autorisations requises aux principaux consommateurs. Par exemple, vous pouvez fournir un accès en lecture seule à des tables ou à des vues spécifiques d'une base de données.	

Accédez aux données depuis le compte client

Tâche	Description	Compétences requises
Créez une référence nommée pour le catalogue de données.	Pour créer une référence de catalogue de données nommée, utilisez CloudShel lune CLI AWS installée localement pour exécuter la commande suivante : `aws athena create-da ta-catalog --name <shared catalog name> --type GLUE --paramet ers catalog-id=<data account id>`	Administrateur du cloud
Accordez au rôle IAM du compte client l'accès aux données.	Associez la politique suivante au rôle IAM dans le compte client pour accorder au rôle un accès multicompte aux données : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::data-bucket/*" }, { "Effect": "Allow",`	Administrateur du cloud

Tâche	Description	Compétences requises
	"Action": "s3:ListBucket", "Resource": "arn:aws:s3:::data-bucket" }, { "Effect": "Allow", "Action": "glue:*", "Resource": ["arn:aws:glue:<region>:<data account id>:catalog", "arn:aws:glue:<region>:<data account id>:database/*", "arn:aws:glue:<region>:<data account id>:table/*"] }] } Ensuite, utilisez le modèle suivant pour spécifier quels utilisateurs peuvent accepter le rôle IAM dans sa politique de confiance : { "Version": "2012-10-17", "Statement": [	

Tâche	Description	Compétences requises

	<pre>{
	"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam::<consumer account id>:user/<IAM user>"
	},
	"Action": "sts:AssumeRole"
	}
	]
	}</pre>
	Enfin, accordez aux utilisateurs l'autorisation d'assumer le rôle IAM en attachant la même politique au groupe d'utilisateurs auquel ils appartiennent.	

Tâche	Description	Compétences requises
(Si nécessaire) Accordez au rôle IAM du compte client l'accès à la clé de chiffrement des données.	Si le compartiment S3 est chiffré par une clé AWS KMS, accordez l'`kms:Decrypt` autorisation d'utiliser la clé pour le rôle IAM dans le compte client en y joignant la politique suivante : `{ "Effect": "Allow", "Action": "kms:Decrypt", "Resource": "arn:aws:kms:<region>:<data account id>:key/<key id>" }`	Administrateur du cloud
Passez au rôle IAM dans le compte client pour accéder aux données.	En tant que consommateur de données, passez au rôle IAM pour accéder aux données du compte de données.	Consommateur de données

Tâche	Description	Compétences requises

Accédez aux données.	Interrogez des données à l'aide d'Athena. Par exemple, ouvrez l'éditeur de requêtes Athena et exécutez la requête suivante :
	`SELECT * FROM <shared catalog name>.<database name>.<table name>`
	Au lieu d'utiliser une référence de catalogue nommée, vous pouvez également faire référence au catalogue par son Amazon Resource Name (ARN).
	Note
	Si vous utilisez une référence de catalogue dynamique dans une requête ou une vue, entourez-la de guillemets évasiés (\ »). Par exemple :
	`SELECT * FROM \"glue:arn:aws:glue:<region>:<data account id>:catalog\".<database name>.<table name>`
		Consommateur de données

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Accès entre comptes aux catalogues de données AWS Glue dans le guide de l'utilisateur Amazon Athena.	

Ressources connexes

- Accès entre comptes aux catalogues de données AWS Glue (documentation Athena)
- (AWS CLI) create-data-catalog (Référence de commande de l'AWS CLI)
- Accès au catalogue de données AWS Glue entre comptes avec Amazon Athena (blog AWS Big Data)
- Bonnes pratiques de sécurité dans l'IAM (documentation IAM)

Informations supplémentaires

Utiliser Lake Formation comme alternative au partage entre comptes

Vous pouvez également utiliser AWS Lake Formation pour partager l'accès aux objets du catalogue AWS Glue entre différents comptes. Lake Formation fournit un contrôle d'accès précis au niveau des colonnes et des lignes, un contrôle d'accès basé sur des balises, des tables gouvernées pour les transactions ACID et d'autres fonctionnalités. Bien que Lake Formation soit bien intégrée à Athena, elle nécessite une configuration supplémentaire par rapport à l'approche uniquement IAM de ce modèle. Nous vous recommandons d'envisager la décision d'utiliser des contrôles d'accès réservés à Lake Formation ou à IAM dans le contexte plus large de l'architecture globale de votre solution. Les considérations incluent les autres services concernés et la manière dont ils s'intègrent aux deux approches.

Convertir la fonctionnalité temporelle Teradata NORMALIZE en Amazon Redshift SQL

Créée par Po Hong (AWS)

Récapitulatif

NORMALIZE est une extension Teradata de la norme ANSI SQL. Lorsqu'une table SQL inclut une colonne contenant un type de données PERIOD, NORMALIZE combine les valeurs qui se rejoignent ou se chevauchent dans cette colonne pour former une période unique qui consolide plusieurs valeurs de période individuelles. Pour utiliser NORMALIZE, au moins une colonne de la liste SQL SELECT doit être du type de données temporelles PERIOD de Teradata. Pour plus d'informations sur NORMALIZE, consultez la documentation Teradata.

Amazon Redshift ne prend pas en charge NORMALIZE, mais vous pouvez implémenter cette fonctionnalité en utilisant la syntaxe SQL native et la fonction de fenêtre LAG dans Amazon Redshift. Ce modèle se concentre sur l'utilisation de l'extension Teradata NORMALIZE avec la condition ON MEETS OR OVERLAPS, qui est le format le plus courant. Il explique comment cette fonctionnalité fonctionne dans Teradata et comment elle peut être convertie en syntaxe SQL native Amazon Redshift.

Conditions préalables et limitations

Prérequis

- Connaissances et expérience de base de Teradata SQL
- Connaissances et expérience d'Amazon Redshift

Architecture

Pile technologique source

- Entrepôt de données Teradata

Pile technologique cible

- Amazon Redshift

Architecture cible

Pour une architecture de haut niveau permettant de migrer une base de données Teradata vers Amazon Redshift, consultez le modèle Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT. La migration ne convertit pas automatiquement la phrase Teradata NORMALIZE en Amazon Redshift SQL. Vous pouvez convertir cette extension Teradata en suivant les instructions de ce modèle.

Outils

Code

Pour illustrer le concept et les fonctionnalités de NORMALIZE, considérez la définition de table suivante dans Teradata :

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          duration      PERIOD(DATE)
     );
```

Exécutez le code SQL suivant pour insérer des exemples de données dans la table :

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  PERIOD(DATE '2010-01-10',
 DATE '2010-03-20') );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  PERIOD(DATE '2010-03-20',
 DATE '2010-07-15') );

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  PERIOD(DATE
 '2010-06-15', DATE '2010-08-18') );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  PERIOD(DATE '2010-03-10',
 DATE '2010-07-20') );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  PERIOD(DATE
 '2020-05-10', DATE '2020-09-20') );

END TRANSACTION;
```

Résultats :

```
select * from systest.project order by 1,2,3;

 *** Query completed. 4 rows found. 4 columns returned.
 *** Total elapsed time was 1 second.

     emp_id  project_name              dept_id  duration
-----------  --------------------  -----------  ------------------------
         10  First Phase                  1000  ('10/01/10', '10/03/20')
         10  First Phase                  2000  ('10/03/20', '10/07/15')
         10  Second Phase                 2000  ('10/06/15', '10/08/18')
         20  First Phase                  2000  ('10/03/10', '10/07/20')
         20  Second Phase                 1000  ('20/05/10', '20/09/20')
```

Cas d'utilisation de Teradata NORMALIZE

Ajoutez maintenant la clause SQL Teradata NORMALIZE à l'instruction SELECT :

```
SELECT NORMALIZE ON MEETS OR OVERLAPS emp_id, duration
FROM systest.project
ORDER BY 1,2;
```

Cette opération NORMALIZE est effectuée sur une seule colonne (emp_id). Pour emp_id=10, les trois valeurs de période qui se chevauchent dans la durée fusionnent en une seule valeur de période, comme suit :

```
     emp_id  duration
-----------  ------------------------
         10  ('10/01/10', '10/08/18')
         20  ('10/03/10', '10/07/20')
         20  ('20/05/10', '20/09/20')
```

L'instruction SELECT suivante exécute une opération NORMALIZE sur project_name et dept_id. Notez que la liste SELECT ne contient qu'une seule colonne PERIOD, la durée.

```
SELECT NORMALIZE project_name, dept_id, duration
FROM systest.project;
```

Sortie :

```
project_name              dept_id  duration
```

```
--------------------  -----------  ------------------------
First Phase                   1000  ('10/01/10', '10/03/20')
Second Phase                  1000  ('20/05/10', '20/09/20')
First Phase                   2000  ('10/03/10', '10/07/20')
Second Phase                  2000  ('10/06/15', '10/08/18')
```

SQL équivalent à Amazon Redshift

Amazon Redshift ne prend actuellement pas en charge le type de données PERIOD dans une table. Vous devez plutôt diviser un champ de données Teradata PERIOD en deux parties : start_date, end_date, comme suit :

```
CREATE TABLE systest.project
     (    emp_id        INTEGER,
          project_name  VARCHAR(20),
          dept_id       INTEGER,
          start_date  DATE,
          end_date    DATE
     );
```

Insérez des exemples de données dans le tableau :

```
BEGIN TRANSACTION;

INSERT INTO systest.project VALUES (10, 'First Phase', 1000,  DATE '2010-01-10', DATE
 '2010-03-20' );
INSERT INTO systest.project VALUES (10, 'First Phase', 2000,  DATE '2010-03-20', DATE
 '2010-07-15');

INSERT INTO systest.project VALUES (10, 'Second Phase', 2000,  DATE '2010-06-15', DATE
 '2010-08-18' );
INSERT INTO systest.project VALUES (20, 'First Phase', 2000,  DATE '2010-03-10', DATE
 '2010-07-20' );

INSERT INTO systest.project VALUES (20, 'Second Phase', 1000,  DATE '2020-05-10', DATE
 '2020-09-20' );

END TRANSACTION;
```

Sortie :

```
 emp_id | project_name | dept_id | start_date |  end_date
```

```
--------+--------------+---------+------------+------------
     10 | First Phase  |    1000 | 2010-01-10 | 2010-03-20
     10 | First Phase  |    2000 | 2010-03-20 | 2010-07-15
     10 | Second Phase |    2000 | 2010-06-15 | 2010-08-18
     20 | First Phase  |    2000 | 2010-03-10 | 2010-07-20
     20 | Second Phase |    1000 | 2020-05-10 | 2020-09-20
(5 rows)
```

Pour réécrire la clause NORMALIZE de Teradata, vous pouvez utiliser la fonction de fenêtre LAG dans Amazon Redshift. Cette fonction renvoie les valeurs d'une ligne à un décalage donné au-dessus (avant) de la ligne actuelle de la partition.

Vous pouvez utiliser la fonction LAG pour identifier chaque ligne qui commence une nouvelle période en déterminant si une période correspond ou chevauche la période précédente (0 dans l'affirmative et 1 dans le cas contraire). Lorsque cet indicateur est additionné de manière cumulative, il fournit un identifiant de groupe qui peut être utilisé dans la clause externe Group By pour obtenir le résultat souhaité dans Amazon Redshift.

Voici un exemple d'instruction SQL Amazon Redshift qui utilise LAG () :

```
SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project
ORDER BY 1,2;
```

Sortie :

```
 emp_id | start_date |  end_date  | groupstartflag
--------+------------+------------+---------------
     10 | 2010-01-10 | 2010-03-20 |              1
     10 | 2010-03-20 | 2010-07-15 |              0
     10 | 2010-06-15 | 2010-08-18 |              0
     20 | 2010-03-10 | 2010-07-20 |              1
     20 | 2020-05-10 | 2020-09-20 |              1
(5 rows)
```

L'instruction SQL Amazon Redshift suivante est normalisée uniquement sur la colonne emp_id :

```
SELECT T2.emp_id, MIN(T2.start_date) as new_start_date, MAX(T2.end_date) as
 new_end_date
```

```
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY emp_id ORDER BY start_date ROWS
 UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT emp_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY emp_id ORDER BY
 start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.emp_id, T2.GroupID
ORDER BY 1,2;
```

Sortie :

```
 emp_id | new_start_date | new_end_date
--------+----------------+-------------------------------------
     10 | 2010-01-10     | 2010-08-18
     20 | 2010-03-10     | 2010-07-20
     20 | 2020-05-10     | 2020-09-20
(3 rows)
```

L'instruction SQL Amazon Redshift suivante normalise les colonnes project_name et dept_id :

```
SELECT T2.project_name, T2.dept_id, MIN(T2.start_date) as new_start_date,
 MAX(T2.end_date) as new_end_date
FROM
( SELECT T1.*, SUM(GroupStartFlag) OVER (PARTITION BY project_name, dept_id ORDER BY
 start_date ROWS UNBOUNDED PRECEDING) As GroupID
FROM ( SELECT project_name, dept_id, start_date, end_date,
            (CASE WHEN start_date <= LAG(end_date) OVER (PARTITION BY project_name,
 dept_id ORDER BY start_date, end_date) THEN 0 ELSE 1 END) AS GroupStartFlag
FROM systest.project ) T1
) T2
GROUP BY T2.project_name, T2.dept_id, T2.GroupID
ORDER BY 1,2,3;
```

Sortie :

```
 project_name | dept_id | new_start_date | new_end_date
--------------+---------+----------------+--------------
 First Phase  |    1000 | 2010-01-10     | 2010-03-20
```

```
 First Phase  |    2000 | 2010-03-10     | 2010-07-20
 Second Phase |    1000 | 2020-05-10     | 2020-09-20
 Second Phase |    2000 | 2010-06-15     | 2010-08-18
(4 rows)
```

Épopées

Convertir NORMALIZE en Amazon Redshift SQL

Tâche	Description	Compétences requises
Créez votre code Teradata SQL.	Utilisez la phrase NORMALIZE en fonction de vos besoins.	SQL Developer
Convertissez le code en Amazon Redshift SQL.	Pour convertir votre code, suivez les instructions de la section « Outils » de ce modèle.	SQL Developer
Exécutez le code dans Amazon Redshift.	Créez votre table, chargez des données dans la table et exécutez votre code dans Amazon Redshift.	SQL Developer

Ressources connexes

Références

- Fonctionnalité temporelle Teradata NORMALIZE (documentation Teradata)
- Fonction de fenêtre LAG (documentation Amazon Redshift)
- Migrer vers Amazon Redshift (site Web AWS)
- Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT (AWS Prescriptive Guidance)
- Convertir la fonctionnalité Teradata RESET WHEN en Amazon Redshift SQL (AWS Prescriptive Guidance)

Outils

- Outil de conversion de schéma AWS (AWS SCT)

Partenaires

- AWS Migration Competency Partners

Convertir la fonctionnalité Teradata RESET WHEN en Amazon Redshift SQL

Créée par Po Hong (AWS)

Récapitulatif

RESET WHEN est une fonctionnalité Teradata utilisée dans les fonctions des fenêtres analytiques SQL. Il s'agit d'une extension de la norme ANSI SQL. RESET WHEN détermine la partition sur laquelle une fonction de fenêtre SQL fonctionne en fonction d'une condition spécifiée. Si la condition est définie sur VRAI, une nouvelle sous-partition dynamique est créée à l'intérieur de la partition de fenêtre existante. Pour plus d'informations sur RESET WHEN, consultez la documentation Teradata.

Amazon Redshift ne prend pas en charge les fonctions RESET WHEN dans les fenêtres SQL. Pour implémenter cette fonctionnalité, vous devez convertir RESET WHEN en syntaxe SQL native dans Amazon Redshift et utiliser plusieurs fonctions imbriquées. Ce modèle montre comment utiliser la fonctionnalité Teradata RESET WHEN et comment la convertir en syntaxe SQL Amazon Redshift.

Conditions préalables et limitations

Prérequis

- Connaissances de base de l'entrepôt de données Teradata et de sa syntaxe SQL
- Bonne compréhension d'Amazon Redshift et de sa syntaxe SQL

Architecture

Pile technologique source

- Entrepôt de données Teradata

Pile technologique cible

- Amazon Redshift

Architecture

Pour une architecture de haut niveau permettant de migrer une base de données Teradata vers Amazon Redshift, consultez le modèle Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT. La migration ne convertit pas automatiquement la phrase Teradata RESET WHEN en Amazon Redshift SQL. Vous pouvez convertir cette extension Teradata en suivant les instructions de la section suivante.

Outils

Code

Pour illustrer le concept de RESET WHEN, considérez la définition de table suivante dans Teradata :

```
create table systest.f_account_balance
( account_id integer NOT NULL,
  month_id integer,
  balance integer )
unique primary index (account_id, month_id);
```

Exécutez le code SQL suivant pour insérer des exemples de données dans la table :

```
BEGIN TRANSACTION;
Insert Into systest.f_account_balance values (1,1,60);
Insert Into systest.f_account_balance values (1,2,99);
Insert Into systest.f_account_balance values (1,3,94);
Insert Into systest.f_account_balance values (1,4,90);
Insert Into systest.f_account_balance values (1,5,80);
Insert Into systest.f_account_balance values (1,6,88);
Insert Into systest.f_account_balance values (1,7,90);
Insert Into systest.f_account_balance values (1,8,92);
Insert Into systest.f_account_balance values (1,9,10);
Insert Into systest.f_account_balance values (1,10,60);
Insert Into systest.f_account_balance values (1,11,80);
Insert Into systest.f_account_balance values (1,12,10);
END TRANSACTION;
```

Le tableau d'exemple contient les données suivantes :

account_id	ID du mois	équilibre
1	1	60

1	2	99
1	3	94
1	4	90
1	5	80
1	6	88
1	7	90
1	8	92
1	9	10
1	10	60
1	11	80
1	12	10

Pour chaque compte, supposons que vous souhaitiez analyser la séquence des augmentations mensuelles consécutives du solde. Lorsque le solde d'un mois est inférieur ou égal au solde du mois précédent, il est nécessaire de remettre le compteur à zéro et de redémarrer.

Cas d'utilisation de Teradata RESET WHEN

Pour analyser ces données, Teradata SQL utilise une fonction de fenêtre avec un agrégat imbriqué et une phrase RESET WHEN, comme suit :

```
SELECT account_id, month_id, balance,
 ( ROW_NUMBER() OVER (PARTITION BY account_id ORDER BY month_id
RESET WHEN balance <= SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS
 BETWEEN 1 PRECEDING AND 1 PRECEDING) ) -1 ) as balance_increase
FROM systest.f_account_balance
ORDER BY 1,2;
```

Sortie :

account_id	ID du mois	équilibre	augmentation du solde
1	1	60	0
1	2	99	1
1	3	94	0
1	4	90	0
1	5	80	0
1	6	88	1
1	7	90	2
1	8	92	3
1	9	10	0 USD
1	10	60	1
1	11	80	2
1	12	10	0 USD

La requête est traitée comme suit dans Teradata :

1. La fonction d'agrégation SUM (balance) calcule la somme de tous les soldes d'un compte donné au cours d'un mois donné.
2. Nous vérifions si le solde d'un mois donné (pour un compte donné) est supérieur au solde du mois précédent.
3. Si le solde augmente, nous suivons une valeur de comptage cumulée. Si la condition RESET WHEN prend la valeur fausse, ce qui signifie que le solde a augmenté au fil des mois, nous continuons à augmenter le nombre.
4. La fonction analytique ordonnée ROW_NUMBER () calcule la valeur du comptage. Lorsque nous atteignons un mois dont le solde est inférieur ou égal au solde du mois précédent, la condition RESET WHEN devient vraie. Si c'est le cas, nous démarrons une nouvelle partition et

ROW_NUMBER () recommence le décompte à partir de 1. Nous utilisons les lignes comprises entre 1 précédent et 1 précédent pour accéder à la valeur de la ligne précédente.

5. Nous soustrayons 1 pour nous assurer que la valeur du comptage commence par 0.

SQL équivalent à Amazon Redshift

Amazon Redshift ne prend pas en charge la phrase RESET WHEN dans une fonction de fenêtre d'analyse SQL. Pour obtenir le même résultat, vous devez réécrire le code SQL Teradata à l'aide de la syntaxe SQL native d'Amazon Redshift et de sous-requêtes imbriquées, comme suit :

```
SELECT account_id, month_id, balance,
   (ROW_NUMBER() OVER(PARTITION BY account_id, new_dynamic_part ORDER BY month_id) -1)
 as balance_increase
FROM
( SELECT account_id, month_id, balance, prev_balance,
SUM(dynamic_part) OVER (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN
 UNBOUNDED PRECEDING AND CURRENT ROW) As new_dynamic_part
FROM ( SELECT account_id, month_id, balance,
SUM(balance) over (PARTITION BY account_id ORDER BY month_id ROWS BETWEEN 1 PRECEDING
 AND 1 PRECEDING) as prev_balance,
(CASE When balance <= prev_balance Then 1 Else 0 END) as dynamic_part
FROM systest.f_account_balance ) A
) B
ORDER BY 1,2;
```

Amazon Redshift ne prenant pas en charge les fonctions de fenêtre imbriquées dans la clause SELECT d'une seule instruction SQL, vous devez utiliser deux sous-requêtes imbriquées.

- Dans la sous-requête interne (alias A), un indicateur de partition dynamique (dynamic_part) est créé et renseigné. dynamic_part est défini sur 1 si le solde d'un mois est inférieur ou égal au solde du mois précédent ; dans le cas contraire, il est défini sur 0.
- Dans la couche suivante (alias B), un attribut new_dynamic_part est généré à la suite d'une fonction de fenêtre SUM.
- Enfin, vous ajoutez new_dynamic_part en tant que nouvel attribut de partition (partition dynamique) à l'attribut de partition existant (account_id) et vous appliquez la même fonction de fenêtre ROW_NUMBER () que dans Teradata (avec moins un).

Après ces modifications, Amazon Redshift SQL génère le même résultat que Teradata.

Épopées

Convertir RESET WHEN en Amazon Redshift SQL

Tâche	Description	Compétences requises
Créez votre fonction de fenêtre Teradata.	Utilisez des agrégats imbriqués et la phrase RESET WHEN selon vos besoins.	SQL Developer
Convertissez le code en Amazon Redshift SQL.	Pour convertir votre code, suivez les instructions de la section « Outils » de ce modèle.	SQL Developer
Exécutez le code dans Amazon Redshift.	Créez votre table, chargez des données dans la table et exécutez votre code dans Amazon Redshift.	SQL Developer

Ressources connexes

Références

- Phrase RÉINITIALISER QUAND (documentation Teradata)
- Explication « RÉINITIALISER QUAND » (Stack Overflow)
- Migrer vers Amazon Redshift (site Web AWS)
- Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT (AWS Prescriptive Guidance)
- Convertir la fonctionnalité temporelle Teradata NORMALIZE en Amazon Redshift SQL (AWS Prescriptive Guidance)

Outils

- Outil de conversion de schéma AWS (AWS SCT)

Partenaires

- AWS Migration Competency Partners

Déployez et gérez un lac de données sans serveur sur le cloud AWS en utilisant l'infrastructure sous forme de code

Créée par Kirankumar Chandrashekar (AWS) et Abdel Jaidi (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle décrit comment utiliser l'informatique sans serveur et l'infrastructure en tant que code (IaC) pour implémenter et administrer un lac de données sur le cloud Amazon Web Services (AWS). Ce modèle est basé sur l'atelier Serverless Data Lake Framework (SDLF) développé par AWS.

Le SDLF est un ensemble de ressources réutilisables qui accélèrent la mise à disposition de lacs de données d'entreprise sur le cloud AWS et contribuent à accélérer le déploiement en production. Il est utilisé pour implémenter la structure de base d'un lac de données en suivant les meilleures pratiques.

SDLF met en œuvre un processus d'intégration/déploiement continu (CI/CD) tout au long du déploiement du code et de l'infrastructure en utilisant des services AWS tels qu'AWS, CodePipeline AWS CodeBuild et AWS. CodeCommit

Ce modèle utilise plusieurs services sans serveur AWS pour simplifier la gestion des lacs de données. Il s'agit notamment d'Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB pour le stockage, d'AWS Lambda et d'AWS Glue pour l'informatique, et d'Amazon Events, Amazon Simple Queue Service (Amazon SQS) CloudWatch et d'AWS Step Functions pour l'orchestration.

AWS CloudFormation et les services de code AWS agissent en tant que couche IaC pour fournir des déploiements rapides et reproductibles avec des opérations et une administration faciles.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée.
- Un client Git, installé et configuré.
- L'atelier SDLF, ouvert dans une fenêtre de navigateur Web et prêt à être utilisé.

Architecture

Le schéma d'architecture illustre un processus piloté par les événements avec les étapes suivantes.

1. Une fois qu'un fichier est ajouté au compartiment S3 de données brutes, une notification d'événement Amazon S3 est placée dans une file d'attente SQS. Chaque notification est envoyée sous forme de fichier JSON, qui contient des métadonnées telles que le nom du compartiment S3, la clé de l'objet ou l'horodatage.
2. Cette notification est consommée par une fonction Lambda qui achemine l'événement vers le processus d'extraction, de transformation et de chargement (ETL) approprié en fonction des métadonnées. La fonction Lambda peut également utiliser des configurations contextuelles stockées dans une table Amazon DynamoDB. Cette étape permet le découplage et le dimensionnement vers plusieurs applications du lac de données.
3. L'événement est acheminé vers la première fonction Lambda du processus ETL, qui transforme et déplace les données de la zone de données brutes vers la zone intermédiaire du lac de données. La première étape consiste à mettre à jour le catalogue complet. Il s'agit d'une table DynamoDB qui contient toutes les métadonnées de fichier du lac de données. Chaque ligne de ce tableau contient des métadonnées opérationnelles relatives à un seul objet stocké dans Amazon S3. Un appel synchrone est effectué vers une fonction Lambda qui effectue une légère transformation, opération peu coûteuse en termes de calcul (telle que la conversion d'un fichier d'un format à un autre), sur l'objet S3. Comme un nouvel objet a été ajouté au compartiment S3 intermédiaire, le catalogue complet est mis à jour et un message est envoyé à la file d'attente SQS en attente de la phase suivante de l'ETL.
4. Une règle CloudWatch Events déclenche une fonction Lambda toutes les 5 minutes. Cette fonction vérifie si des messages ont été remis à la file d'attente SQS lors de la phase ETL précédente. Si un message a été remis, la fonction Lambda lance la deuxième fonction d'AWS Step Functions dans le processus ETL.
5. Une transformation lourde est ensuite appliquée à un lot de fichiers. Cette transformation lourde est une opération coûteuse en termes de calcul, telle qu'un appel synchrone vers une tâche AWS Glue, une tâche AWS Fargate, une étape Amazon EMR ou un bloc-notes Amazon. SageMaker Les métadonnées des tables sont extraites des fichiers de sortie à l'aide d'un robot d'exploration AWS Glue, qui met à jour le catalogue AWS Glue. Les métadonnées des fichiers sont également ajoutées à la table complète du catalogue dans DynamoDB. Enfin, une étape de qualité des données utilisant Deequ est également exécutée.

Pile technologique

- CloudWatch Événements Amazon
- AWS CloudFormation
- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- Amazon DynamoDB
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SQS
- AWS Step Functions

Outils

- Amazon CloudWatch Events — CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS CloudFormation : CloudFormation permet de créer et de fournir des déploiements d'infrastructure AWS de manière prévisible et répétée.
- AWS CodeBuild CodeBuild est un service de génération entièrement géré qui compile votre code source, exécute des tests unitaires et produit des artefacts prêts à être déployés.
- AWS CodeCommit CodeCommit est un service de contrôle de version hébergé par AWS que vous pouvez utiliser pour stocker et gérer des actifs privés (tels que le code source et les fichiers binaires).
- AWS CodePipeline CodePipeline est un service de livraison continue que vous pouvez utiliser pour modéliser, visualiser et automatiser les étapes nécessaires à la publication continue des modifications apportées à vos logiciels.
- Amazon DynamoDB — DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité.
- AWS Glue — AWS Glue est un service ETL entièrement géré qui facilite la préparation et le chargement des données à des fins d'analyse.

- AWS Lambda — Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif. Amazon S3 peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- AWS Step Functions - AWS Step Functions est un orchestrateur de fonctions sans serveur qui facilite le séquençage des fonctions AWS Lambda et de multiples services AWS dans des applications critiques pour l'entreprise.
- Amazon SQS — Amazon Simple Queue Service (Amazon SQS) est un service de mise en file d'attente de messages entièrement géré qui vous aide à découpler et à dimensionner les microservices, les systèmes distribués et les applications sans serveur.
- Deequ — Deequ est un outil qui vous aide à calculer les mesures de qualité des données pour de grands ensembles de données, à définir et à vérifier les contraintes de qualité des données et à rester informé des changements dans la distribution des données.

Référentiel de code

Le code source et les ressources du SDLF sont disponibles dans le GitHub référentiel AWS Labs.

Épopées

Configurer le pipeline CI/CD pour approvisionner l'iAc

Tâche	Description	Compétences requises
Configurez le pipeline CI/CD pour gérer l'IaC pour le lac de données.	Connectez-vous à l'AWS Management Console et suivez les étapes décrites dans la section Configuration initiale de l'atelier SDLF. Cela crée les ressources CI/CD initiales, telles que les CodeCommit référentiels, les CodeBuild environnements et les CodePipeline pipelines qui	DevOps ingénieur

Tâche	Description	Compétences requises
	fournissent et gèrent l'IaC pour le lac de données.	

Contrôle de version de l'iAc

Tâche	Description	Compétences requises
Clonez le CodeCommit dépôt sur votre machine locale.	Suivez les étapes décrites dans la section Déploiement des fondations de l'atelier SDLF. Cela vous permet de cloner le dépôt Git qui héberge IaC dans votre environnement local. Pour plus d'informations, consultez la section Connexion aux CodeCommit référentiels dans la CodeCommit documentation.	DevOps ingénieur
Modifiez les CloudFormation modèles.	Utilisez votre poste de travail local et un éditeur de code pour modifier les CloudFormation modèles en fonction de vos cas d'utilisation ou de vos besoins. Commettez-les dans le dépôt Git cloné localement. Pour plus d'informations, consultez la section Travailler avec les CloudFormation modèles AWS dans la CloudFormation documentation AWS.	DevOps ingénieur

Tâche	Description	Compétences requises
Transférez les modifications au CodeCommit référentiel.	Votre code d'infrastructure est désormais sous contrôle de version et les modifications apportées à votre base de code sont suivies. Lorsque vous apportez une modification au CodeCommit référentiel, celle-ci est CodePipeline automatiquement appliquée à votre infrastructure et transmise à CodeBuild. **⚠ Important** Si vous utilisez l'interface de ligne de commande AWS SAM dans CodeBuild, exécutez les `sam deploy` commandes `sam package` and. Si vous utilisez l'AWS CLI, exécutez les `aws cloudformation deploy` commandes `aws cloudformation package` and.	DevOps ingénieur

Ressources connexes

Configurer le pipeline CI/CD pour approvisionner l'iAc

- Atelier SDLF — Configuration initiale

Contrôle de version de l'iAc

- Atelier SDLF — Déployer les fondations
- Connexion aux CodeCommit référentiels
- Utilisation de CloudFormation modèles AWS

Autres ressources

- Architecture de référence du pipeline d'analyse de données sans serveur AWS
- Documentation SDLF

Appliquer le balisage des clusters Amazon EMR au lancement

Créée par Priyanka Chaudhary (AWS)

Récapitulatif

Ce modèle fournit un contrôle de sécurité qui garantit que les clusters Amazon EMR sont balisés lors de leur création.

Amazon EMR est un service Amazon Web Services (AWS) permettant de traiter et d'analyser de grandes quantités de données. Amazon EMR propose un service extensible à faible configuration qui constitue une alternative plus simple à l'exécution de clusters informatiques en interne. Vous pouvez utiliser le balisage pour classer les ressources AWS de différentes manières, par exemple en fonction de leur objectif, de leur propriétaire ou de leur environnement. Par exemple, vous pouvez baliser vos clusters Amazon EMR en attribuant des métadonnées personnalisées à chaque cluster. Une balise est composée d'une clé et d'une valeur que vous définissez. Nous vous recommandons de créer un ensemble cohérent de balises pour répondre aux exigences de votre organisation. Lorsque vous ajoutez une balise à un cluster Amazon EMR, la balise est également propagée à chaque instance Amazon Elastic Compute Cloud (Amazon EC2) active associée au cluster. De même, lorsque vous supprimez une balise d'un cluster Amazon EMR, cette balise est également supprimée de chaque EC2 instance active associée.

La commande de détection surveille les appels d'API et lance un événement Amazon CloudWatch Events pour les RunJobFlow, AddTagsRemoveTags, et CreateTags APIs. L'événement appelle AWS Lambda, qui exécute un script Python. La fonction Python obtient l'ID du cluster Amazon EMR à partir de l'entrée JSON de l'événement et effectue les vérifications suivantes :

- Vérifiez si le cluster Amazon EMR est configuré avec les noms de balises que vous spécifiez.
- Dans le cas contraire, envoyez une notification Amazon Simple Notification Service (Amazon SNS) à l'utilisateur avec les informations pertinentes : le nom du cluster Amazon EMR, les détails de la violation, la région AWS, le compte AWS et le nom de ressource Amazon (ARN) pour Lambda d'où provient cette notification.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

- Un bucket Amazon Simple Storage Service (Amazon S3) pour télécharger le code Lambda fourni. Vous pouvez également créer un compartiment S3 à cette fin, comme décrit dans la section Epics.
- Adresse e-mail active à laquelle vous souhaitez recevoir des notifications de violation.
- Liste des balises obligatoires que vous souhaitez vérifier.

Limites

- Ce contrôle de sécurité est régional. Vous devez le déployer dans chaque région AWS que vous souhaitez surveiller.

Versions du produit

- Amazon EMR version 4.8.0 et versions ultérieures.

Architecture

Architecture du flux de travail

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.
- Amazon CloudWatch Events - Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.

- Amazon EMR - Amazon EMR est un service Web qui simplifie la gestion des infrastructures de mégadonnées et le traitement efficace de grandes quantités de données.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Ce modèle inclut les pièces jointes suivantes :

- `EMRTagValidation.zip`— Le code Lambda pour le contrôle de sécurité.
- `EMRTagValidation.yml`— Le CloudFormation modèle qui définit l'événement et la fonction Lambda.

Épopées

Configuration du compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 pour héberger le fichier .zip de code Lambda. Ce compartiment S3 doit se trouver dans la même région AWS que le cluster Amazon EMR que	Architecte du cloud

Tâche	Description	Compétences requises
	vous souhaitez surveiller. Un nom de compartiment Amazon S3 est globalement unique et l'espace de noms est partagé entre tous les comptes AWS. Le nom du compartiment S3 ne peut pas inclure de barres obliques en tête.	
Téléchargez le code Lambda.	Téléchargez le fichier .zip de code Lambda fourni dans la section Pièces jointes dans le compartiment S3.	Architecte du cloud

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle AWS.	Ouvrez la CloudFormation console AWS dans la même région AWS que votre compartiment S3 et déployez le modèle. Pour plus d'informations sur le déploiement de CloudFormation modèles AWS, consultez la section Création d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation.	Architecte du cloud
Complétez les paramètres du modèle.	Lorsque vous lancez le modèle, les informati	Architecte du cloud

Tâche	Description	Compétences requises
	ons suivantes vous sont demandées : • Compartiment S3 : Spécifiez le compartiment que vous avez créé ou sélectionné dans le premier épisode épique. C'est ici que vous avez chargé le code Lambda joint (fichier .zip). • Clé S3 : Spécifiez l'emplacement du fichier Lambda .zip dans votre compartiment S3 (par exemple, nom de fichier .zip ou controls/ nom de fichier .zip). N'incluez pas de barres obliques en tête. • E-mail de notification : indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications Amazon SNS. • Noms des clés de balisage : indiquez les balises que vous souhaitez vérifier, dans une liste séparée par des virgules (par exemple,`ApplicationID` ,`Environment`). `Owner` L'événement CloudWatch Events surveille le cluster pour détecter ces balises et	

Tâche	Description	Compétences requises
	envoie une notification si elles ne sont pas trouvées. • Niveau de journalisation Lambda : Spécifiez le niveau et la fréquence de journalisation pour la fonction Lambda. Utilisez Info pour consigner des messages d'information détaillés sur la progression, Erreur pour les événement s d'erreur susceptibles de permettre la poursuite du déploiement et Avertisse ment pour les situations potentiellement dangereus es.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Vous devez confirmer cet abonnement par e-mail pour commencer à recevoir des notifications de violation.	Architecte du cloud

Ressources connexes

- Guide du développeur AWS Lambda
- Balisage de clusters dans Amazon EMR

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Assurez-vous que la journalisation d'Amazon EMR sur Amazon S3 est activée au lancement

Créée par Priyanka Chaudhary (AWS)

Récapitulatif

Ce modèle fournit un contrôle de sécurité qui surveille la configuration de journalisation pour les clusters Amazon EMR exécutés sur Amazon Web Services (AWS).

Amazon EMR est un outil AWS pour le traitement et l'analyse des mégadonnées. Amazon EMR propose le service extensible à faible configuration comme alternative à l'exécution de clusters informatiques en interne. Amazon EMR fournit deux types de clusters EMR.

- Clusters Amazon EMR transitoires : les clusters Amazon EMR transitoires s'arrêtent automatiquement et cessent d'entraîner des coûts une fois le traitement terminé.
- Clusters Amazon EMR persistants : les clusters Amazon EMR persistants continuent de s'exécuter une fois la tâche de traitement des données terminée.

Amazon EMR et Hadoop génèrent des fichiers journaux qui indiquent l'état du cluster. Par défaut, ils sont écrits sur le nœud principal dans le répertoire mnt/var/log//. Selon la façon dont vous configurez le cluster lorsque vous le lancez, vous pouvez également enregistrer ces journaux dans Amazon Simple Storage Service (Amazon S3) et les consulter via l'outil de débogage graphique. Notez que la journalisation Amazon S3 ne peut être spécifiée que lorsque le cluster est lancé. Avec cette configuration, les journaux sont envoyés du nœud principal à l'emplacement Amazon S3 toutes les 5 minutes. Pour les clusters transitoires, la journalisation Amazon S3 est importante car les clusters disparaissent une fois le traitement terminé, et ces fichiers journaux peuvent être utilisés pour déboguer les tâches ayant échoué.

Le modèle utilise un CloudFormation modèle AWS pour déployer un contrôle de sécurité qui surveille les appels d'API et lance Amazon CloudWatch Events le « »RunJobFlow. Le déclencheur invoque AWS Lambda, qui exécute un script Python. La fonction Lambda récupère l'ID du cluster EMR à partir de l'entrée JSON de l'événement et vérifie également la présence d'un URI du journal Amazon S3. Si aucune URI Amazon S3 n'est trouvée, la fonction Lambda envoie une notification Amazon Simple Notification Service (Amazon SNS) détaillant le nom du cluster EMR, les détails de la violation, la région AWS, le compte AWS et le nom de ressource Lambda Amazon (ARN) d'où provient la notification.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un compartiment S3 pour le fichier .zip de code Lambda
- Adresse e-mail à laquelle vous souhaitez recevoir la notification de violation

Limites

- Ce contrôle de détection est régional et doit être déployé dans les régions AWS que vous souhaitez surveiller.

Versions du produit

- Amazon EMR version 4.8.0 et versions ultérieures

Architecture

Pile technologique cible

- Événement Amazon CloudWatch Events
- Amazon EMR
- fonction Lambda
- Compartiment S3
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS CloudFormation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Outils

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer les ressources AWS en utilisant l'infrastructure sous forme de code.
- AWS Cloudwatch Events — AWS CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- Amazon EMR — Amazon EMR est une plateforme de clusters gérés qui simplifie l'exécution de frameworks de mégadonnées.
- AWS Lambda — AWS Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon S3 est une interface de services Web que vous pouvez utiliser pour stocker et récupérer n'importe quel volume de données, où que vous soyez sur le Web.
- Amazon SNS — Amazon SNS est un service Web qui coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Code

- Un fichier .zip du projet est disponible en pièce jointe.

Épopées

Définition du compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Pour héberger le fichier .zip de code Lambda, choisissez ou créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques en tête. Le nom d'un compartiment S3 est unique	Architecte du cloud

Tâche	Description	Compétences requises
	au monde et l'espace de noms est partagé par tous les comptes AWS. Votre compartiment S3 doit se trouver dans la même région AWS que le cluster Amazon EMR en cours d'évaluation.	

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le fichier .zip de code Lambda fourni dans la section « Pièces jointes » dans le compartiment S3. Le compartiment S3 doit se trouver dans la même région que le cluster Amazon EMR en cours d'évaluation.	Architecte du cloud

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle AWS.	Sur la CloudFormation console AWS, dans la même région que votre compartiment S3, déployez le CloudForm ation modèle AWS fourni en pièce jointe à ce modèle. Dans l'épopée suivante, indiquez les valeurs des paramètres. Pour plus d'informations sur le	Architecte du cloud

Tâche	Description	Compétences requises
	déploiement CloudFormation de modèles AWS, consultez la section « Ressources associées ».	

Complétez les paramètres dans le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Nommez le compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud
Fournissez la clé Amazon S3.	<directory><file-name>Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,/.zip).	Architecte du cloud
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. « Info » désigne des messages d'information détaillés sur le déroulement de l'application. Le terme « Erreur » désigne les événements d'erreur susceptibles de permettre à l'applica	Architecte du cloud

Tâche	Description	Compétences requises
	tion de continuer à fonctionn er. Le terme « Avertisse ment » désigne des situations potentiellement dangereuses.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail fournie. Vous devez confirmer cet abonnement par e-mail pour recevoir des notifications de violation.	Architecte du cloud

Ressources connexes

- AWS Lambda
- Journalisation Amazon EMR
- Déploiement de CloudFormation modèles AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Génération de données de test à l'aide d'une tâche AWS Glue et de Python

Créée par Moinul Al-Mamun (AWS)

Récapitulatif

Ce modèle vous montre comment générer rapidement et facilement des millions d'exemples de fichiers simultanément en créant une tâche AWS Glue écrite en Python. Les fichiers d'exemple sont stockés dans un compartiment Amazon Simple Storage Service (Amazon S3). La capacité à générer rapidement un grand nombre de fichiers d'exemple est importante pour tester ou évaluer les services dans le cloud AWS. Par exemple, vous pouvez tester les performances des DataBrew tâches AWS Glue Studio ou AWS Glue en analysant les données de millions de petits fichiers contenus dans un préfixe Amazon S3.

Bien que vous puissiez utiliser d'autres services AWS pour générer des exemples de jeux de données, nous vous recommandons d'utiliser AWS Glue. Vous n'avez pas besoin de gérer d'infrastructure car AWS Glue est un service de traitement de données sans serveur. Vous pouvez simplement apporter votre code et l'exécuter dans un cluster AWS Glue. En outre, AWS Glue fournit, configure et adapte les ressources nécessaires à l'exécution de vos tâches. Vous ne payez que pour les ressources utilisées par vos tâches pendant leur exécution.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI), installée et configurée pour fonctionner avec le compte AWS

Versions du produit

- Python 3.9
- Version 2 de l'interface de ligne de commande AWS

Limites

Le nombre maximum de tâches AWS Glue par déclencheur est de 50. Pour plus d'informations, consultez la section Points de terminaison et quotas AWS Glue.

Architecture

Le schéma suivant décrit un exemple d'architecture centré sur une tâche AWS Glue qui écrit sa sortie (c'est-à-dire des fichiers d'exemple) dans un compartiment S3.

Le diagramme inclut le flux de travail suivant :

1. Vous utilisez l'interface de ligne de commande AWS, la console de gestion AWS ou une API pour lancer la tâche AWS Glue. La CLI ou l'API AWS vous permet d'automatiser la parallélisation de la tâche invoquée et de réduire le temps d'exécution nécessaire à la génération de fichiers d'exemple.
2. La tâche AWS Glue génère le contenu du fichier de manière aléatoire, le convertit au format CSV, puis le stocke sous la forme d'un objet Amazon S3 sous un préfixe commun. Chaque fichier pèse moins d'un kilo-octet. La tâche AWS Glue accepte deux paramètres de tâche définis par l'utilisateur : `START_RANGE` et`END_RANGE`. Vous pouvez utiliser ces paramètres pour définir les noms de fichiers et le nombre de fichiers générés dans Amazon S3 par chaque tâche exécutée. Vous pouvez exécuter plusieurs instances de cette tâche en parallèle (par exemple, 100 instances).

Outils

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

Bonnes pratiques

Tenez compte des bonnes pratiques AWS Glue suivantes lors de la mise en œuvre de ce modèle :

- Utilisez le bon type de travailleur AWS Glue pour réduire les coûts. Nous vous recommandons de comprendre les différentes propriétés des types de travailleurs, puis de choisir le type de travailleur adapté à votre charge de travail en fonction des besoins en termes de processeur et de mémoire. Pour ce modèle, nous vous recommandons d'utiliser une tâche shell Python comme type de tâche afin de minimiser le DPU et de réduire les coûts. Pour plus d'informations, consultez la section Ajout de tâches dans AWS Glue dans le manuel AWS Glue Developer Guide.
- Utilisez la bonne limite de simultanéité pour adapter votre travail. Nous vous recommandons de baser la simultanéité maximale de votre tâche AWS Glue sur le temps nécessaire et le nombre de fichiers requis.
- Commencez par générer un petit nombre de fichiers. Pour réduire les coûts et gagner du temps lors de la création de vos tâches AWS Glue, commencez par un petit nombre de fichiers (1 000, par exemple). Cela peut faciliter le dépannage. Si la génération d'un petit nombre de fichiers est réussie, vous pouvez passer à un plus grand nombre de fichiers.
- Exécutez d'abord localement. Pour réduire les coûts et gagner du temps lors de la création de vos tâches AWS Glue, lancez le développement localement et testez votre code. Pour obtenir des instructions sur la configuration d'un conteneur Docker qui peut vous aider à écrire des tâches d'extraction, de transformation et de chargement (ETL) AWS Glue à la fois dans un shell et dans un environnement de développement intégré (IDE), consultez le billet Developing AWS Glue ETL local à l'aide d'un conteneur sur le blog AWS Big Data.

Pour en savoir plus sur les meilleures pratiques d'AWS Glue, consultez la section Meilleures pratiques de la documentation d'AWS Glue.

Épopées

Création d'un compartiment S3 de destination et d'un rôle IAM

Tâche	Description	Compétences requises
Créez un compartiment S3 pour stocker les fichiers.	Créez un compartiment S3 et un préfixe à l'intérieur de celui-ci.	Développeur d’applications

Tâche	Description	Compétences requises
	Note Ce modèle utilise l'`s3://{your-s3-bucket-name}/small-files/` emplacement à des fins de démonstration.	

Tâche	Description	Compétences requises
Créez et configurez un rôle IAM.	Vous devez créer un rôle IAM que votre tâche AWS Glue peut utiliser pour écrire dans votre compartiment S3. 1. Créez un rôle IAM (par exemple, appelé`"AWSGlueServiceRole-smallfiles"`). 2. Choisissez AWS Glue comme entité de confiance pour la politique. 3. Associez une politique gérée par AWS appelée `"AWSGlueServiceRole"` au rôle. 4. Créez une politique intégrée ou une politique gérée par le client appelée `"s3-small-file-access"` en fonction de la configuration suivante. `"{bucket}"` Remplacez-le par le nom de votre compartiment. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [`	Développeur d'applications

Tâche	Description	Compétences requises

	<pre>"s3:GetObject",
	
	"s3:PutObject"
	],
	"Resource
	": [
	
	"arn:aws:s3:::{buc
	ket}/small-files/i
	nput/*"
	]
	}
	]
	}</pre> 5. Associez la `"s3-small-file-access"` politique à votre rôle.	

Création et configuration d'une tâche AWS Glue pour gérer des exécutions simultanées

Tâche	Description	Compétences requises
Créez une tâche AWS Glue.	Vous devez créer une tâche AWS Glue qui génère votre contenu et le stocke dans un compartiment S3. Créez une tâche AWS Glue, puis configurez votre tâche en effectuant les étapes suivantes : 1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Glue.	Développeur d’applications

Tâche	Description	Compétences requises
	2. Dans le volet de navigation, sous Intégration des données et ETL, sélectionnez Jobs. 3. Dans la section Créer une tâche, choisissez l'éditeur de script Python Shell. 4. Dans la section Options, sélectionnez Créer un nouveau script avec un code standard, puis choisissez Créer. 5. Choisissez Détails du Job. 6. Dans Nom, entrez create_small_files. 7. Pour le rôle IAM, sélectionnez le rôle IAM que vous avez créé précédemment. 8. Dans la section This job runs, sélectionnez Un nouveau script que vous devez créer. 9. Développez les propriétés avancées. 10. Pour Maximum de simultanéité, entrez 100 à des fins de démonstration. Remarque : La simultanéité maximale définit le nombre d'instances du job que vous pouvez exécuter en parallèle. 11. Choisissez Enregistrer.	

Tâche	Description	Compétences requises

Mettez à jour le code de tâche.	1. Ouvrez la console AWS Glue.
	2. Dans le volet de navigation, sélectionnez Tâches.
	3. Dans la section Vos tâches, choisissez la tâche que vous avez créée précédemment.
	4. Choisissez l'onglet Script, puis mettez à jour le script en fonction du code suivant. Mettez à jour les `text_str` variables BUCKET_NAME `PREFIX`, et avec vos valeurs.
	`from awsglue.utils import getResolvedOptions`
	`import sys`
	`import boto3`
	`from random import randrange`
	
	`# Two arguments`
	`args = getResolvedOptions(sys.argv, ['START_RANGE', 'END_RANGE'])`
	
	`START_RANGE = int(args['START_RANGE'])`
	`END_RANGE = int(args['END_RANGE'])`
		Développeur d'applications

Tâche	Description	Compétences requises

	<pre>BUCKET_NAME = '{BUCKET_NAME}'
	PREFIX = 'small-files/input/'
	s3 = boto3.resource('s3')
	for x in range(START_RANGE, END_RANGE):
	    # generate file name
	    file_name = f"input_{x}.txt"
	    # generate text
	    text_str = str(randrange(100000))+","+str(randrange(100000))+", " + str(randrange(10000000)) + "," + str(randrange(10000))
	    # write in s3
	s3.Object(BUCKET_NAME, PREFIX + file_name).put(Body=text_str)</pre> 5. Choisissez Enregistrer.	

Exécutez le job AWS Glue depuis la ligne de commande ou la console

Tâche	Description	Compétences requises
Exécutez le job AWS Glue depuis la ligne de commande.	Pour exécuter votre tâche AWS Glue à partir de l'interface de ligne de commande AWS, exécutez la commande	Développeur d’applications

Tâche	Description	Compétences requises

	suivante à l'aide de vos valeurs :
	
	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"0","--END_RANGE":"1000000"}'`
	`cmd:~$ aws glue start-job-run --job-name create_small_files --arguments '{"--START_RANGE":"1000000","--END_RANGE":"2000000"}'`
	
	Note
	Pour obtenir des instructions sur l'exécution de la tâche AWS Glue depuis l'AWS Management Console, consultez l'article intitulé Exécuter la tâche AWS Glue dans l'AWS Management Console sur ce modèle.
	
	Tip
	Nous vous recommandons d'utiliser l'interface de	

Tâche	Description	Compétences requises
	ligne de commande AWS pour exécuter des tâches AWS Glue si vous souhaitez exécuter plusieurs exécutions à la fois avec des paramètre s différents, comme indiqué dans l'exemple ci-dessus.	

	Pour générer toutes les commandes de l'AWS CLI requises pour générer un nombre défini de fichiers à l'aide d'un certain facteur de parallélisation, exécutez le code bash suivant (en utilisant vos valeurs) :
	`# define parameters NUMBER_OF_FILES= 10000000; PARALLELIZATION=50;`
	`# initialize _SB=0;`
	`# generate commands for i in $(seq 1 $PARALLELIZATION); do echo aws glue start-job-run -- job-name create_sm all_files --argumen ts "'"'{"--START_RANG`	

Tâche	Description	Compétences requises

```
E":"'$(((NUMBER_OF
_FILES/PARALLELIZA
TION) * (i-1) +
 _SB))'","--END_RAN
GE":"'$(((NUMBER_O
F_FILES/PARALLELIZ
ATION) * (i)))'"}'"'";
      _SB=1;
done
```

Si vous utilisez le script ci-dessus, tenez compte des points suivants :

- Le script simplifie l'invocation et la génération de petits fichiers à grande échelle.
- Mettez à jour `NUMBER_OF_FILES` et `PARALLELIZATION` avec vos valeurs.
- Le script ci-dessus affiche la liste des commandes que vous devez exécuter. Copiez ces commandes de sortie, puis exécutez-les dans votre terminal.
- Si vous souhaitez exécuter les commandes directement depuis le script, supprimez l'`echo`instruction de la ligne 11.

> **Note**
>
> Pour voir un exemple de sortie du script ci-

Tâche	Description	Compétences requises
	dessus, consultez la section Sortie du script Shell dans la section Informations supplémentaires de ce modèle.	
Exécutez la tâche AWS Glue dans l'AWS Management Console.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Glue. 2. Dans le volet de navigation, sous Intégration des données et ETL, sélectionnez Jobs. 3. Dans la section Vos emplois, choisissez votre poste. 4. Dans la section Paramètres (facultatif), mettez à jour vos paramètres. 5. Choisissez Action, puis Run job. 6. Répétez les étapes 3 à 5 autant de fois que nécessaire. Par exemple, pour créer 10 millions de fichiers, répétez ce processus 10 fois.	Développeur d’applications

Tâche	Description	Compétences requises
Vérifiez le statut de votre tâche AWS Glue.	1. Ouvrez la console AWS Glue. 2. Dans le volet de navigation, sélectionnez Tâches. 3. Dans la section Vos tâches, choisissez la tâche que vous avez créée précédemment (c'est-à-dire `create_small_files`). 4. Pour avoir un aperçu de la progression et de la génération de vos fichiers, consultez les colonnes Run ID, Run Status et les autres colonnes.	Développeur d'applications

Ressources connexes

Références

- Registre des données ouvertes sur AWS
- Ensembles de données pour l'analyse
- Données ouvertes sur AWS
- Ajouter des tâches dans AWS Glue
- Commencer à utiliser AWS Glue

Guides et modèles

- Bonnes pratiques relatives à AWS Glue
- Tests de charge des applications

Informations supplémentaires

Test d'analyse comparative

Ce modèle a été utilisé pour générer 10 millions de fichiers en utilisant différents paramètres de parallélisation dans le cadre d'un test d'analyse comparative. Le tableau suivant montre le résultat du test :

Parallélisation	Nombre de fichiers générés par l'exécution d'une tâche	Durée du job	Speed (Vitesse)
10	1 000 000	6 heures, 40 minutes	Très lent
50	200 000	80 minutes	Modérée
100	100 000	40 minutes	Rapide

Si vous souhaitez accélérer le processus, vous pouvez configurer davantage d'exécutions simultanées dans la configuration de votre tâche. Vous pouvez facilement ajuster la configuration des tâches en fonction de vos besoins, mais gardez à l'esprit qu'il existe une limite de quota pour le service AWS Glue. Pour plus d'informations, consultez la section Points de terminaison et quotas AWS Glue.

Sortie du script Shell

L'exemple suivant montre la sortie du script shell de la tâche Run the AWS Glue à partir de l'histoire de la ligne de commande selon ce modèle.

```
user@MUC-1234567890 MINGW64 ~
  $ # define parameters
  NUMBER_OF_FILES=10000000;
  PARALLELIZATION=50;
  # initialize
  _SB=0;

  # generate commands
  for i in $(seq 1 $PARALLELIZATION);
   do
```

```
        echo aws glue start-job-run --job-name create_small_files --arguments
 "'"'{"--START_RANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i-1) + SB))'","--
ENDRANGE":"'$(((NUMBER_OF_FILES/PARALLELIZATION)  (i)))'"}'"'";
        _SB=1;
   done

  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"0","--END_RANGE":"200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"200001","--END_RANGE":"400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"400001","--END_RANGE":"600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"600001","--END_RANGE":"800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"800001","--END_RANGE":"1000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1000001","--END_RANGE":"1200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1200001","--END_RANGE":"1400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1400001","--END_RANGE":"1600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1600001","--END_RANGE":"1800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"1800001","--END_RANGE":"2000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2000001","--END_RANGE":"2200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2200001","--END_RANGE":"2400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2400001","--END_RANGE":"2600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2600001","--END_RANGE":"2800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"2800001","--END_RANGE":"3000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3000001","--END_RANGE":"3200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3200001","--END_RANGE":"3400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3400001","--END_RANGE":"3600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3600001","--END_RANGE":"3800000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"3800001","--END_RANGE":"4000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4000001","--END_RANGE":"4200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4200001","--END_RANGE":"4400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4400001","--END_RANGE":"4600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4600001","--END_RANGE":"4800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"4800001","--END_RANGE":"5000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5000001","--END_RANGE":"5200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5200001","--END_RANGE":"5400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5400001","--END_RANGE":"5600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5600001","--END_RANGE":"5800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"5800001","--END_RANGE":"6000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6000001","--END_RANGE":"6200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6200001","--END_RANGE":"6400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6400001","--END_RANGE":"6600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6600001","--END_RANGE":"6800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"6800001","--END_RANGE":"7000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7000001","--END_RANGE":"7200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7200001","--END_RANGE":"7400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7400001","--END_RANGE":"7600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7600001","--END_RANGE":"7800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"7800001","--END_RANGE":"8000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8000001","--END_RANGE":"8200000"}'
```

```
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8200001","--END_RANGE":"8400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8400001","--END_RANGE":"8600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8600001","--END_RANGE":"8800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"8800001","--END_RANGE":"9000000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9000001","--END_RANGE":"9200000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9200001","--END_RANGE":"9400000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9400001","--END_RANGE":"9600000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9600001","--END_RANGE":"9800000"}'
  aws glue start-job-run --job-name create_small_files --arguments '{"--
START_RANGE":"9800001","--END_RANGE":"10000000"}'

  user@MUC-1234567890 MINGW64 ~
```

FAQ

Combien d'exécutions simultanées ou de tâches parallèles dois-je utiliser ?

Le nombre d'exécutions simultanées et de tâches parallèles dépend du temps nécessaire et du nombre de fichiers de test souhaités. Nous vous recommandons de vérifier la taille des fichiers que vous créez. Vérifiez d'abord le temps nécessaire à une tâche AWS Glue pour générer le nombre de fichiers souhaité. Utilisez ensuite le bon nombre de courses simultanées pour atteindre vos objectifs. Par exemple, si vous supposez que l'exécution de 100 000 fichiers prend 40 minutes mais que votre durée cible est de 30 minutes, vous devez augmenter le paramètre de simultanéité pour votre tâche AWS Glue.

Quel type de contenu puis-je créer à l'aide de ce modèle ?

Vous pouvez créer n'importe quel type de contenu, tel que des fichiers texte avec différents délimiteurs (par exemple, PIPE, JSON ou CSV). Ce modèle utilise Boto3 pour écrire dans un fichier, puis enregistre le fichier dans un compartiment S3.

De quel niveau d'autorisation IAM ai-je besoin dans le compartiment S3 ?

Vous devez disposer d'une politique basée sur l'identité qui autorise `Write` l'accès aux objets de votre compartiment S3. Pour plus d'informations, consultez Amazon S3 : autorise l'accès en lecture et en écriture aux objets d'un compartiment S3 dans la documentation Amazon S3.

Ingérez de manière rentable des données IoT directement dans Amazon S3 à l'aide d'AWS IoT Greengrass

Créée par Sebastian Viviani (AWS) et Rizwan Syed (AWS)

Récapitulatif

Ce modèle vous montre comment ingérer de manière rentable des données de l'Internet des objets (IoT) directement dans un bucket Amazon Simple Storage Service (Amazon S3) à l'aide d'un appareil AWS IoT Greengrass version 2. L'appareil exécute un composant personnalisé qui lit les données IoT et les enregistre dans un stockage persistant (c'est-à-dire un disque ou un volume local). L'appareil compresse ensuite les données IoT dans un fichier Apache Parquet et les télécharge périodiquement dans un compartiment S3.

La quantité et la vitesse des données IoT que vous ingérez ne sont limitées que par les capacités de votre matériel de pointe et la bande passante de votre réseau. Vous pouvez utiliser Amazon Athena pour analyser de manière rentable les données ingérées. Athena prend en charge les fichiers Apache Parquet compressés et la visualisation des données à l'aide d'Amazon Managed Grafana.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une passerelle périphérique qui s'exécute sur AWS IoT Greengrass version 2 et collecte des données à partir de capteurs (les sources de données et le processus de collecte de données dépassent le cadre de ce modèle, mais vous pouvez utiliser presque tous les types de données de capteurs. Ce modèle utilise un broker MQTT local avec des capteurs ou des passerelles qui publient les données localement.)
- Composants, rôles et dépendances du SDK AWS IoT Greengrass
- Un composant de gestionnaire de flux pour télécharger les données dans le compartiment S3
- SDK AWS pour Java, SDK AWS pour ou SDK AWS JavaScript pour Python (Boto3) pour exécuter APIs

Limites

- Les données de ce modèle ne sont pas téléchargées en temps réel dans le compartiment S3. Il existe un délai, que vous pouvez configurer. Les données sont temporairement mises en mémoire tampon dans le périphérique périphérique, puis téléchargées une fois la période expirée.
- Le SDK est uniquement disponible en Java, Node.js et Python.

Architecture

Pile technologique cible

- Amazon S3
- AWS IoT Greengrass
- courtier MQTT
- Composant du gestionnaire de flux

Architecture cible

Le schéma suivant montre une architecture conçue pour ingérer les données des capteurs IoT et les stocker dans un compartiment S3.

Le schéma suivant illustre le flux de travail suivant :

1. Les mises à jour de plusieurs capteurs (par exemple, la température et les vannes) sont publiées sur un courtier MQTT local.
2. Le compresseur de fichiers Parquet abonné à ces capteurs met à jour les rubriques et reçoit ces mises à jour.
3. Le compresseur de fichiers Parquet stocke les mises à jour localement.
4. Une fois la période écoulée, les fichiers stockés sont compressés dans des fichiers Parquet et transmis au gestionnaire de flux pour être téléchargés dans le compartiment S3 spécifié.
5. Le gestionnaire de flux télécharge les fichiers Parquet dans le compartiment S3.

> **Note**
>
> Le gestionnaire de flux (`StreamManager`) est un composant géré. Pour des exemples d'exportation de données vers Amazon S3, consultez Stream manager dans la

documentation d'AWS IoT Greengrass. Vous pouvez utiliser un broker MQTT local comme composant ou un autre broker comme Eclipse Mosquitto.

Outils

Outils AWS

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS IoT Greengrass est un environnement d'exécution IoT Edge et un service cloud open source qui vous aident à créer, déployer et gérer des applications IoT sur vos appareils.

Autres outils

- Apache Parquet est un format de fichier de données open source orienté colonne conçu pour le stockage et la récupération.
- MQTT (Message Queuing Telemetry Transport) est un protocole de messagerie léger conçu pour les appareils limités.

Bonnes pratiques

Utilisez le bon format de partition pour les données téléchargées

Il n'existe aucune exigence spécifique concernant les noms de préfixes racines dans le compartiment S3 (par exemple, `"myAwesomeDataSet/"` ou`"dataFromSource"`), mais nous vous recommandons d'utiliser une partition et un préfixe significatifs afin de comprendre facilement l'objectif de l'ensemble de données.

Nous vous recommandons également d'utiliser le bon partitionnement dans Amazon S3 afin que les requêtes s'exécutent de manière optimale sur l'ensemble de données. Dans l'exemple suivant, les données sont partitionnées au format HIVE afin d'optimiser la quantité de données numérisées par chaque requête Athena. Cela améliore les performances et réduit les coûts.

```
s3://<ingestionBucket>/<rootPrefix>/year=YY/month=MM/day=DD/
HHMM_<suffix>.parquet
```

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises
Créez un compartiment S3.	1. Créez un compartiment S3 ou utilisez un compartiment existant. 2. Créez un préfixe significatif pour le compartiment S3 dans lequel vous souhaitez ingérer les données IoT (par exemple,`s3:\\<bucket>\<prefix>`). 3. Enregistrez votre préfixe pour une utilisation ultérieure.	Développeur d'applications
Ajoutez des autorisations IAM au compartiment S3.	Pour accorder aux utilisateurs un accès en écriture au compartiment S3 et au préfixe que vous avez créés précédemment, ajoutez la politique IAM suivante à votre rôle AWS IoT Greengrass : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "S3DataUpload", "Effect": "Allow", "Action": [ "s3:List*",`	Développeur d'applications

Tâche	Description	Compétences requises

	<pre>"s3:Put*"
	],
	"Resource":
	[
	
	"arn:aws:s3:::<ingestionBucket>",
	
	"arn:aws:s3:::<ingestionBucket>/<prefix>/*"
	]
	}
	]
	}</pre>
	Pour plus d'informations, consultez la section Création d'une politique IAM pour accéder aux ressources Amazon S3 dans la documentation Aurora.
	
	Ensuite, mettez à jour la politique de ressources (si nécessaire) pour le compartiment S3 afin d'autoriser l'accès en écriture avec les principes AWS appropriés.	

Créez et déployez le composant AWS IoT Greengrass

Tâche	Description	Compétences requises
Mettez à jour la recette du composant.	Mettez à jour la configuration des composants lorsque vous	Développeur d’applications

Tâche	Description	Compétences requises
	créez un déploiement en vous basant sur l'exemple suivant : `{ "region": "<region>", "parquet_period": <period>, "s3_bucket": "<s3Bucket>", "s3_key_prefix": "<s3prefix>" }` `<region>`Remplacez-le par votre région AWS, `<period>` par votre intervalle périodique, `<s3Bucket>` par votre compartiment S3 et `<s3prefix>` par votre préfixe.	

Tâche	Description	Compétences requises
Créez le composant.	Effectuez l'une des actions suivantes : • Créez le composant. • Ajoutez le composant au pipeline CI/CD (s'il en existe un). Veillez à copier l'artefact depuis le référentiel d'artefacts vers le bucket d'artefacts AWS IoT Greengrass. Créez ou mettez à jour votre composant AWS IoT Greengrass. • **Note** Ajoutez le broker MQTT en tant que composant ou ajoutez-le manuellement ultérieurement. : Cette décision affecte le schéma d'authentification que vous pouvez utiliser avec le courtier. L'ajout manuel d'un courtier dissocie celui-ci d'AWS IoT Greengrass et active tout schéma d'authentification	Développeur d'applications

Tâche	Description	Compétences requises
	pris en charge par le courtier. Les composants du broker fournis par AWS ont des schémas d'authentification prédéfinis. Pour plus d'informations, consultez le courtier MQTT 3.1.1 (Moquette) et le courtier MQTT 5 (EMQX).	
Mettez à jour le client MQTT.	L'exemple de code n'utilise pas l'authentification car le composant se connecte localement au courtier. Si votre scénario est différent, mettez à jour la section du client MQTT selon vos besoins. Procédez également comme suit : 1. Mettez à jour les rubriques MQTT de l'abonnement. 2. Mettez à jour l'analyseur de messages MQTT selon les besoins, car les messages provenant de chaque source peuvent différer.	Développeur d’applications

Ajoutez le composant à l'appareil principal AWS IoT Greengrass version 2

Tâche	Description	Compétences requises
Mettez à jour le déploiement du périphérique principal.	Si le déploiement du dispositif principal AWS IoT Greengrass version 2 existe déjà, revoyez le déploiement. Si le déploiement n'existe pas, créez-en un nouveau. Pour attribuer le nom correct au composant, mettez à jour la configuration du gestionnaire de journaux pour le nouveau composant (si nécessaire) en fonction des éléments suivants : `{ "logsUploaderConfiguration": { "systemLogsConfiguration": { ... }, "componentLogsConfigurationMap": { "<com.iot.ingest.parquet>": { "minimumLogLevel": "INFO", "diskSpaceLimit": "20", "diskSpaceLimitUnit": "MB", "deleteLogFileAfterCloudUpload": "false" } ...`	Développeur d’applications

Tâche	Description	Compétences requises

	<pre> }
	  },
	  "periodicUploadInterval Sec": "300"
	}</pre> Enfin, terminez la révision du déploiement de votre appareil principal AWS IoT Greengrass.	

Vérifiez l'ingestion de données dans le compartiment S3

Tâche	Description	Compétences requises
Consultez les journaux du volume AWS IoT Greengrass.	Vérifiez les points suivants : • Le client MQTT est correctement connecté au courtier MQTT local. • Le client MQTT est abonné aux bonnes rubriques. • Des messages de mise à jour du capteur sont envoyés au broker sur les sujets MQTT. • La compression du parquet se produit à chaque intervalle périodique.	Développeur d’applications
Vérifiez le compartiment S3.	Vérifiez si les données sont téléchargées dans le compartiment S3. Vous pouvez voir les fichiers téléchargés à chaque période.	Développeur d’applications

Tâche	Description	Compétences requises
	Vous pouvez également vérifier si les données sont chargées dans le compartiment S3 en interrogeant les données dans la section suivante.	

Configurer les requêtes depuis Athéna

Tâche	Description	Compétences requises
Créez une base de données et une table.	1. Créez une base de données AWS Glue (si nécessaire). 2. Créez une table dans AWS Glue manuellement ou en exécutant un robot d'exploration dans AWS Glue.	Développeur d’applications
Accordez à Athéna l'accès aux données.	1. Mettez à jour les autorisations pour permettre à Athena d'accéder au compartiment S3. Pour plus d'informations, consultez la section Accès détaillé aux bases de données et aux tables dans le catalogue de données AWS Glue dans la documentation Athena. 2. Interrogez la table de votre base de données.	Développeur d’applications

Résolution des problèmes

Problème	Solution
Le client MQTT ne parvient pas à se connecter	• Validez les autorisations sur le broker MQTT. Si vous avez un courtier MQTT d'AWS, consultez le courtier MQTT 3.1.1 (Moquette) et le courtier MQTT 5 (EMQX). • Validez les informations d'identification sur le client MQTT. Si vous avez un courtier MQTT d'AWS, consultez le courtier MQTT 3.1.1 (Moquette) et le courtier MQTT 5 (EMQX).
Le client MQTT ne parvient pas à s'abonner	Validez les autorisations sur le broker MQTT. Si vous avez un courtier MQTT d'AWS, consultez le courtier MQTT 3.1.1 (Moquette) et le courtier MQTT 5 (EMQX).
Les fichiers de parquet ne sont pas créés	• Vérifiez que les rubriques MQTT sont correctes. • Vérifiez que le format des messages MQTT émis par les capteurs est correct.
Les objets ne sont pas chargés dans le compartiment S3	• Vérifiez que vous disposez d'une connectivité Internet et d'une connectivité aux terminaux. • Vérifiez que la politique de ressources de votre compartiment S3 est correcte. • Vérifiez les autorisations pour le rôle d'appareil principal d'AWS IoT Greengrass version 2.

Ressources connexes

- DataFrame(Documentation sur les pandas)
- Documentation d'Apache Parquet (documentation de Parquet)

- Développement de composants AWS IoT Greengrass (Guide du développeur AWS IoT Greengrass, version 2)
- Déploiement de composants AWS IoT Greengrass sur des appareils (Guide du développeur AWS IoT Greengrass, version 2)
- Interagissez avec des appareils IoT locaux (Guide du développeur AWS IoT Greengrass, version 2)
- Courtier MQTT 3.1.1 (Moquette) (Guide du développeur AWS IoT Greengrass, version 2)
- Broker MQTT 5 (EMQX) (Guide du développeur AWS IoT Greengrass, version 2)

Informations supplémentaires

Analyse des coûts

Le scénario d'analyse des coûts suivant montre comment l'approche d'ingestion de données décrite dans ce modèle peut avoir un impact sur les coûts d'ingestion de données dans le cloud AWS. Les exemples de tarification de ce scénario sont basés sur les prix au moment de la publication. Les prix sont susceptibles d'être modifiés. En outre, vos coûts peuvent varier en fonction de votre région AWS, des quotas de service AWS et d'autres facteurs liés à votre environnement cloud.

Set de signaux d'entrée

Cette analyse utilise l'ensemble de signaux d'entrée suivant comme base pour comparer les coûts d'ingestion de l'IoT avec les autres alternatives disponibles.

Nombre de signaux	Frequency (Fréquence)	Données par signal
125	25 Hz	8 bytes

Dans ce scénario, le système reçoit 125 signaux. Chaque signal est de 8 octets et se produit toutes les 40 millisecondes (25 Hz). Ces signaux peuvent être fournis individuellement ou regroupés dans une charge utile commune. Vous avez la possibilité de diviser et de regrouper ces signaux en fonction de vos besoins. Vous pouvez également déterminer la latence. La latence correspond à la période pendant laquelle les données sont reçues, accumulées et ingérées.

À des fins de comparaison, l'opération d'ingestion pour ce scénario est basée dans la région `us-east-1` AWS. La comparaison des coûts s'applique uniquement aux services AWS. Les autres coûts, tels que le matériel ou la connectivité, ne sont pas pris en compte dans l'analyse.

Comparaisons de coûts

Le tableau suivant indique le coût mensuel en dollars américains (USD) pour chaque méthode d'ingestion.

Method	Coût mensuel
AWS IoT SiteWise *	331.77 USD
AWS IoT SiteWise Edge avec pack de traitement des données (conservation de toutes les données à la périphérie)	200 DOLLARS AMÉRICAINS
Règles d'accès aux données brutes d'AWS IoT Core et d'Amazon S3	84.54 DOLLARS AMÉRICAINS
Compression de fichiers Parquet à la périphérie et téléchargement vers Amazon S3	0,5 DOLLARS AMÉRICAINS

*Les données doivent être sous-échantillonnées pour respecter les quotas de service. Cela signifie qu'il y a une certaine perte de données avec cette méthode.

Méthodes alternatives

Cette section indique les coûts équivalents pour les méthodes alternatives suivantes :

- AWS IoT SiteWise — Chaque signal doit être chargé dans un message individuel. Par conséquent, le nombre total de messages par mois est de 125 × 25 × 3600 × 24 × 30, soit 8,1 milliards de messages par mois. Cependant, AWS IoT ne SiteWise peut gérer que 10 points de données par seconde et par propriété. En supposant que les données soient sous-échantillonnées à 10 Hz, le nombre de messages par mois est réduit à 125 × 10 × 3600 × 24 × 30, soit 3,24 milliards. Si vous utilisez le composant éditeur qui regroupe les mesures par groupes de 10 (à 1 USD par million de messages), vous obtenez un coût mensuel de 324 USD par mois. En supposant que chaque message est de 8 octets (1 Kb/125), cela représente 25,92 Go de stockage de données. Cela ajoute un coût mensuel de 7,77 USD par mois. Le coût total pour le premier mois est de 331,77 USD et augmente de 7,77 USD par mois.
- AWS IoT SiteWise Edge avec pack de traitement des données, comprenant tous les modèles et signaux entièrement traités en périphérie (c'est-à-dire sans ingestion du cloud) : vous pouvez

utiliser le pack de traitement des données comme alternative pour réduire les coûts et configurer tous les modèles calculés à la périphérie. Cela peut fonctionner uniquement pour le stockage et la visualisation, même si aucun calcul réel n'est effectué. Dans ce cas, il est nécessaire d'utiliser un matériel puissant pour la passerelle Edge. Il y a un coût fixe de 200 USD par mois.

- Intégration directe à AWS IoT Core par MQTT et règle IoT pour stocker les données brutes dans Amazon S3 — En supposant que tous les signaux soient publiés dans une charge utile commune, le nombre total de messages publiés sur AWS IoT Core est de 25 × 3600 × 24 × 30, soit 64,8 millions par mois. À 1 USD par million de messages, cela représente un coût mensuel de 64,8 USD par mois. À 0,15 USD par million d'activations de règles et à raison d'une règle par message, cela ajoute un coût mensuel de 19,44 USD par mois. Au coût de 0,023 USD par Go de stockage dans Amazon S3, cela ajoute 1,5 USD par mois (augmentation mensuelle pour refléter les nouvelles données). Le coût total pour le premier mois est de 84,54 USD et augmente de 1,5 USD par mois.
- Compression des données en périphérie dans un fichier Parquet et chargement vers Amazon S3 (méthode proposée) : le taux de compression dépend du type de données. Avec les mêmes données industrielles testées pour le MQTT, le total des données de sortie pour un mois complet est de 1,2 Go. Cela coûte 0,03 USD par mois. Les taux de compression (basés sur des données aléatoires) décrits dans d'autres benchmarks sont de l'ordre de 66 % (ce qui est plus proche du pire des scénarios). Le total des données est de 21 Go et coûte 0,5 USD par mois.

Générateur de fichiers pour parquet

L'exemple de code suivant montre la structure d'un générateur de fichiers Parquet écrit en Python. L'exemple de code est fourni à titre d'illustration uniquement et ne fonctionnera pas s'il est collé dans votre environnement.

```
import queue
import paho.mqtt.client as mqtt
import pandas as pd

#queue for decoupling the MQTT thread
messageQueue = queue.Queue()
client = mqtt.Client()
streammanager = StreamManagerClient()

def feederListener(topic, message):
    payload = {
        "topic" : topic,
        "payload" : message,
    }
```

```
    messageQueue.put_nowait(payload)

def on_connect(client_instance, userdata, flags, rc):
    client.subscribe("#",qos=0)

def on_message(client, userdata, message):
    feederListener(topic=str(message.topic),
 message=str(message.payload.decode("utf-8")))


filename = "tempfile.parquet"
streamname = "mystream"
destination_bucket= "amzn-s3-demo-bucket"
keyname="mykey"
period= 60

client.on_connect = on_connect
client.on_message = on_message
streammanager.create_message_stream(
            MessageStreamDefinition(name=streamname,
 strategy_on_full=StrategyOnFull.OverwriteOldestData)
        )


while True:
   try:
       message = messageQueue.get(timeout=myArgs.mqtt_timeout)
   except (queue.Empty):
       logger.warning("MQTT message reception timed out")

   currentTimestamp = getCurrentTime()
   if currentTimestamp >= nextUploadTimestamp:
       df = pd.DataFrame.from_dict(accumulator)
       df.to_parquet(filename)
       s3_export_task_definition = S3ExportTaskDefinition(input_url=filename,
 bucket=destination_bucket, key=key_name)
       streammanager.append_message(streamname,
 Util.validate_and_serialize_to_json_bytes(s3_export_task_definition))
       accumulator = {}
       nextUploadTimestamp += period
   else:
        accumulator.append(message)
```

Lancer une tâche Spark dans un cluster EMR transitoire à l'aide d'une fonction Lambda

Créée par Dhrubajyoti Mukherjee (AWS)

Récapitulatif

Ce modèle utilise l'action d' RunJobFlow API Amazon EMR pour lancer un cluster transitoire afin d'exécuter une tâche Spark à partir d'une fonction Lambda. Un cluster EMR transitoire est conçu pour s'arrêter dès que le travail est terminé ou en cas d'erreur. Un cluster transitoire permet de réaliser des économies car il ne s'exécute que pendant le temps de calcul et offre évolutivité et flexibilité dans un environnement cloud.

Le cluster EMR transitoire est lancé à l'aide de l'API Boto3 et du langage de programmation Python dans une fonction Lambda. La fonction Lambda, écrite en Python, offre la flexibilité supplémentaire de lancer le cluster lorsque cela est nécessaire.

Pour illustrer un exemple de calcul et de sortie par lots, ce modèle lancera une tâche Spark dans un cluster EMR à partir d'une fonction Lambda et exécutera un calcul par lots sur la base des données de vente d'exemple d'une entreprise fictive. La sortie de la tâche Spark sera un fichier de valeurs séparées par des virgules (CSV) dans Amazon Simple Storage Service (Amazon S3). Le fichier de données d'entrée, le fichier Spark .jar, un extrait de code et un CloudFormation modèle AWS pour un cloud privé virtuel (VPC) et les rôles AWS Identity and Access Management (IAM) permettant d'exécuter le calcul sont fournis en pièce jointe.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

Limites

- Une seule tâche Spark peut être initiée à partir du code à la fois.

Versions du produit

- Testé sur Amazon EMR 6.0.0

Architecture

Pile technologique cible

- Amazon EMR
- AWS Lambda
- Amazon S3
- Apache Spark

Architecture cible

Automatisation et mise à l'échelle

Pour automatiser le calcul par lots de Spark-EMR, vous pouvez utiliser l'une des options suivantes.

- Implémentez une EventBridge règle Amazon capable de lancer la fonction Lambda dans un calendrier cron. Pour plus d'informations, consultez Tutoriel : Programmez les fonctions AWS Lambda à l'aide de. EventBridge
- Configurez les notifications d'événements Amazon S3 pour lancer la fonction Lambda à l'arrivée du fichier.
- Transmettez les paramètres d'entrée à la fonction AWS Lambda via le corps de l'événement et les variables d'environnement Lambda.

Outils

Services AWS

- Amazon EMR est une plate-forme de cluster gérée qui simplifie l'exécution de frameworks de mégadonnées sur AWS afin de traiter et d'analyser de grandes quantités de données.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Apache Spark est un moteur d'analyse multilingue destiné au traitement de données à grande échelle.

Épopées

Création des rôles Amazon EMR et Lambda IAM et du VPC

Tâche	Description	Compétences requises
Créez les rôles IAM et le VPC.	Si vous possédez déjà les rôles IAM AWS Lambda et Amazon EMR ainsi qu'un VPC, vous pouvez ignorer cette étape. Pour exécuter le code, le cluster EMR et la fonction Lambda nécessite nt des rôles IAM. Le cluster EMR nécessite également un VPC avec un sous-rése au public ou un sous-rése au privé avec une passerell e NAT. Pour créer automatiq uement tous les rôles IAM et un VPC, déployez le modèle CloudFormation AWS joint tel quel, ou vous pouvez créer les rôles et le VPC manuellement comme indiqué dans la section Informations supplémentaires.	Architecte du cloud
Notez les clés de sortie du CloudFormation modèle AWS.	Une fois le CloudFormation modèle déployé avec succès, accédez à l'onglet Outputs de la CloudFormation console	Architecte du cloud

Tâche	Description	Compétences requises
	AWS. Notez les cinq touches de sortie : • `S3Bucket` • `LambdaExecutionRole` • `ServiceRole` • `JobFlowRole` • `Ec2SubnetId` Vous utiliserez les valeurs de ces clés lorsque vous créerez la fonction Lambda.	

Téléchargez le fichier Spark .jar

Tâche	Description	Compétences requises
Téléchargez le fichier .jar Spark.	Téléchargez le fichier .jar Spark dans le compartiment S3 créé par la CloudFormation pile AWS. Le nom du bucket est identique à celui de la clé de sortie`S3Bucket`.	AWS général

Créez la fonction Lambda pour lancer le cluster EMR

Tâche	Description	Compétences requises
Créez une fonction Lambda.	Sur la console Lambda, créez une fonction Lambda Python 3.9+ avec un rôle d'exécution. La politique de rôle d'exécuti on doit permettre à Lambda de	Ingénieur de données, ingénieur cloud

Tâche	Description	Compétences requises
	lancer un cluster EMR. (Voir le CloudFormation modèle AWS ci-joint.)	
Copiez et collez le code.	Remplacez le code du `lambda_function.py` fichier par le code de la section Informations supplémentaires de ce modèle.	Ingénieur de données, ingénieur cloud
Modifiez les paramètres du code.	Suivez les commentaires du code pour modifier les valeurs des paramètres en fonction de votre compte AWS.	Ingénieur de données, ingénieur cloud
Lancez la fonction pour lancer le cluster.	Lancez la fonction pour lancer la création d'un cluster EMR transitoire à l'aide du fichier Spark .jar fourni. Il exécutera la tâche Spark et s'arrêtera automatiquement lorsque la tâche sera terminée.	Ingénieur de données, ingénieur cloud
Vérifiez l'état du cluster EMR.	Une fois le cluster EMR lancé, il apparaît dans la console Amazon EMR sous l'onglet Clusters. Toute erreur lors du lancement du cluster ou de l'exécution de la tâche peut être vérifiée en conséquence.	Ingénieur de données, ingénieur cloud

Configuration et exécution de l'exemple de démonstration

Tâche	Description	Compétences requises
Téléchargez le fichier .jar Spark.	Téléchargez le fichier Spark .jar depuis la section Pièces jointes et chargez-le dans le compartiment S3.	Ingénieur de données, ingénieur cloud
Téléchargez le jeu de données en entrée.	Téléchargez le `fake_sales_data.csv` fichier joint dans le compartiment S3.	Ingénieur de données, ingénieur cloud
Collez le code Lambda et modifiez les paramètres.	Copiez le code de la section Outils, puis collez-le dans une fonction Lambda en remplaçant le fichier de code`lambda_function.py` . Modifiez les valeurs des paramètres pour qu'elles correspondent à celles de votre compte.	Ingénieur de données, ingénieur cloud
Lancez la fonction et vérifiez le résultat.	Une fois que la fonction Lambda a lancé le cluster avec la tâche Spark fournie, elle génère un fichier .csv dans le compartiment S3.	Ingénieur de données, ingénieur cloud

Ressources connexes

- Construire Spark
- Apache Spark et Amazon EMR
- Documentation de Boto3 Docs run_job_flow
- Informations et documentation sur Apache Spark

Informations supplémentaires

Code

```
"""
Copy paste the following code in your Lambda function. Make sure to change the
 following key parameters for the API as per your account

-Name (Name of Spark cluster)
-LogUri (S3 bucket to store EMR logs)
-Ec2SubnetId (The subnet to launch the cluster into)
-JobFlowRole (Service role for EC2)
-ServiceRole (Service role for Amazon EMR)

The following parameters are additional parameters for the Spark job itself. Change the
 bucket name and prefix for the Spark job (located at the bottom).

-s3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar (Spark jar file)
-s3://your-bucket-name/prefix/fake_sales_data.csv (Input data file in S3)
-s3://your-bucket-name/prefix/outputs/report_1/ (Output location in S3)
"""
import boto3

client = boto3.client('emr')


def lambda_handler(event, context):
    response = client.run_job_flow(
        Name='spark_job_cluster',
        LogUri='s3://your-bucket-name/prefix/logs',
        ReleaseLabel='emr-6.0.0',
        Instances={
            'MasterInstanceType': 'm5.xlarge',
            'SlaveInstanceType': 'm5.large',
            'InstanceCount': 1,
            'KeepJobFlowAliveWhenNoSteps': False,
            'TerminationProtected': False,
            'Ec2SubnetId': 'subnet-XXXXXXXXXXXXX'
        },
        Applications=[{'Name': 'Spark'}],
        Configurations=[
            {'Classification': 'spark-hive-site',
             'Properties': {
```

```
                'hive.metastore.client.factory.class':
'com.amazonaws.glue.catalog.metastore.AWSGlueDataCatalogHiveClientFactory'}
            }
        ],
        VisibleToAllUsers=True,
        JobFlowRole='EMRLambda-EMREC2InstanceProfile-XXXXXXXXX',
        ServiceRole='EMRLambda-EMRRole-XXXXXXXXX',
        Steps=[
            {
                'Name': 'flow-log-analysis',
                'ActionOnFailure': 'TERMINATE_CLUSTER',
                'HadoopJarStep': {
                    'Jar': 'command-runner.jar',
                    'Args': [
                        'spark-submit',
                        '--deploy-mode', 'cluster',
                        '--executor-memory', '6G',
                        '--num-executors', '1',
                        '--executor-cores', '2',
                        '--class', 'com.aws.emr.ProfitCalc',
                        's3://your-bucket-name/prefix/lambda-emr/SparkProfitCalc.jar',
                        's3://your-bucket-name/prefix/fake_sales_data.csv',
                        's3://your-bucket-name/prefix/outputs/report_1/'
                    ]
                }
            }
        ]
    )
```

Rôles IAM et création de VPC

Pour lancer le cluster EMR dans une fonction Lambda, un VPC et des rôles IAM sont nécessaires. Vous pouvez configurer les rôles VPC et IAM à l'aide du CloudFormation modèle AWS dans la section Pièces jointes de ce modèle, ou vous pouvez les créer manuellement en utilisant les liens suivants.

Les rôles IAM suivants sont requis pour exécuter Lambda et Amazon EMR.

Rôle d'exécution Lambda

Le rôle d'exécution d'une fonction Lambda lui donne l'autorisation d'accéder aux services et ressources AWS.

Rôle de service pour Amazon EMR

Le rôle Amazon EMR définit les actions autorisées pour Amazon EMR lors du provisionnement de ressources et de l'exécution de tâches de niveau de service qui ne sont pas effectuées dans le contexte d'une instance Amazon Elastic Compute Cloud (Amazon) exécutée au sein d'un cluster. EC2 Par exemple, le rôle de service est utilisé pour provisionner EC2 des instances lors du lancement d'un cluster.

Rôle de service pour les EC2 instances

Le rôle de service pour les EC2 instances de cluster (également appelé profil d' EC2 instance pour Amazon EMR) est un type spécial de rôle de service attribué à chaque EC2 instance d'un cluster Amazon EMR lors du lancement de l'instance. Les processus d'application qui s'exécutent sur Apache Hadoop assument ce rôle pour les autorisations d'interaction avec d'autres services AWS.

Création de VPC et de sous-réseaux

Vous pouvez créer un VPC à partir de la console VPC.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrez les charges de travail Apache Cassandra vers Amazon Keyspaces à l'aide d'AWS Glue

Créée par Nikolai Kolesnikov (AWS), Karthiga Priya Chandran (AWS) et Samir Patel (AWS)

Récapitulatif

Ce modèle vous montre comment migrer vos charges de travail Apache Cassandra existantes vers Amazon Keyspaces (pour Apache Cassandra) à l'aide d'AWS Glue. CQLReplicator Vous pouvez utiliser CQLReplicator AWS Glue pour réduire à quelques minutes le délai de réplication lié à la migration de vos charges de travail. Vous apprendrez également à utiliser un bucket Amazon Simple Storage Service (Amazon S3) pour stocker les données nécessaires à la migration, notamment les fichiers Apache Parquet, les fichiers de configuration et les scripts. Ce modèle suppose que vos charges de travail Cassandra sont hébergées sur des instances Amazon Elastic Compute Cloud EC2 (Amazon) dans un cloud privé virtuel (VPC).

Conditions préalables et limitations

Prérequis

- Cluster Cassandra avec table source
- Table cible dans Amazon Keyspaces pour répliquer la charge de travail
- Compartiment S3 pour stocker les fichiers Parquet intermédiaires contenant des modifications de données incrémentielles
- Compartiment S3 pour stocker les fichiers de configuration des tâches et les scripts

Limites

- CQLReplicator sur AWS Glue nécessite un certain temps pour fournir des unités de traitement des données (DPUs) pour les charges de travail de Cassandra. Le délai de réplication entre le cluster Cassandra et l'espace de touches et la table cibles dans Amazon Keyspaces ne durera probablement que quelques minutes.

Architecture

Pile technologique source

- Apache Cassandra
- DataStax serveur
- ScyllaDB

Pile technologique cible

- Amazon Keyspaces

Architecture de migration

Le schéma suivant montre un exemple d'architecture dans lequel un cluster Cassandra est hébergé sur des EC2 instances et réparti sur trois zones de disponibilité. Les nœuds Cassandra sont hébergés dans des sous-réseaux privés.

Le schéma suivant illustre le flux de travail suivant :

1. Un rôle de service personnalisé permet d'accéder à Amazon Keyspaces et au compartiment S3.
2. Une tâche AWS Glue lit la configuration de la tâche et les scripts contenus dans le compartiment S3.
3. La tâche AWS Glue se connecte via le port 9042 pour lire les données du cluster Cassandra.
4. La tâche AWS Glue se connecte via le port 9142 pour écrire des données sur Amazon Keyspaces.

Outils

Services et outils AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS CloudShell est un shell basé sur un navigateur que vous pouvez utiliser pour gérer les services AWS à l'aide de l'AWS Command Line Interface (AWS CLI) et d'une gamme d'outils de développement préinstallés.
- AWS Glue est un service ETL entièrement géré qui vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.

- Amazon Keyspaces (pour Apache Cassandra) est un service de base de données géré qui vous aide à migrer, exécuter et dimensionner vos charges de travail Cassandra dans le cloud AWS.

Code

Le code de ce modèle est disponible dans le GitHub CQLReplicatorréférentiel.

Bonnes pratiques

- Pour déterminer les ressources AWS Glue nécessaires à la migration, estimez le nombre de lignes de la table source Cassandra. Par exemple, 250 000 lignes par 0,25 DPU (2 VCPUs, 4 Go de mémoire) avec un disque de 84 Go.
- Préchauffez les tables Amazon Keyspaces avant de les lancer. CQLReplicator Par exemple, huit CQLReplicator tuiles (tâches AWS Glue) peuvent écrire jusqu'à 22 K WCUs par seconde. La cible doit donc être préchauffée à 25-30 K WCUs par seconde.
- Pour activer la communication entre les composants AWS Glue, utilisez une règle d'autoréférencement entrant pour tous les ports TCP de votre groupe de sécurité.
- Utilisez la stratégie de trafic incrémentiel pour répartir la charge de travail de migration dans le temps.

Épopées

Déployer CQLReplicator

Tâche	Description	Compétences requises
Créez un espace de touches et un tableau cibles.	1. Créez un espace de touches et un tableau dans Amazon Keyspaces. Pour plus d'informations sur la capacité d'écriture, voir Calculs des unités d'écriture dans la section Informations supplémentaires de ce modèle.	Propriétaire de l'application, administrateur AWS, DBA, développeur d'applications

Tâche	Description	Compétences requises
	Vous pouvez également créer un espace de touches à l'aide du langage de requête Cassandra (CQL). Pour plus d'informations, voir Création d'un espace de touches à l'aide de CQL dans la section Informations supplémentaires de ce modèle. **Note** Après avoir créé le tableau, pensez à le faire passer en mode capacité à la demande pour éviter des frais inutiles. 2. Pour passer en mode débit, exécutez le script suivant : `ALTER TABLE target_keyspace.target_table WITH CUSTOM_PROPERTIES = { 'capacity_mode': { 'throughput_mode': 'PAY_PER_REQUEST'} }`	

Tâche	Description	Compétences requises
Configurez le pilote Cassandra pour vous connecter à Cassandra.	Utilisez le script de configuration suivant : `Datastax-java-driver { basic.request.consistency = “LOCAL_QUORUM” basic.contact-points = [“127.0.0.1:9042”] advanced.reconnect-on-init = true basic.load-balancing-policy { local-datacenter = “datacenter1” } advanced.auth-provider = { class = PlainTextAuthProvider username = “user-at-sample” password = “S@MPLE=PASSWORD=” } }` **Note** Le script précédent utilise le connecteur Spark Cassandra. Pour plus d'informations, consultez la configuration	DBA

Tâche	Description	Compétences requises
	de référence pour Cassandra.	

Tâche	Description	Compétences requises

Configurez le pilote Cassandra pour vous connecter à Amazon Keyspaces.	Utilisez le script de configuration suivant :
	`datastax-java-driver {`
	`basic {`
	`  load-balancing-pol`
	`icy {`
	`  local-datacenter =`
	` us-west-2`
	`  }`
	`  contact-points = [`
	`  "cassandr`
	`a.us-west-2.amazon`
	`aws.com:9142"`
	`  ]`
	`  request {`
	`  page-size = 2500`
	`  timeout = 360 seconds`
	`  consistency =`
	` LOCAL_QUORUM`
	`  }`
	`  }`
	`advanced {`
	` control-connection {`
	`  timeout = 360 seconds`
	`  }`
	` session-leak.thres`
	`hold = 6`
	` connection {`
	` connect-timeout = 360`
	` seconds`
	` init-query-timeout =`
	` 360 seconds`
	` warn-on-init-error =`
	` false`
	`  }`
	` auth-provider = {`
	`  class = software.`
	`aws.mcs.auth.SigV4`
	`AuthProvider`
		DBA

Tâche	Description	Compétences requises

	<pre> aws-region = us-
	west-2
	 }
	
	 ssl-engine-factory {
	  class = DefaultSs
	lEngineFactory
	        }
	    }
	}</pre>
	Note
	Le script précédent utilise le connecteur Spark Cassandra. Pour plus d'informations, consultez la configuration de référence pour Cassandra.	

Tâche	Description	Compétences requises
Créez un rôle IAM pour la tâche AWS Glue.	Créez un nouveau rôle de service AWS nommé `glue-cassandra-migration` avec AWS Glue en tant qu'entité de confiance. **Note** Ils `glue-cassandra-migration` devraient fournir un accès en lecture et en écriture au compartiment S3 et à Amazon Keyspaces . Le compartiment S3 contient les fichiers .jar, les fichiers de configuration pour Amazon Keyspaces et Cassandra, ainsi que les fichiers Parquet intermédiaires. Par exemple, il contient le `AWSGlueServiceRole` `AmazonS3FullAccess` , et les politiques `AmazonKeyspacesFullAccess` gérées.	AWS DevOps

Tâche	Description	Compétences requises

Téléchargez CQLReplicator dans AWS CloudShell.	Téléchargez le projet dans votre dossier personnel en exécutant la commande suivante :
	`git clone https://github.com/aws-samples/cql-replicator.git`
	`cd cql-replicator/glue`
	`# Only for AWS CloudShell, the bc package includes bc and dc. Bc is an arbitrary precision numeric processing arithmetic language`
	`sudo yum install bc -y`	

Modifiez les fichiers de configuration de référence.	Copiez `CassandraConnector.conf` et `KeyspacesConnector.conf` dans le `../glue/conf` répertoire du dossier du projet.	AWS DevOps

Tâche	Description	Compétences requises

Lancez le processus de migration.	La commande suivante initialise l' CQLReplicator environnement. L'initialisation implique de copier des artefacts .jar et de créer un connecteur AWS Glue, un compartiment S3, une tâche AWS Glue, le `migration` keyspace et la table : `ledger`
	
	`cd cql-replicator/glue/bin`
	`./cqlreplicator --state init --sg '"sg-1","sg-2"' \ --subnet "subnet-XXXXXXXXXXXX" \ --az us-west-2a --region us-west-2 \ --glue-iam-role glue-cassandra-migration \ --landing-zone s3://cql-replicator-1234567890-us-west-2`
	
	Le script comprend les paramètres suivants :
	
	• `--sg`— Les groupes de sécurité qui autorisent l'accès au cluster Cassandra depuis AWS Glue et incluent la règle
		AWS DevOps

Tâche	Description	Compétences requises
	d'autoréférencement entrant pour l'ensemble du trafic • `--subnet`— Le sous-rése au auquel appartient le cluster Cassandra • `--az`— La zone de disponibilité du sous-réseau • `--region`— La région AWS dans laquelle le cluster Cassandra est déployé • `--glue-iam-role` — Les autorisations de rôle IAM qu'AWS Glue peut assumer lorsque vous appelez Amazon Keyspaces et Amazon S3 en votre nom • `--landing zone`— Paramètre facultatif pour la réutilisation d'un compartim ent S3 (si vous ne fournisse z pas de valeur pour le `--landing zone` paramètre, le `init` processus essaiera de créer un nouveau compartiment pour stocker les fichiers de configura tion, les artefacts .jar et les fichiers intermédiaires.)	

Tâche	Description	Compétences requises
Validez le déploiement.	Après avoir exécuté la commande précédente, le compte AWS doit contenir les éléments suivants : • La tâche CQLReplicator AWS Glue et le connecteur AWS Glue dans AWS Glue • Le compartiment S3 qui stocke les artefacts • L'espace de touches cible `migration` et le `ledger` tableau dans Amazon Keyspaces	AWS DevOps

Courir CQLReplicator

Tâche	Description	Compétences requises
Lancez le processus de migration.	Pour utiliser CQLReplicator AWS Glue, vous devez utiliser la `--state run` commande, suivie d'une série de paramètres. La configuration précise de ces paramètres est principalement déterminée par vos exigences uniques en matière de migration. Par exemple, ces paramètres peuvent varier si vous choisissez de répliquer les valeurs de durée de vie (TTL) et les mises à jour, ou si vous	AWS DevOps

Tâche	Description	Compétences requises
	déchargez des objets de plus de 1 Mo vers Amazon S3. Pour répliquer la charge de travail du cluster Cassandra vers Amazon Keyspaces , exécutez la commande suivante : `./cqlreplicator --state run --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace \ --src-table source_table \ --trg-keyspace taget_keyspace \ --writetime-column column_name \ --trg-table target_table --inc-traffic` Votre keyspace source et votre table se trouvent `source_keyspace.source_table` dans le cluster Cassandra. Votre espace de touches et votre	

Tâche	Description	Compétences requises
	table cibles se trouvent `target_keyspace.target_table` dans Amazon Keyspaces. Ce paramètre `--inc-traffic` permet d'éviter que le trafic incrémentiel ne surcharge le cluster Cassandra et Amazon Keyspaces avec un nombre élevé de demandes. Pour répliquer les mises à jour, ajoutez-les `--writetime-column regular_column_name` à votre ligne de commande. La colonne normale va être utilisée comme source de l'horodatage d'écriture.	

Surveiller le processus de migration

Tâche	Description	Compétences requises
Validez les lignes Cassandra migrées pendant la phase de migration historique.	Pour obtenir le nombre de lignes répliquées pendant la phase de remblayage, exécutez la commande suivante : `./cqlreplicator --state stats \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \`	AWS DevOps

Tâche	Description	Compétences requises
	`--src-keyspace source_keyspace --src-table source_table --region us-west-2`	

Arrêtez le processus de migration

Tâche	Description	Compétences requises
Utilisez la `cqlreplicator` commande ou la console AWS Glue.	Pour arrêter le processus de migration correctement, exécutez la commande suivante : `./cqlreplicator --state request-stop --tiles 8 \ --landing-zone s3://cql-replicator-1234567890-us-west-2 \ --region us-west-2 \ --src-keyspace source_keyspace --src-table source_table` Pour arrêter immédiatement le processus de migration, utilisez la console AWS Glue.	AWS DevOps

Nettoyage

Tâche	Description	Compétences requises
Supprimez les ressources déployées.	La commande suivante supprimera la tâche AWS Glue, le connecteur, le compartiment S3 et la table Keyspaces : `ledger` `./cqlreplicator --state cleanup --landing-zone s3://cql-replicator-1234567890-us-west-2`	AWS DevOps

Résolution des problèmes

Problème	Solution
Les tâches AWS Glue ont échoué et ont renvoyé une erreur OOM (Out of Memory).	1. Modifiez le type de travailleur (agrandissez). Par exemple, changez `G0.25X` de `G.1X` ou `G.1X` de`G.2X`. Vous pouvez également augmenter le nombre de DPUs par tâche AWS Glue (scalez vers l'extérieur) CQLReplicator. 2. Démarrez le processus de migration à partir du point où il a été interrompu. Pour redémarrer les CQLReplicator tâches qui ont échoué, réexécutez la `--state run` commande avec les mêmes paramètres.

Ressources connexes

- CQLReplicator avec AWS Glue README.MD

- Documentation d'AWS Glue
- Documentation Amazon Keyspaces
- Apache Cassandre

Informations supplémentaires

Considérations concernant la migration

Vous pouvez utiliser AWS Glue pour migrer votre charge de travail Cassandra vers Amazon Keyspaces, tout en préservant le bon fonctionnement de vos bases de données sources Cassandra pendant le processus de migration. Une fois la réplication terminée, vous pouvez choisir de transférer vos applications vers Amazon Keyspaces avec un délai de réplication minimal (moins de quelques minutes) entre le cluster Cassandra et Amazon Keyspaces. Pour garantir la cohérence des données, vous pouvez également utiliser un pipeline similaire pour répliquer les données vers le cluster Cassandra à partir d'Amazon Keyspaces.

Écrire des calculs unitaires

Par exemple, imaginez que vous avez l'intention d'écrire 500 000 000 avec une taille de ligne de 1 KiB pendant une heure. Le nombre total d'unités d'écriture Amazon Keyspaces (WCUs) dont vous avez besoin est basé sur ce calcul :

```
(number of rows/60 mins 60s) 1 WCU per row = (500,000,000/(60*60s) * 1 WCU)
= 69,444 WCUs required
```

69 444 dollars WCUs par seconde, c'est le tarif pour une heure, mais vous pouvez ajouter une certaine marge de manœuvre pour couvrir les frais généraux. Par exemple, `69,444 * 1.10 = 76,388 WCUs` a des frais généraux de 10 %.

Création d'un espace de touches à l'aide de CQL

Pour créer un espace de touches à l'aide de CQL, exécutez les commandes suivantes :

```
CREATE KEYSPACE target_keyspace WITH replication = {'class': 'SingleRegionStrategy'}
CREATE TABLE target_keyspace.target_table ( userid uuid, level text, gameid int,
 description text, nickname text, zip text, email text, updatetime text, PRIMARY KEY
 (userid, level, gameid) ) WITH default_time_to_live = 0 AND CUSTOM_PROPERTIES =
 {'capacity_mode':{ 'throughput_mode':'PROVISIONED', 'write_capacity_units':76388,
 'read_capacity_units':3612 }} AND CLUSTERING ORDER BY (level ASC, gameid ASC)
```

Migrez les données Hadoop vers Amazon S3 à l'aide de Migrator WANdisco LiveData

Créée par Tony Velcich

Récapitulatif

Ce modèle décrit le processus de migration des données Apache Hadoop d'un système de fichiers distribué Hadoop (HDFS) vers Amazon Simple Storage Service (Amazon S3). Il utilise WANdisco LiveData Migrator pour automatiser le processus de migration des données.

Conditions préalables et limitations

Prérequis

- Nœud périphérique du cluster Hadoop sur lequel LiveData Migrator sera installé. Le nœud doit répondre aux exigences suivantes :
  - Spécifications minimales : 4 CPUs, 16 Go de RAM, 100 Go de stockage.
  - Réseau de 2 Gbit/s minimum.
  - Le port 8081 est accessible sur votre nœud périphérique pour accéder à l' WANdisco interface utilisateur.
  - Java 1.8 64 bits.
  - Bibliothèques clientes Hadoop installées sur le nœud Edge.
  - Possibilité de s'authentifier en tant que superutilisateur HDFS (par exemple, « hdfs »).
  - Si Kerberos est activé sur votre cluster Hadoop, un keytab valide contenant un principal adapté au superutilisateur HDFS doit être disponible sur le nœud Edge.
- Un compte AWS actif avec accès à un compartiment S3.
- Un lien AWS Direct Connect établi entre votre cluster Hadoop sur site (en particulier le nœud périphérique) et AWS.

Versions du produit

- LiveData Migrateur 1.8.6
- WANdisco Interface utilisateur (OneUI) 5.8.0

Architecture

Pile technologique source

- Cluster Hadoop sur site

Pile technologique cible

- Amazon S3

Architecture

Le schéma suivant montre l'architecture de la solution LiveData Migrator.

Le flux de travail comprend quatre composants principaux pour la migration des données d'un HDFS sur site vers Amazon S3.

- LiveData Migrateur : automatise la migration des données de HDFS vers Amazon S3 et réside sur un nœud périphérique du cluster Hadoop.
- HDFS : système de fichiers distribué qui fournit un accès haut débit aux données des applications.
- Amazon S3 — Un service de stockage d'objets qui offre évolutivité, disponibilité des données, sécurité et performances.
- AWS Direct Connect : service qui établit une connexion réseau dédiée entre vos centres de données sur site et AWS.

Automatisation et mise à l'échelle

Vous créerez généralement plusieurs migrations afin de pouvoir sélectionner un contenu spécifique de votre système de fichiers source par chemin ou répertoire. Vous pouvez également migrer des données vers plusieurs systèmes de fichiers indépendants en même temps en définissant plusieurs ressources de migration.

Épopées

Configurer le stockage Amazon S3 dans votre compte AWS

Tâche	Description	Compétences requises
Ouvrez une session de votre compte AWS.	Connectez-vous à la console de gestion AWS et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.	Expérience AWS
Créez un compartiment S3.	Si vous n'avez pas encore de compartiment S3 à utiliser comme espace de stockage cible, choisissez l'option « Créer un compartiment » sur la console Amazon S3 et spécifiez le nom du compartiment, la région AWS et les paramètres du compartiment pour bloquer l'accès public. AWS et WANdisco nous vous recommandons d'activer les options de blocage de l'accès public pour le compartiment S3 et de configurer les politiques d'accès au compartiment et d'autorisation des utilisateurs afin de répondre aux exigences de votre organisation. Un exemple AWS est fourni à l'https://docs.aws.amazon.com/AmazonS3/latest/dev/exampleadresse - walkthroughs-	Expérience AWS

Tâche	Description	Compétences requises
	managing-access-example 1.html.	

Installez LiveData Migrator

Tâche	Description	Compétences requises
Téléchargez le programme d'installation de LiveData Migrator.	Téléchargez le programme d'installation de LiveData Migrator et chargez-le sur le nœud Hadoop Edge. Vous pouvez télécharger une version d'essai gratuite de LiveData Migrator sur / aws.amazon. https://w ww2.wandisco.com/ldm-trial. You can also obtain access to LiveData Migrator from AWS Marketplace, at https:/ com/ marketplace/pp/B07B8SZND9.	Administrateur Hadoop, propriétaire de l'application
Installez LiveData Migrator.	Utilisez le programme d'install ation téléchargé et installez LiveData Migrator en tant que superutilisateur HDFS sur un nœud périphérique de votre cluster Hadoop. Consultez la section « Informations supplémentaires » pour les commandes d'installation.	Administrateur Hadoop, propriétaire de l'application
Vérifiez l'état de LiveData Migrator et des autres services.	Vérifiez l'état du LiveData migrateur, du migrateur Hive et de l' WANdisco interface utilisateur à l'aide	Administrateur Hadoop, propriétaire de l'application

Tâche	Description	Compétences requises
	des commandes fournies dans la section « Informations supplémentaires ».	

Configuration du stockage via l' WANdisco interface utilisateur

Tâche	Description	Compétences requises
Enregistrez votre compte LiveData Migrator.	Connectez-vous à l' WANdisco interface utilisateur via un navigateur Web sur le port 8081 (sur le nœud Hadoop Edge) et fournissez vos informations pour l'enregis trement. Par exemple, si vous exécutez LiveData Migrator sur un hôte nommé myldmhost.example.com, l'URL serait : http://my ldmhost.example.com:8081	Propriétaire de l'application
Configurez votre stockage HDFS source.	Fournissez les détails de configuration nécessaires pour votre stockage HDFS source. Cela inclura la valeur « fs.DefaultFS » et un nom de stockage défini par l'utilisa teur. Si Kerberos est activé, indiquez l'emplacement principal et l'emplacement keytab que LiveData Migrator doit utiliser. Si NameNode HA est activé sur le cluster, fournissez un chemin d'accès aux fichiers core-site.xml et	Administrateur Hadoop, propriétaire de l'application

Tâche	Description	Compétences requises
	hdfs-site.xml sur le nœud Edge.	
Configurez votre espace de stockage Amazon S3 cible.	Ajoutez votre stockage cible en tant que type S3a. Indiquez le nom de stockage défini par l'utilisateur et le nom du compartiment S3. Entrez « org.apache.hadoop.fs.s3a.fournisseur simple AWSCredentials » pour l'option Credentials Provider, puis fournissez les clés d'accès et secrètes AWS pour le compartiment S3. Des propriétés S3a supplémentaires seront également nécessaires. Pour plus de détails, consultez la section « Propriétés du S3a » dans la documentation du LiveData migrateur à l'adresse https://docs.wandisco.com/live-data-migrator/ filesystem-add-s docs/command-reference/#3a.	AWS, propriétaire de l'application

Préparez-vous à la migration

Tâche	Description	Compétences requises
Ajoutez des exclusions (si nécessaire).	Si vous souhaitez exclure des ensembles de données spécifiques de la migration, ajoutez des exclusions pour le stockage HDFS source.	Administrateur Hadoop, propriétaire de l'application

Tâche	Description	Compétences requises
	Ces exclusions peuvent être basées sur la taille du fichier, les noms de fichiers (basés sur des modèles regex) et la date de modification.	

Création et lancement de la migration

Tâche	Description	Compétences requises
Créez et configurez la migration.	Créez une migration dans le tableau de bord de l' WANdisco interface utilisate ur. Choisissez votre source (HDFS) et votre cible (le compartiment S3). Ajoutez les nouvelles exclusions que vous avez définies à l'étape précédente. Sélectionnez l'option « Remplacer » ou « Ignorer si la taille correspon d ». Créez la migration lorsque tous les champs sont remplis.	Administrateur Hadoop, propriétaire de l'application
Lancez la migration.	Sur le tableau de bord, sélectionnez la migration que vous avez créée. Cliquez pour démarrer la migration. Vous pouvez également démarrer une migration automatiq uement en choisissant l'option de démarrage automatiq ue lorsque vous créez la migration.	Propriétaire de l'application

Gérer la bande passante (facultatif)

Tâche	Description	Compétences requises
Définissez une limite de bande passante réseau entre la source et la cible.	Dans la liste des stockages du tableau de bord, sélection nez votre stockage source et sélectionnez « Gestion de la bande passante » dans la liste des regroupements. Désactivez l'option illimitée et définissez la limite et l'unité de bande passante maximales. Choisissez « Appliquer ».	Propriétaire de l'application, mise en réseau

Surveiller et gérer les migrations

Tâche	Description	Compétences requises
Consultez les informations de migration à l'aide de l' WANdisco interface utilisateur.	Utilisez l' WANdisco interface utilisateur pour consulter les informations de licence, de bande passante, de stockage et de migration. L'interface utilisateur fournit également un système de notification qui vous permet de recevoir des notifications concernant les erreurs, les avertissements ou les étapes importantes de votre utilisation.	Administrateur Hadoop, propriétaire de l'application
Arrêtez, reprenez et supprimez les migrations.	Vous pouvez empêcher une migration de transférer le contenu vers sa cible en le plaçant à l'état STOPPÉ. Les	Administrateur Hadoop, propriétaire de l'application

Tâche	Description	Compétences requises
	migrations arrêtées peuvent être reprises. Les migration s à l'état STOPPÉ peuvent également être supprimées.	

Ressources connexes

- LiveData Documentation sur le migrateur
- LiveData Migrateur sur AWS Marketplace
- WANdisco LiveData Démonstration de Migrator (vidéo)

Informations supplémentaires

Installation de LiveData Migrator

Vous pouvez utiliser les commandes suivantes pour installer LiveData Migrator, en supposant que le programme d'installation se trouve dans votre répertoire de travail :

```
su - hdfs
chmod +x livedata-migrator.sh && sudo ./livedata-migrator.sh
```

Vérification de l'état de LiveData Migrator et des autres services après l'installation

Utilisez les commandes suivantes pour vérifier l'état du LiveData migrateur, du migrateur Hive et de l'interface utilisateur : WANdisco

```
service livedata-migrator status
service hivemigrator status
service livedata-ui status
```

Migrer Oracle Business Intelligence 12c vers le cloud AWS à partir de serveurs sur site

Créée par Lanre (Lan-Ray) showunmi (AWS) et Patrick Huang (AWS)

Récapitulatif

Ce modèle montre comment migrer Oracle Business Intelligence Enterprise Edition 12c depuis des serveurs sur site vers le cloud AWS à l'aide d'AWS. CloudFormation Il décrit également comment vous pouvez utiliser d'autres services AWS pour implémenter des composants Oracle BI 12c offrant une haute disponibilité, une sécurité, une flexibilité et une capacité d'évolution dynamique.

Pour obtenir une liste des meilleures pratiques relatives à la migration d'Oracle BI 12c vers le cloud AWS, consultez la section Informations supplémentaires de ce modèle.

> **Note**
>
> Il est recommandé d'exécuter plusieurs migrations de test avant de transférer vos données Oracle BI 12c existantes vers le cloud. Ces tests vous aident à affiner votre approche de migration, à identifier et à résoudre les problèmes potentiels et à estimer les besoins en temps d'arrêt avec plus de précision.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Connectivité réseau sécurisée entre vos serveurs sur site et AWS via les services de réseau privé virtuel (VPN AWS) ou AWS Direct Connect
- Licences logicielles pour votre système d'exploitation Oracle, Oracle BI 12c, Oracle Database, Oracle WebLogic Server et Oracle HTTP Server

Limites

Pour plus d'informations sur les limites de taille de stockage, consultez la documentation Amazon Relational Database Service (Amazon RDS) pour Oracle.

Versions du produit

- Oracle Business Intelligence Enterprise Edition 12c
- WebLogic Serveur Oracle 12c
- Serveur HTTP Oracle 12c
- Oracle Database 12c (ou version ultérieure)
- Oracle Java SE 8

Architecture

Le schéma suivant montre un exemple d'architecture permettant d'exécuter des composants Oracle BI 12c dans le cloud AWS :

Ce schéma montre l'architecture suivante :

1. Amazon Route 53 fournit la configuration du service de nom de domaine (DNS).
2. Elastic Load Balancing (ELB) répartit le trafic réseau afin d'améliorer l'évolutivité et la disponibilité des composants Oracle BI 12c sur plusieurs zones de disponibilité.
3. Les groupes Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling hébergent les serveurs HTTP Oracle, le serveur d'administration Weblogic et les serveurs de BI gérés dans plusieurs zones de disponibilité.
4. Les bases de données Amazon Relational Database Service (Amazon RDS) pour Oracle stockent les métadonnées du serveur BI dans plusieurs zones de disponibilité.
5. Amazon Elastic File System (Amazon EFS) est monté sur chaque composant Oracle BI 12c pour le stockage de fichiers partagés.

Pile technologique

- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic File System (Amazon EFS)
- Amazon RDS for Oracle
- AWS Certificate Manager (ACM)

- Elastic Load Balancing (ELB)
- Oracle BI 12c
- WebLogic Serveur Oracle 12c
- Serveur HTTP Oracle (OHS)

Outils

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS Certificate Manager (ACM) vous aide à créer, stocker et renouveler les certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et applications AWS.
- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les faire rapidement évoluer vers le haut ou vers le bas.
- Amazon EC2 Auto Scaling vous aide à maintenir la disponibilité des applications et vous permet d'ajouter ou de supprimer automatiquement EC2 des instances Amazon selon les conditions que vous définissez.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS.
- Elastic Load Balancing répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

- Oracle Data Pump vous aide à déplacer des données et des métadonnées d'une base de données à une autre à grande vitesse.
- Oracle Fusion Middleware est une suite d'outils de développement d'applications et de solutions d'intégration pour la gestion des identités, la collaboration et les rapports de business intelligence.
- Oracle vous GoldenGate aide à concevoir, exécuter, orchestrer et surveiller vos solutions de réplication et de traitement des données en continu dans l'infrastructure cloud Oracle.
- Oracle WebLogic Scripting Tool (WLST) fournit une interface de ligne de commande qui vous permet de dimensionner horizontalement vos WebLogic clusters.

Épopées

Évaluer l'environnement source

Tâche	Description	Compétences requises
Rassemblez les informations d'inventaire des logiciels.	Identifiez les versions et les niveaux de correctif pour chacun des composants logiciels de votre infrastructure technologique source, notamment les suivants : • Système d'exploitation Oracle • Oracle Database • Oracle BI 12c • WebLogic Serveur Oracle • Serveur HTTP Oracle • Java	Architecte de migration, architecte de solutions, propriétaire de l'application, administrateur Oracle BI
Collectez des informations d'inventaire de calcul et de stockage.	Dans votre environnement source, passez en revue les indicateurs d'utilisation actuels et historiques pour les éléments suivants :	Architecte de migration, architecte de solutions, propriétaire de l'application, administrateur Oracle BI, administrateur système

Tâche	Description	Compétences requises
	• Utilisation de l'UC • Utilisation de la mémoire • Utilisation du stockage ⚠ Important Assurez-vous de tenir compte des pics d'utilisation historiques.	
Rassemblez des informations sur l'architecture de l'environnement source et ses exigences.	Obtenez une compréhension complète de l'architecture de votre environnement source et de ses exigences, notamment en ce qui concerne les éléments suivants : • Configuration WebLogic du domaine du serveur Oracle • Regroupement • Equilibrage de charge • Connectivité • Disponibilité • Exigences relatives à la reprise après sinistre	Architecte de migration, architecte de solutions, propriétaire de l'application, administrateur Oracle BI
Identifiez les sources de données JDBC (Java Database Connectivity).	Rassemblez des informations sur les sources de données et les pilotes JDBC de votre environnement source pour chaque moteur de base de données qu'il utilise.	Architecte de migration, propriétaire de l'application, administrateur Oracle BI, ingénieur ou administrateur de base de données

Tâche	Description	Compétences requises
Rassemblez des informations sur les paramètres spécifiques à l'environnement.	Collectez des informations sur les paramètres et les configurations spécifiques à votre environnement source, notamment les suivants : • Scripts de démarrage et d'arrêt personnalisés • Java et autres variables d'environnement • Certificats	Architecte de migration , architecte de solutions, propriétaire de l'application, administrateur Oracle BI
Identifiez toute dépendance vis-à-vis d'autres applications.	Collectez des informations sur les intégrations dans votre environnement source qui créent des dépendances avec d'autres applications. **Important** Assurez-vous d'identifier les intégrations du protocole LDAP (Lightweight Directory Access Protocol) et les autres exigences réseau.	Architecte de migration , architecte de solutions, propriétaire de l'application, administrateur Oracle BI

Concevez votre environnement cible

Tâche	Description	Compétences requises
Créez un document de conception de haut niveau.	Créez un document de conception d'architecture	Architecte de solutions, Architecte d'applications,

Tâche	Description	Compétences requises
	cible. Assurez-vous d'utiliser les informations que vous avez collectées lors de l'évaluation de votre environnement source pour éclairer le document de conception.	Ingénieur de base de données, Architecte de migration
Obtenir l'approbation du document de conception.	Passez en revue le document de conception avec les parties prenantes et obtenez les approbations requises.	Responsable de l'application ou du service, architecte de solutions, architecte d'applications

Déployer l'infrastructure

Tâche	Description	Compétences requises
Préparez le code d'infrastructure dans CloudFormation.	Créez des CloudFormation modèles pour provisionner votre infrastructure Oracle BI 12c dans le cloud AWS. Pour plus d'informations, consultez la section Utilisation des CloudFormation modèles AWS dans le guide de CloudFormation l'utilisateur AWS. **Note** Il est recommandé de créer des CloudFormation modèles modulaires pour chaque niveau	Architecte d'infrastructure cloud, architecte de solutions, architecte d'applications

Tâche	Description	Compétences requises
	d'Oracle BI 12c, plutôt qu'un seul modèle volumineu x pour toutes vos ressources. Pour plus d'informations sur les CloudForm ation meilleures pratiques, consultez les 8 meilleures pratiques relatives à l'automatisation de vos déploiements avec AWS CloudFormation sur le blog AWS.	
Téléchargez le logiciel requis.	DDownload les logiciels suivants ainsi que les versions et correctifs requis sur le site Web d'Oracle : • Java JDK8 • WebLogic Serveur Oracle 12c • Oracle BI 12c	Architecte de migration , ingénieur de base de données, architecte d'applica tions

Tâche	Description	Compétences requises
Préparez les scripts d'installation.	Créez des scripts d'installation logicielle qui exécutent une installation silencieuse. Ces scripts simplifient l'automatisation du déploiement. Pour plus d'informations, voir OBIEE 12c : Comment effectuer une installation silencieuse ? sur le site Oracle Support. Vous avez besoin d'un compte Oracle Support pour consulter la documentation.	Architecte de migration, ingénieur de base de données, architecte d'applications

Tâche	Description	Compétences requises
Créez une AMI Linux basée sur Amazon EBS pour vos niveaux Web et applicatif.	1. Déployez et configurez EC2 des instances Amazon pour vos niveaux Web et applicatif. Assurez-vous que les instances répondent aux conditions requises pour exécuter les opérations suivantes : • Configuration de l'environnement du système d'exploitation Oracle • Configuration du compte utilisateur du système d'exploitation Oracle • Installation du logiciel Java 2. Créez des Amazon Machine Images (AMIs) des instances et enregistrez-en des copies pour une utilisation future. Pour obtenir des instructions, consultez la section Créer une AMI Linux basée sur Amazon EBS dans le guide de EC2 l'utilisateur Amazon pour les instances Linux.	Architecte de migration, ingénieur de base de données, architecte d'applications

Tâche	Description	Compétences requises
Lancez votre infrastructure AWS en utilisant CloudFormation.	Déployez vos niveaux Web et applicatif Oracle BI 12c dans des modules à l'aide des CloudFormation modèles que vous avez créés. Pour obtenir des instructions, consultez Getting started with AWS CloudFormation dans le guide de CloudFormation l'utilisateur AWS.	Architecte d'infrastructure cloud, architecte de solutions, architecte d'applications

Migrez Oracle BI 12c vers AWS à l'aide d'une nouvelle installation

Tâche	Description	Compétences requises
Mettez en scène le logiciel requis.	Placez le logiciel requis dans un emplacement accessible aux EC2 instances Amazon. Par exemple, vous pouvez installer le logiciel dans Amazon S3 ou dans une autre EC2 instance Amazon qui serait accessible à vos serveurs Web et d'applications.	Architecte de migration, architecte Oracle BI, architecte d'infrastructure cloud, architecte de solutions, architecte d'applications
Préparez votre base de données de référentiel pour l'installation d'Oracle BI 12c.	Créez des schémas Oracle BI 12c en exécutant l'utilitaire de création de référentiel Oracle (RCU) sur une nouvelle instance de base de données Amazon RDS for Oracle.	Architecte d'infrastructure cloud, architecte de solutions, architecte d'applications, architecte de migration, architecte Oracle BI

Tâche	Description	Compétences requises
Installez Oracle Fusion Middleware 12c et Oracle BI 12c.	1. En commençant par une EC2 instance Amazon, installez l'infrastructure Oracle Fusion Middlewar e 12c et OBIEE 12c. Pour plus d'informations, consultez les sections suivantes du guide de déploiement d'Oracle Fusion Middleware Enterprise pour Oracle Business Intelligence : • Démarrage du programme d'install ation de l'infrastructure le BIHOST1 • Installation d'Oracle Business Intelligence en vue d'un déploiement en entreprise **Note** Utilisez Amazon EFS pour héberger des annuaires qui seront partagés entre les nœuds du cluster Oracle BI 12c. 2. Appliquez tous les correctifs nécessaires à l'installation.	Architecte de migration, architecte Oracle BI

Tâche	Description	Compétences requises
	3. Création AMIs des instances et sauvegarde des copies pour une utilisation future.	
Configurez le domaine WebLogic de votre serveur Oracle pour Oracle BI 12c.	Configurez votre domaine Oracle BI 12c en tant que déploiement non clusterisé. Pour plus d'informations, consultez la section Configuration du domaine BI dans le guide de déploiement d'Oracle Fusion Middleware Enterprise pour Oracle Business Intelligence.	Architecte de migration, architecte Oracle BI
Effectuez une mise à l'échelle horizontale à partir de l'Oracle BI 12c.	Diminuez horizontalement le nœud unique jusqu'au nombre de nœuds souhaité. Pour plus d'informations, consultez la section Scaling out Oracle Business Intelligence dans le guide de déploiement d'Oracle Fusion Middleware Enterprise pour Oracle Business Intelligence.	Architecte de migration, architecte Oracle BI

Tâche	Description	Compétences requises
Installez le serveur HTTP Oracle 12c.	1. Installez le serveur HTTP Oracle 12c sur les EC2 instances Amazon au niveau Web d'Oracle. Pour obtenir des instructions, voir Installer le serveur HTTP Oracle 12c dans Installer et configurer le serveur HTTP Oracle pour Oracle Access Management 12c. 2. Appliquez tous les correctifs nécessaires à l'installation. 3. Création AMIs des instances et sauvegarde des copies pour une utilisation future.	Architecte de migration, architecte Oracle BI
Configurez les équilibreurs de charge pour la terminaison SSL.	1. Créez ou importez des certificats SSL dans ACM. 2. Associez les certificats SSL à ELB.	Architecte d'infrastructure cloud, architecte de migration

Tâche	Description	Compétences requises
Migrez les artefacts de métadonnées de business intelligence vers AWS.	1. Exportez des fichiers Oracle Business Intelligence Application Archive (BAR) depuis l'installation Oracle BI 12c sur site. Pour exporter les fichiers BAR, utilisez l'outil de WebLogic script (WLST) pour exécuter la exportServiceInstancecommande. 2. Importez les fichiers BAR locaux dans l'installation AWS Oracle BI 12c. Pour importer les fichiers BAR, exécutez la commande importServiceInstanceWLST.	Architecte de migration, architecte Oracle BI

Tâche	Description	Compétences requises
Effectuez des tâches après la migration.	Après avoir importé les fichiers BAR, procédez comme suit : • Configurez toutes les sources de données JDBC supplémentaires. • Installez des pilotes pour d'autres sources de données telles que PostgreSQL ou Amazon Redshift. • Configurez Oracle LDAP, SSL, l'authentification unique (SSO) et WebLogic le magasin de sécurité. • Configurez les politiques AWS Identity and Access Management (IAM). • Activez le suivi de l'utilisation. • Configurez des intégrations à d'autres systèmes. • Migrez tous les scripts personnalisés.	Architecte de migration, architecte Oracle BI

Testez le nouvel environnement

Tâche	Description	Compétences requises
Testez le nouvel environnement Oracle BI 12c.	Effectuez end-to-end des tests sur le nouvel environnement Oracle BI 12c. Utilisez	Architecte de migration, architecte de solutions, propriétaire de l'application, administrateur Oracle BI

Tâche	Description	Compétences requises
	l'automatisation autant que possible. Voici des exemples d'activités de test : • Validation des tableaux de bord, des rapports et URLs • Tests d'acceptation par l'utilisateur (UAT) • Tests d'acceptation opérationnelle (OAT) **Note** Procéder à des tests et à des validations supplémentaires selon les besoins.	

Passez au nouvel environnement

Tâche	Description	Compétences requises
Déconnectez le trafic de l'environnement Oracle BI 12c sur site.	À la fenêtre de transition indiquée, arrêtez tout le trafic vers l'environnement Oracle BI 12c sur site.	Architecte de migration , architecte de solutions, propriétaire de l'application, administrateur Oracle BI
Resynchronisez la nouvelle base de données du référenti el Oracle BI 12c avec la base de données source.	Resynchronisez la base de données du référentiel Amazon RDS Oracle Oracle BI 12c avec la base de données locale.	Administrateur Oracle BI, ingénieur/administrateur de base de données

Tâche	Description	Compétences requises
	Pour synchroniser les bases de données, vous pouvez utiliser une actualisation d'Oracle Data Pump ou une capture de données de modification (CDC) AWS DMS.	
Basculez votre Oracle BI 12c URLs pour qu'il pointe vers le nouvel environnement AWS.	Mettez à jour l'Oracle BI 12c URLs sur vos serveurs DNS internes afin qu'ils pointent vers la nouvelle installation AWS.	Architecte de migration , architecte de solutions, propriétaire de l'application, administrateur Oracle BI
Surveillez le nouvel environnement.	Surveillez le nouvel environnement Oracle BI 12c à l'aide de l'un des outils suivants : • Amazon CloudWatch • Analyse des performances d'Amazon RDS • Oracle Enterprise Manager	Administrateur Oracle BI, ingénieur/administrateur de base de données, administrateur d'applications
Obtenez l'approbation du projet.	Passez en revue les résultats des tests avec les parties prenantes et obtenez les approbations requises pour terminer la migration.	Propriétaire de l'application, responsable du service, architecte d'infrastructure cloud, architecte de migration, architecte Oracle BI

Ressources connexes

- Utilisation de l'utilitaire de création de référentiel Oracle sur RDS pour Oracle (Amazon RDS User Guide)
- Oracle sur Amazon RDS (Guide de l'utilisateur Amazon RDS)
- Oracle WebLogic Server 12c sur AWS (livre blanc AWS)

- Déploiement d'Oracle Business Intelligence pour une haute disponibilité (Oracle Help Center)
- Fichiers d'archivage des applications Oracle Business Intelligence (BAR) (Oracle Help Center)
- Comment faire migrer OBI 12c entre les environnements (Oracle Support)

Informations supplémentaires

Vous trouverez ci-dessous une liste des meilleures pratiques relatives à la migration d'Oracle BI 12c vers le cloud AWS.

bases de données du référentiel

Il est recommandé d'héberger les schémas de base de données Oracle BI 12c sur une instance Amazon RDS for Oracle. Ce type d'instance fournit une capacité rentable et redimensionnable tout en automatisant les tâches d'administration, telles que le provisionnement du matériel, la configuration de bases de données, l'application de correctifs et les sauvegardes.

Pour plus d'informations, consultez la section Utilisation de l'utilitaire de création de référentiel Oracle sur RDS pour Oracle dans le guide de l'utilisateur Amazon RDS.

Niveaux Web et applicatifs

Les EC2 instances Amazon optimisées pour la mémoire sont souvent bien adaptées aux serveurs Oracle BI 12c. Quel que soit le type d'instance que vous choisissez, assurez-vous que les instances que vous provisionnez répondent aux exigences d'utilisation de la mémoire de votre système. Assurez-vous également de configurer une taille de segment de machine virtuelle WebLogic Java (JVM) suffisante en fonction de la mémoire disponible de votre EC2 instance Amazon.

Stockage local

Les E/S jouent un rôle important dans les performances globales de votre application Oracle BI 12c. Amazon Elastic Block Store (Amazon EBS) propose différentes classes de stockage optimisées pour différents modèles de charge de travail. Assurez-vous de choisir un type de volume Amazon EBS adapté à votre cas d'utilisation.

Pour plus d'informations sur les types de volumes EBS, consultez les fonctionnalités d'Amazon EBS dans la documentation Amazon EBS.

Stockage partagé

Un domaine Oracle BI 12c en cluster nécessite un stockage partagé pour les ressources suivantes :

- Fichiers de configuration
- Répertoire de données singleton (SDD) Oracle BI 12c
- Cache global Oracle
- Scripts du planificateur Oracle BI
- Binaires WebLogic du serveur Oracle

Vous pouvez répondre à cette exigence de stockage partagé en utilisant Amazon EFS, qui fournit un système de fichiers NFS (Elastic Network File System) évolutif et entièrement géré.

Affiner les performances du stockage partagé

Amazon EFS propose deux modes de débit : Provisioned et Bursting. Le service dispose également de deux modes de performance : General Purpose et Max I/O.

Pour optimiser les performances, commencez par tester vos charges de travail en mode performance à usage général et en mode débit provisionné. Ces tests vous aideront à déterminer si ces modes de référence sont suffisants pour atteindre les niveaux de service souhaités.

Pour plus d'informations, consultez la section relative aux performances d'Amazon EFS dans le guide de l'utilisateur Amazon EFS.

Disponibilité et reprise après sinistre

Il est recommandé de déployer des composants Oracle BI 12c dans plusieurs zones de disponibilité afin de protéger ces ressources en cas de défaillance d'une zone de disponibilité. Voici une liste des meilleures pratiques en matière de disponibilité et de reprise après sinistre pour des ressources Oracle BI 12c spécifiques hébergées dans le cloud AWS :

- Bases de données de référentiel Oracle BI 12c : déployez une instance de base de données Amazon RDS multi-AZ dans votre base de données de référentiel Oracle BI 12c. Dans un déploiement multi-AZ, Amazon RDS provisionne et gère automatiquement une réplique de secours synchrone dans une autre zone de disponibilité. L'exécution d'une instance de base de données de référentiel Oracle BI 12c dans des zones de disponibilité peut améliorer la disponibilité lors de la maintenance planifiée du système et contribuer à protéger vos bases de données contre les défaillances d'instance et de zone de disponibilité.
- Serveurs gérés Oracle BI 12c : pour garantir la tolérance aux pannes, il est recommandé de déployer les composants du système Oracle BI 12c sur les serveurs gérés d'un groupe Amazon

EC2 Auto Scaling configuré pour couvrir plusieurs zones de disponibilité. Auto Scaling remplace les instances défectueuses sur la base des bilans EC2 de santé d'Amazon. En cas de défaillance d'une zone de disponibilité, les serveurs HTTP Oracle continuent de diriger le trafic vers les serveurs gérés dans la zone de disponibilité fonctionnelle. Auto Scaling lance ensuite des instances pour répondre à vos exigences en matière de nombre d'hôtes. Il est recommandé d'activer la réplication de l'état des sessions HTTP pour garantir un basculement fluide des sessions existantes vers les serveurs gérés fonctionnels.

- Serveurs d'administration Oracle BI 12c : pour garantir la haute disponibilité de votre serveur d'administration, hébergez-le dans un groupe Amazon EC2 Auto Scaling configuré pour couvrir plusieurs zones de disponibilité. Définissez ensuite la taille minimale et maximale du groupe sur 1. En cas de défaillance d'une zone de disponibilité, Amazon EC2 Auto Scaling démarre un serveur d'administration de remplacement dans une autre zone de disponibilité. Pour récupérer tout hôte sous-jacent défaillant au sein de la même zone de disponibilité, vous pouvez activer Amazon EC2 Auto Recovery.
- Serveurs Oracle Web Tier : il est recommandé d'associer votre serveur HTTP Oracle au domaine de votre WebLogic serveur Oracle. Pour une haute disponibilité, déployez votre serveur HTTP Oracle dans un groupe Amazon EC2 Auto Scaling configuré pour englober plusieurs zones de disponibilité. Placez ensuite le serveur derrière un équilibreur de charge élastique ELB. Pour fournir une protection supplémentaire contre les pannes de l'hôte, vous pouvez activer Amazon EC2 Auto Recovery.

Evolutivité

L'élasticité du cloud AWS vous permet de faire évoluer les applications horizontalement ou verticalement en fonction des exigences de charge de travail.

Mise à l'échelle verticale

Pour dimensionner verticalement votre application, vous pouvez modifier la taille et le type des EC2 instances Amazon qui exécutent vos composants Oracle BI 12c. Il n'est pas nécessaire de surprovisionner les instances au début de votre déploiement et d'encourir des coûts inutiles.

Mise à l'échelle horizontale

Amazon EC2 Auto Scaling vous aide à dimensionner horizontalement votre application en ajoutant ou en supprimant automatiquement des serveurs gérés en fonction des exigences de charge de travail.

> **Note**
>
> La mise à l'échelle horizontale avec Amazon EC2 Auto Scaling nécessite des compétences en matière de script et des tests approfondis pour être mise en œuvre.

Backup et restauration

Voici une liste des meilleures pratiques de sauvegarde et de restauration pour des ressources Oracle BI 12c spécifiques hébergées dans le cloud AWS :

- Référentiels de métadonnées Oracle Business Intelligence : Amazon RDS crée et enregistre automatiquement des sauvegardes de vos instances de base de données. Ces sauvegardes sont conservées pendant une période que vous spécifiez. Assurez-vous de configurer la durée de sauvegarde et les paramètres de conservation de votre Amazon RDS en fonction de vos exigences en matière de protection des données. Pour plus d'informations, veuillez consulter Amazon RDS backup and restore.
- Serveurs gérés, serveurs d'administration et serveurs Web : assurez-vous de configurer les instantanés Amazon EBS en fonction de vos exigences en matière de protection et de conservation des données.
- Stockage partagé : vous pouvez gérer la sauvegarde et la restauration des fichiers stockés dans Amazon EFS à l'aide d'AWS Backup. Le service AWS Backup peut également être déployé pour gérer de manière centralisée la sauvegarde et la restauration d'autres services, notamment Amazon EC2, Amazon EBS et Amazon RDS. Pour plus d'informations, consultez Qu'est-ce qu'AWS Backup ? Dans le manuel AWS Backup Developer Guide.

Sécurité et conformité

Vous trouverez ci-dessous une liste des meilleures pratiques de sécurité et des services AWS qui peuvent vous aider à protéger vos applications Oracle BI 12c dans le cloud AWS :

- Chiffrement au repos : Amazon RDS, Amazon EFS et Amazon EBS prennent tous en charge les algorithmes de chiffrement standard du secteur. Vous pouvez utiliser AWS Key Management Service (AWS KMS) pour créer et gérer des clés cryptographiques et contrôler leur utilisation dans les services AWS et dans vos applications. Vous pouvez également configurer Oracle Transparent Data Encryption (TDE) sur l'instance de base de données Amazon RDS for Oracle qui héberge votre base de données de référentiel Oracle BI 12c.

- Chiffrement en transit : il est recommandé d'activer les protocoles SSL ou TLS pour protéger les données en transit entre les différentes couches de votre installation Oracle BI 12c. Vous pouvez utiliser AWS Certificate Manager (ACM) pour approvisionner, gérer et déployer des certificats SSL et TLS publics et privés pour vos ressources Oracle BI 12c.
- Sécurité du réseau : assurez-vous de déployer vos ressources Oracle BI 12c dans un Amazon VPC doté des contrôles d'accès appropriés configurés pour votre cas d'utilisation. Configurez vos groupes de sécurité pour filtrer le trafic entrant et sortant des EC2 instances Amazon qui exécutent votre installation. Assurez-vous également de configurer des listes de contrôle d'accès réseau (NACLs) qui autorisent ou refusent le trafic en fonction de règles définies.
- Surveillance et journalisation : vous pouvez utiliser AWS CloudTrail pour suivre les appels d'API vers votre infrastructure AWS, y compris vos ressources Oracle BI 12c. Cette fonctionnalité est utile lors du suivi des modifications apportées à l'infrastructure ou lors d'une analyse de sécurité. Vous pouvez également utiliser Amazon CloudWatch pour consulter les données opérationnelles qui peuvent vous fournir des informations exploitables sur les performances et l'état de votre application Oracle BI 12c. Vous pouvez également configurer des alarmes et effectuer des actions automatisées en fonction de ces alarmes. Amazon RDS fournit des outils de surveillance supplémentaires, notamment Enhanced Monitoring et Performance Insights.

Migrez un cluster Apache Kafka sur site vers Amazon MSK en utilisant MirrorMaker

Créée par Han Zhang (AWS) et Tanner Pratt (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'un cluster Apache Kafka sur site, autogéré ou hébergé vers Amazon Managed Streaming for Apache Kafka (Amazon MSK). Vous pouvez également utiliser ce modèle pour migrer d'un cluster Amazon MSK à un autre.

Apache Kafka inclut MirrorMaker cette fonctionnalité qui réplique les données entre deux clusters Kafka. MirrorMaker consiste en un ensemble de consommateurs faisant partie d'un groupe de consommateurs. Les consommateurs lisent les données des rubriques du cluster source, puis transmettent ces données aux producteurs, qui les écrivent dans le cluster cible.

La documentation Amazon MSK contient une présentation détaillée du processus d'utilisation de la MirrorMaker version 1.0 pour migrer des clusters Kafka sur site vers Amazon MSK. Ce modèle complète ces informations en proposant des step-by-step instructions complètes pour l'utilisation de MirrorMaker la version 2.0.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cluster source Kafka qui est l'un des suivants :
  - Dans un centre de données sur site
  - Autogéré dans le cloud
  - Hébergé par un partenaire

Limites

- Pour utiliser MirrorMaker la version 2.0, le cluster source doit utiliser Apache Kafka version 2.4.0 ou ultérieure. Pour les versions antérieures, consultez les instructions de la documentation Amazon MSK afin d'utiliser la MirrorMaker version 1.0.

Versions du produit

- MirrorMaker version 2.0
- Apache Kafka version 2.4.0 ou ultérieure. Pour plus d'informations sur les versions d'Apache Kafka prises en charge par Amazon MSK, consultez la section Versions d'Apache Kafka prises en charge.

Architecture

Pile technologique source

- Cluster Kafka sur site ou autogéré

Pile technologique cible

- Cluster Amazon MSK

Architecture cible

Le schéma montre le processus suivant :

1. MirrorMaker lit les données des sujets et des groupes de consommateurs du cluster Kafka source.
2. MirrorMaker réplique les données et les informations relatives aux consommateurs vers le cluster Amazon MSK cible.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Managed Streaming for Apache Kafka (Amazon MSK) est un service entièrement géré qui vous permet de créer et d'exécuter des applications utilisant Apache Kafka pour traiter les données de streaming.

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Autres outils

- Apache Kafka est une plateforme open source de streaming d'événements. Dans ce modèle, vous utilisez la MirrorMakerfonctionnalité de Kafka pour effectuer la migration entre clusters.

Bonnes pratiques

Vous pouvez MirrorMaker l'exécuter dans l'environnement source ou cible, mais il est recommandé de l'exécuter le plus près possible du cluster cible. Pour plus d'informations, consultez la section Meilleures pratiques : consommation à distance, production en local dans la documentation d'Apache Kafka.

Épopées

Créez le VPC et ciblez le cluster Amazon MSK

Tâche	Description	Compétences requises
Créez un VPC.	1. Créez un VPC dans le compte AWS cible. Pour obtenir des instructions, consultez la section Créer un VPC. 2. Créez trois sous-réseaux privés dans différentes zones de disponibilité du nouveau VPC. Pour obtenir des instructions, consultez la section Création d'un sous-réseau. L'utilisation de différentes zones de disponibilité garantit une	Administrateur système AWS, DevOps ingénieur, administr ateur du cloud

Tâche	Description	Compétences requises
	haute disponibilité et une tolérance aux pannes. **Note** Si vous utilisez une connexion Internet publique pour migrer le cluster Kafka, créez des sous-réseaux publics et activez l'accès public au cluster Amazon MSK.	
Créez le cluster Amazon MSK.	Créez un cluster Amazon MSK. Pour obtenir des instructions, consultez Création d'un cluster à l'aide de l'AWS Management Console ou Création d'un cluster à l'aide de l'AWS CLI. Configurez le cluster pour utiliser le VPC et les sous-réseaux que vous avez créés précédemment.	Administrateur système AWS, DevOps ingénieur, administrateur du cloud

Configurez MirrorMaker

Tâche	Description	Compétences requises
Installez MirrorMaker.	1. Lancez une EC2 instance. 2. Connectez-vous à votre EC2 instance. 3. Sur l' EC2 instance, téléchargez et extrayez la dernière version de Kafka. Pour obtenir des instructions, consultez Quick Start (documentation Kafka). **Note** Dans ce modèle, vous installez la MirrorMaker version 2.0 en tant que MirrorMaker cluster dédié sur une EC2 instance Amazon. Cette option est acceptable pour les environnements de développement et constitue l'approche utilisée dans ce modèle. Pour plus d'informations sur les autres options de déploiement pour la MirrorMaker version 2.0, consultez la section Informations	Administrateur système AWS, administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	supplémentaires de ce modèle.	
Spécifiez les informations du cluster Kafka.	Dans le `bin` dossier d'installation du client Kafka, créez un fichier mm2.properties et configurez-le pour votre cluster Kafka source. Pour obtenir des instructions, consultez Exécuter un MirrorMaker cluster dédié (documentation Kafka).	Administrateur système AWS, administrateur cloud, DevOps ingénieur
Démarrez MirrorMaker.	Entrez la commande suivante pour démarrer MirrorMaker et transmettre le fichier mm2.properties. `$ ./bin/connect-mirror-maker.sh mm2.properties`	Administrateur système AWS, administrateur cloud, DevOps ingénieur
Surveillez les progrès.	Vérifiez la progression en vérifiant le décalage entre le dernier décalage pour chaque sujet et le décalage actuel pour le sujet MirrorMaker consommé. Pour obtenir des instructions, consultez la section Surveillance de la géoréplication dans la documentation de Kafka.	Administrateur système AWS, administrateur cloud, DevOps ingénieur

Découper

Tâche	Description	Compétences requises
Arrêtez les applications destinées aux consommateurs.	Arrêtez toutes les applications grand public qui consomment les données du cluster source.	Développeur d’applications
Démarrez les applications destinées aux consommateurs.	Modifiez la configuration du bootstrap de l'application pour qu'elle pointe vers le cluster de destination. Commencez ensuite à consommer sur le cluster cible.	Développeur d’applications
Arrêtez les producteurs du cluster source.	Lorsque les applications grand public sont consommées avec succès sur le cluster cible, arrêtez les producteurs sur le cluster source.	Développeur d’applications
Démarrez les producteurs sur le cluster cible.	Modifiez la configuration des serveurs bootstrap du producteur et pointez sur le cluster cible. Attendez la fin MirrorMaker de la mise en miroir de toutes les données du cluster source avant de démarrer les producteurs.	Développeur d’applications
Arrête MirrorMaker.	Une fois que les producteurs se sont déplacés vers le cluster cible, arrêtez MirrorMaker.	Administrateur système AWS, administrateur cloud, DevOps ingénieur

Ressources connexes

Ressources AWS

- Migration de clusters à l'aide de MirrorMaker (documentation Amazon MSK)
- Laboratoires de migration Amazon MSK (studio d'atelier AWS)

Autres ressources

- MirrorMaker 2.0 (Propositions d'amélioration d'Apache Kafka)
- Géo-réplication : mise en miroir des données entre clusters (documentation Apache Kafka)

Informations supplémentaires

Ce modèle s'exécute en MirrorMaker version 2.0 en tant que MirrorMaker cluster dédié sur Amazon EC2. Cette option est acceptable pour les environnements de développement. Bien que cela ne soit pas abordé dans ce modèle, vous pouvez également exécuter la MirrorMaker version 2.0 dans un cluster Kafka Connect. Cette option de déploiement utilise un framework au sein de l'écosystème Kafka qui améliore le dimensionnement et la maintenance. Vous déployez le connecteur dans un cluster Kafka Connect avec la configuration associée pour exécuter l'application. Le connecteur peut fonctionner en mode autonome pour le développement ou les tests ou en mode distribué pour la production. Pour plus d'informations, consultez Running MirrorMaker in a Connect cluster (documentation Apache Kafka). Pour plus d'informations sur les autres options de déploiement MirrorMaker 2.0, voir Procédure pas à pas : Running MirrorMaker 2.0 (documentation Kafka).

Migrer une pile ELK vers Elastic Cloud sur AWS

Créée par Battulga Purevragchaa (AWS), Uday Reddy et Antony Prasad Thevaraj (AWS)

Récapitulatif

Elastic fournit des services depuis de nombreuses années, ses utilisateurs et clients gérant généralement Elastic eux-mêmes sur site. Elastic Cloud, le service Elasticsearch géré, permet d'utiliser la Suite Elastic (ELK Stack) et les solutions de recherche, d'observabilité et de sécurité en entreprise. Vous pouvez accéder aux solutions Elastic avec des applications telles que Logs, Metrics, APM (surveillance des performances des applications) et SIEM (informations de sécurité et gestion des événements). Vous pouvez utiliser des fonctionnalités intégrées telles que l'apprentissage automatique, la gestion du cycle de vie des index, Kibana Lens (pour les visualisations par glisser-déposer).

Lorsque vous passez d'Elasticsearch autogéré à Elastic Cloud, le service Elasticsearch prend en charge les tâches suivantes :

- Provisionnement et gestion de l'infrastructure sous-jacente
- Création et gestion de clusters Elasticsearch
- Faire évoluer les clusters vers le haut ou vers le bas
- Mises à niveau, application de correctifs et prise de clichés

Cela vous donne plus de temps pour vous concentrer sur la résolution d'autres défis.

Ce modèle définit comment migrer Elasticsearch 7.13 sur site vers Elasticsearch on Elastic Cloud on Amazon Web Services (AWS). D'autres versions peuvent nécessiter de légères modifications des processus décrits dans ce modèle. Pour plus d'informations, contactez votre représentant Elastic.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec accès à Amazon Simple Storage Service (Amazon S3) pour les instantanés
- Lien privé sécurisé avec une bande passante suffisamment élevée pour copier des fichiers de données instantanés vers Amazon S3
- Amazon S3 Transfer Acceleration

- Politiques Elastic Snapshot pour garantir que l'ingestion des données est archivée régulièrement, soit dans un magasin de données local suffisamment important, soit dans un stockage à distance (Amazon S3)

Vous devez connaître la taille de vos instantanés et les règles de cycle de vie des index associés sur site avant de lancer votre migration. Pour plus d'informations, contactez Elastic.

Rôles et compétences

Le processus de migration nécessite également les rôles et l'expertise décrits dans le tableau suivant.

Rôle	Expertise	Responsabilités
Assistance pour les applications	Connaissance d'Elastic Cloud et d'Elastic on premise	Toutes les tâches liées à Elastic
Administrateur système ou DBA	Connaissance approfondie de l'environnement Elastic sur site et de sa configuration	Possibilité de provisionner le stockage, d'installer et d'utiliser l'interface de ligne de commande AWS (AWS CLI) et d'identifier toutes les sources de données alimentant Elastic sur site
Administrateur réseau	Connaissance de la connectivité, de la sécurité et des performances du réseau sur site avec AWS	Établissement de liens réseau entre le site et Amazon S3, avec une compréhension de la bande passante de connectivité

Limites

- Elasticsearch sur Elastic Cloud n'est disponible que dans les régions AWS prises en charge (septembre 2021).

Versions du produit

- Elasticsearch 7.13

Architecture

Pile technologique source

Elasticsearch 7.13 ou version ultérieure sur site :

- Instantanés de cluster
- Instantanés de l'index
- Configuration de Beats

Architecture de la technologie source

Le schéma suivant montre une architecture locale typique avec différentes méthodes d'ingestion, différents types de nœuds et Kibana. Les différents types de nœuds reflètent le cluster Elasticsearch, ainsi que les rôles d'authentification et de visualisation.

1. Ingestion de Beats vers Logstash
2. Ingestion depuis Beats vers la file d'attente de messagerie Apache Kafka
3. Ingestion de Filebeat vers Logstash
4. Ingestion depuis la file de messagerie Apache Kafka vers Logstash
5. Ingestion de Logstash vers un cluster Elasticsearch
6. Cluster Elasticsearch
7. Nœud d'authentification et de notification
8. Kibana et nœuds blob

Pile technologique cible

Elastic Cloud est déployé sur votre compte SaaS dans plusieurs régions AWS avec réplication entre clusters.

- Instantanés de cluster
- Instantanés de l'index
- Configurations Beats

- Cloud élastique
- Network Load Balancer
- Amazon Route 53
- Amazon S3

Architecture cible

L'infrastructure Elastic Cloud gérée est la suivante :

- Haute disponibilité, présence dans plusieurs zones de disponibilité et plusieurs régions AWS.
- La région est tolérante aux défaillances car les données (index et instantanés) sont répliquées à l'aide de la réplication inter-clusters (CCR) Elastic Cloud
- Archivage, car les instantanés sont archivés dans Amazon S3
- Tolérance aux partitions réseau grâce à une combinaison d'équilibreurs de charge réseau et de Route 53
- Ingestion de données provenant (mais sans s'y limiter) d'Elastic APM, Beats, Logstash

Étapes de migration de haut niveau

Elastic a développé sa propre méthodologie prescriptive pour la migration d'Elastic Cluster sur site vers Elastic Cloud. La méthodologie Elastic est directement alignée et complémentaire sur les conseils et les meilleures pratiques d'AWS en matière de migration, notamment Well-Architected Framework et AWS Migration Acceleration Program (MAP). En général, les trois phases de migration vers AWS sont les suivantes :

- Évaluation
- Mobilisation
- Migration et modernisation

Elastic suit des phases de migration similaires avec une terminologie complémentaire :

- Initier
- Plan

- Mettre en œuvre
- Livrer
- Fermer

Elastic utilise la méthodologie de mise en œuvre Elastic pour faciliter l'obtention des résultats du projet. Cela est inclusif dès la conception afin de garantir que Elastic, les équipes de conseil et les équipes clients travaillent ensemble avec clarté pour obtenir conjointement les résultats escomptés.

La méthodologie Elastic combine le phasage en cascade traditionnel avec Scrum au cours de la phase de mise en œuvre. Les configurations des exigences techniques sont fournies de manière itérative de manière collaborative tout en minimisant les risques.

Outils

Services AWS

- Amazon Route 53 — Amazon Route 53 est un service Web de système de noms de domaine (DNS) hautement disponible et évolutif. Vous pouvez utiliser Route 53 pour effectuer trois fonctions importantes dans n'importe quelle combinaison : l'enregistrement de domaine, le routage DNS et la surveillance de l'état.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web. Ce modèle utilise un compartiment S3 et Amazon S3 Transfer Acceleration.
- Elastic Load Balancing — Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles, telles que les EC2 instances, les conteneurs et les adresses IP, dans une ou plusieurs zones de disponibilité.

Autres outils

- Beats — Beats expédie des données depuis Logstash ou Elasticsearch
- Elastic Cloud — Elastic Cloud est un service géré pour l'hébergement d'Elasticsearch.
- Elasticsearch — Elasticsearch est un moteur de recherche et d'analyse qui utilise la Suite Elastic pour stocker de manière centralisée vos données à des fins de recherche et d'analyse évolutives. Ce modèle utilise également la création de snapshots et la réplication entre clusters.

- Logstash — Logstash est un pipeline de traitement de données côté serveur qui ingère des données provenant de plusieurs sources, les transforme, puis les envoie vers votre espace de stockage de données.

Épopées

Préparer la migration

Tâche	Description	Compétences requises
Identifiez les serveurs exécutant la solution Elastic sur site.	Vérifiez que la migration élastique est prise en charge.	Propriétaire de l'application
Comprenez la configuration du serveur sur site.	Pour comprendre la configuration du serveur nécessaire pour gérer correctement les charges de travail sur site, déterminez l'encombrement matériel du serveur, la configuration réseau et les caractéristiques de stockage actuellement utilisées	Support pour les applications
Collectez les informations relatives aux comptes des utilisateurs et des applications.	Identifiez les noms d'utilisateur et les noms d'applications utilisés par l'environnement Elastic sur site.	Administrateur système, support des applications
Documentez la configuration de Beats et de l'expéditeur de données.	Pour documenter les configurations, examinez les sources de données et les récepteurs existants. Pour plus d'informations, consultez la documentation Elastic.	Assistance pour les applications

Tâche	Description	Compétences requises
Déterminez la vélocité et le volume des données.	Établissez une base de référence pour la quantité de données traitée par le cluster.	Administrateur système, support des applications
Documentez les scénarios RPO et RTO.	Documentez les scénarios d'objectif de point de reprise (RPO) et d'objectif de temps de reprise (RTO) en termes de pannes et d'accords de niveau de service ()SLAs.	Propriétaire de l'application, administrateur système, assistance de l'application
Déterminez les paramètres de cycle de vie des instantanés optimaux.	Définissez la fréquence à laquelle les données doivent être sécurisées en utilisant des instantanés Elastic pendant et après la migration.	Propriétaire de l'application, administrateur système, assistance de l'application
Définissez les attentes en matière de performances après la migration.	Générez des métriques sur l'actualisation actuelle et attendue de l'écran, les temps d'exécution des requêtes et les comportements de l'interfa ce utilisateur.	Administrateur système, support des applications
Documentez les exigences en matière de transport, de bande passante et de disponibilité de l'accès à Internet.	Vérifiez la vitesse, la latence et la résilience des connexion s Internet pour copier des instantanés vers Amazon S3.	Administrateur réseau
Documentez les coûts actuels de l'exécution sur site pour Elastic.	Assurez-vous que le dimensionnement de l'environ nement cible AWS est conçu pour être à la fois performant et rentable.	DBA, administrateur système, support des applications

Tâche	Description	Compétences requises
Identifiez les besoins en matière d'authentification et d'autorisation.	Les fonctionnalités de sécurité d'Elastic Stack fournissent des domaines intégrés tels que le protocole LDAP (Lightweight Directory Access Protocol), le langage SAML (Security Assertion Markup Language) et OpenID Connect (OIDC).	DBA, administrateur système, support des applications
Comprenez les exigences réglementaires spécifiques en fonction de la situation géographique.	Assurez-vous que les données sont exportées et cryptées conformément à vos exigences et à toutes les exigences nationales pertinentes.	DBA, administrateur système, support des applications

Mettre en œuvre la migration

Tâche	Description	Compétences requises
Préparez la zone de transit sur Amazon S3.	Pour recevoir des instantanés sur Amazon S3, créez un compartiment S3 et un rôle AWS Identity and Access Management (IAM) temporaire avec un accès complet à votre compartiment nouvellement créé. Pour plus d'informations, consultez la section Création d'un rôle pour déléguer des autorisations à un utilisateur IAM. Utilisez le service AWS Security Token Service pour demander des informations	Administrateur AWS

Tâche	Description	Compétences requises
	d'identification de sécurité temporaires. Protégez l'identifiant de la clé d'accès, la clé d'accès secrète et le jeton de session. Activez Amazon S3 Transfer Acceleration sur le compartiment.	
Installez l'AWS CLI et le plug-in Amazon S3 sur site.	Sur chaque nœud Elasticsearch, exécutez la commande suivante. `sudo bin/elasticsearch-plugin install repository-s3` Redémarrez ensuite le nœud.	Administrateur AWS

Configurez l'accès au client Amazon S3.	Ajoutez les clés créées précédemment en exécutant les commandes suivantes.
	
	`elasticsearch-keystore add s3.client.default.access_key`
	
	`elasticsearch-keystore add s3.client.default.secret_key`
	
	`elasticsearch-keystore add s3.client.default.session_token`
		Administrateur AWS

Tâche	Description	Compétences requises
Enregistrer un référentiel de snapshots pour Elastic Data	Utilisez les outils de développement Kibana pour indiquer au cluster local sur site dans quel compartiment S3 distant il doit écrire.	Administrateur AWS
Configurez la politique de capture instantanée.	Pour configurer la gestion du cycle de vie des snapshots, dans l'onglet Politiques de Kibana, choisissez la politique SLM et définissez les heures, les flux de données ou les index à inclure, ainsi que les noms à utiliser. Configurez une politique qui prend fréquemment des instantanés. Les instantanés sont incrémentiels et permettent une utilisation efficace du stockage. Faites correspondre votre décision d'évaluation de l'état de préparation. Une politique peut également spécifier une politique de rétention et supprimer automatiquement les instantanés lorsqu'ils ne sont plus nécessaires.	Assistance pour les applications

Tâche	Description	Compétences requises
Vérifiez que les instantanés fonctionnent.	Dans Kibana Dev Tools, exécutez la commande suivante. `GET _snapshot/<your_repo_name>/_all`	administrateur AWS, support des applications,
Déployez un nouveau cluster sur Elastic Cloud.	Connectez-vous à Elastic et choisissez un cluster pour « l'observabilité, la recherche ou la sécurité » en fonction des résultats de l'évaluation du niveau de préparation de votre entreprise.	Administrateur AWS, support des applications
Configurez l'accès au magasin de clés du cluster.	Le nouveau cluster doit accéder au compartiment S3 qui stockera les instantanés. Sur la console Elasticsearch Service, choisissez Security, puis entrez les clés d'accès et secrètes IAM que vous avez créées précédemment.	Administrateur AWS

Tâche	Description	Compétences requises
Configurez le cluster hébergé par Elastic Cloud pour accéder à Amazon S3.	Configurez un nouvel accès de cluster au référentiel de snapshots créé précédemment dans Amazon S3. À l'aide de Kibana, procédez comme suit : 1. Choisissez Stack Management, Snapshot Settings, RegisterRepo. 2. Dans le champ Alias, entrez le nom du référentiel. 3. Pour le nom du client S3, choisissez secondaire. 4. Ajoutez le compartiment S3 que vous avez créé précédemment au référentiel. 5. Choisissez Compresser l'instantané. 6. Pour les paramètres de chiffrement, conservez les valeurs par défaut.	Administrateur AWS, Support des applications
Vérifiez le nouveau référentiel Amazon S3.	Assurez-vous que vous pouvez accéder à votre nouveau référentiel hébergé dans le cluster Elastic Cloud.	Administrateur AWS

Tâche	Description	Compétences requises

Initialisez le cluster de services Elasticsearch.	Sur l'Elasticsearch Service Console, initialisez le cluster de services Elasticsearch à partir du snapshot S3.
	
	Exécutez les commandes suivantes en tant que POST.
	
	`*/_close?expand_wildcards=all`
	
	`/_snapshot/<your-repo-name>/  <your-snapshot-name>/_restore`
	
	`*/_open?expand_wildcards=all`
		Support pour les applications

Terminez la migration

Tâche	Description	Compétences requises
Vérifiez que la restauration du snapshot a réussi.	À l'aide de Kibana Dev Tools, exécutez la commande suivante. `GET _cat/indices`	Assistance pour les applications
Redéployez les services d'ingestion.	Connectez les points de terminaison de Beats et Logstash au nouveau point de terminaison du service Elasticsearch.	Assistance pour les applications

Testez l'environnement du cluster et nettoyez

Tâche	Description	Compétences requises
Validez l'environnement du cluster.	Une fois l'environnement de cluster Elastic sur site migré vers AWS, vous pouvez vous y connecter et utiliser vos propres outils de test d'acceptation utilisateur (UAT) pour valider le nouvel environnement.	Assistance pour les applications
Nettoyez les ressources.	Après avoir vérifié que le cluster a bien migré, supprimez le compartiment S3 et le rôle IAM utilisés pour la migration.	Administrateur AWS

Ressources connexes

Références élastiques

- Cloud élastique
- Elasticsearch et Kibana gérés sur AWS
- Recherche d'entreprise élastique
- Intégrations élastiques
- Observabilité élastique
- Sécurité élastique
- Battements
- APM élastique
- Migrer vers la gestion du cycle de vie des index
- Abonnements élastiques
- Contactez Elastic

Articles de blog Elastic

- Comment migrer d'Elasticsearch autogéré vers Elastic Cloud sur AWS (article de blog)
- Migration vers Elastic Cloud (article de blog)

Documentation élastique

- Tutoriel : Automatisez les sauvegardes avec SLM
- ILM : gestion du cycle de vie des index
- Logstash
- Réplication entre clusters (CCR)
- Pipelines d'ingestion
- Exécuter des requêtes d'API Elasticsearch
- Conservation des instantanés

Vidéo et webinaire Elastic

- Migration élastique vers le cloud
- Elastic Cloud : pourquoi les clients migrent-ils (webinaire)

Références AWS

- Elastic Cloud sur AWS Marketplace
- interface ligne de commande AWS
- AWS Direct Connect
- Programme d’accélération des migrations AWS
- Network Load Balancers
- Régions et zones de disponibilité
- Amazon Route 53
- Amazon Simple Storage Service
- Amazon S3 Transfer Acceleration
- Connexions VPN
- Framework Well-Architected

Informations supplémentaires

Si vous envisagez de migrer des charges de travail complexes, faites appel à Elastic Consulting Services. Si vous avez des questions de base concernant les configurations et les services, contactez l'équipe du Support Elastic.

Migrez les données vers le à AWS Cloud l'aide de Starburst

Créée par Antony Prasad Thevaraj (AWS), Shaun Van Staden et Suresh Veeragoni (AWS)

Récapitulatif

Starburst vous aide à accélérer votre migration de données vers Amazon Web Services (AWS) en fournissant un moteur de requête d'entreprise qui réunit les sources de données existantes dans un point d'accès unique. Vous pouvez effectuer des analyses sur plusieurs sources de données pour obtenir des informations précieuses, avant de finaliser tout plan de migration. Sans perturber les business-as-usual analyses, vous pouvez migrer les données à l'aide du moteur Starburst ou d'une application d'extraction, de transformation et de chargement (ETL) dédiée.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un cloud privé virtuel (VPC)
- Un cluster Amazon Elastic Kubernetes Service (Amazon EKS)
- Un groupe Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling
- Liste des charges de travail actuelles du système qui doivent être migrées
- Connectivité réseau depuis AWS votre environnement sur site

Architecture

Architecture de référence

Le schéma d'architecture de haut niveau suivant montre le déploiement typique de Starburst Enterprise dans AWS Cloud :

1. Le cluster Starburst Enterprise s'exécute dans votre Compte AWS.
2. Un utilisateur s'authentifie à l'aide du protocole LDAP (Lightweight Directory Access Protocol) ou d'Open Authorization (OAuth) et interagit directement avec le cluster Starburst.
3. Starburst peut se connecter à plusieurs sources de AWS données AWS Glue, telles qu'Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service (Amazon RDS) et

Amazon Redshift. Starburst fournit des fonctionnalités de requêtes fédérées entre les sources de données dans AWS Cloud, sur site ou dans d'autres environnements cloud.

4. Vous lancez Starburst Enterprise dans un cluster Amazon EKS à l'aide de diagrammes Helm.
5. Starburst Enterprise utilise les groupes Amazon EC2 Auto Scaling et les instances Amazon EC2 Spot pour optimiser son infrastructure.
6. Starburst Enterprise se connecte directement à vos sources de données sur site existantes pour lire les données en temps réel. En outre, si vous avez déjà déployé Starburst Enterprise dans cet environnement, vous pouvez connecter directement votre nouveau cluster Starburst AWS Cloud à ce cluster existant.

Veuillez noter ce qui suit :

- Starburst n'est pas une plateforme de virtualisation de données. Il s'agit d'un moteur de requêtes MPP (Massively Parallel Processing) basé sur SQL qui constitue la base d'une stratégie globale de maillage des données pour l'analyse.
- Lorsque Starburst est déployé dans le cadre d'une migration, il dispose d'une connectivité directe à l'infrastructure sur site existante.
- Starburst fournit plusieurs connecteurs d'entreprise et open source intégrés qui facilitent la connectivité à une variété de systèmes existants. Pour une liste complète des connecteurs et de leurs fonctionnalités, voir Connecteurs dans le guide de l'utilisateur de Starburst Enterprise.
- Starburst peut interroger des données en temps réel à partir de sources de données locales. Cela permet d'éviter les interruptions des opérations commerciales régulières pendant la migration des données.
- Si vous migrez depuis un déploiement Starburst Enterprise sur site existant, vous pouvez utiliser un connecteur spécial, Starburst Stargate, pour connecter votre cluster Starburst Enterprise directement à votre cluster sur site. AWS Cela offre des avantages supplémentaires en termes de performances lorsque les utilisateurs professionnels et les analystes de données fédérent les AWS Cloud requêtes depuis votre environnement sur site.

Présentation générale du processus

Vous pouvez accélérer les projets de migration de données en utilisant Starburst, car Starburst permet d'obtenir des informations sur toutes vos données avant de les migrer. L'image suivante montre le processus typique de migration de données à l'aide de Starburst.

Rôles

Les rôles suivants sont généralement requis pour effectuer une migration à l'aide de Starburst :

- Administrateur du cloud : responsable de la mise à disposition des ressources du cloud pour exécuter l'application Starburst Enterprise
- Administrateur Starburst : responsable de l'installation, de la configuration, de la gestion et du support de l'application Starburst
- Ingénieur de données — Responsable de :
  - Migration des données existantes vers le cloud
  - Création de vues sémantiques à l'appui de l'analyse
- Propriétaire de la solution ou du système : responsable de la mise en œuvre globale de la solution

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.

Autres outils

- Helm — Helm est un gestionnaire de packages pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes.
- Starburst Enterprise — Starburst Enterprise est un moteur de requêtes MPP (Massively Parallel Processing) basé sur SQL qui constitue la base d'une stratégie globale de maillage des données pour l'analyse.
- Starburst Stargate — Starburst Stargate relie les catalogues et les sources de données d'un environnement Starburst Enterprise, tel qu'un cluster dans un centre de données sur site, aux catalogues et sources de données d'un autre environnement Starburst Enterprise, tel qu'un cluster dans le. AWS Cloud

Épopées

Évaluez les données

Tâche	Description	Compétences requises
Identifiez et hiérarchisez vos données.	Identifiez les données que vous souhaitez déplacer. Les grands systèmes existants sur site peuvent inclure des données de base que vous souhaitez migrer ainsi que des données que vous ne souhaitez pas déplacer ou ne peuvent pas être déplacées pour des raisons de conformité. Commencer par un inventaire des données vous permet de hiérarchi ser les données à cibler en premier. Pour plus d'informa tions, voir Commencer la découverte automatique de portefeuilles.	Ingénieur de données, DBA
Explorez, inventoriez et sauvegardez vos données.	Validez la qualité, la quantité et la pertinence des données pour votre cas d'utilisation. Sauvegardez ou créez un instantané des données selon vos besoins, puis finalisez l'environnement cible pour les données.	Ingénieur de données, DBA

Configuration de l'environnement Starburst Enterprise

Tâche	Description	Compétences requises
Configurez Starburst Enterprise dans le. AWS Cloud	Pendant le catalogage des données, configurez Starburst Enterprise dans un cluster Amazon EKS géré. Pour plus d'informations, voir Déploiement avec Kubernetes dans la documentation de référence de Starburst Enterprise. Cela permet d' business-as-usuale ffectuer des analyses pendant le processus de migration des données.	Administrateur AWS, développeur d'applications
Connect Starburst aux sources de données.	Après avoir identifié les données et configuré Starburst Enterprise, connectez Starburst aux sources de données. Starburst lit les données directement à partir de la source de données sous forme de requête SQL. Pour plus d'informations, consultez la documentation de référence de Starburst Enterprise.	Administrateur AWS, développeur d'applications

Migrer les données

Tâche	Description	Compétences requises
Créez et exécutez les pipelines ETL.	Commencez le processus de migration des données. Cette activité peut avoir lieu	Ingénieur de données

Tâche	Description	Compétences requises
	en même temps que les business-as-usual analyses. Pour la migration, vous pouvez utiliser un produit tiers ou Starburst. Starburst a la capacité de lire et d'écrire des données provenant de différentes sources. Pour plus d'informations, consultez la documentation de référence de Starburst Enterprise.	
Validez les données.	Une fois les données migrées, validez-les pour vous assurer que toutes les données requises ont été déplacées et sont intactes.	Ingénieur de données, DevOps ingénieur

Découper

Tâche	Description	Compétences requises
Réduisez les données.	Une fois la migration et la validation des données terminées, vous pouvez supprimer les données. Cela implique de modifier les liens de connexion de données dans Starburst . Au lieu de pointer vers les sources locales, vous pointez vers les nouvelles sources cloud et vous mettez à jour les vues sémantiqu es. Pour plus d'informations,	Ingénieur de données, responsable du transfert

Tâche	Description	Compétences requises
	consultez Connecteurs dans la documentation de référence de Starburst Enterprise.	
Déployez le produit auprès des utilisateurs.	Les consommateurs de données commencent à travailler à partir des sources de données migrées. Ce processus est invisible pour les utilisateurs finaux des outils d'analyse.	Responsable du transfert, ingénieur des données

Ressources connexes

AWS Marketplace

- Galaxie Starburst
- Starburst Entreprise
- Données Starburst JumpStart
- Starburst Enterprise avec Graviton

Documentation sur Starburst

- Guide de l'utilisateur de Starburst Enterprise
- Documentation de référence de Starburst Enterprise

Autres AWS documentations

- Commencez par la découverte automatisée des portefeuilles (directives AWS prescriptives)
- Optimisation des coûts et des performances de l'infrastructure cloud avec Starburst on AWS (article de AWS blog)

Optimisation de l'ingestion ETL de la taille du fichier d'entrée sur AWS

Créée par Apoorva Patrikar (AWS)

Récapitulatif

Ce modèle vous montre comment optimiser l'étape d'ingestion du processus d'extraction, de transformation et de chargement (ETL) pour le Big Data et les charges de travail Apache Spark sur AWS Glue en optimisant la taille des fichiers avant de traiter vos données. Utilisez ce modèle pour prévenir ou résoudre le problème des petits fichiers. C'est-à-dire lorsqu'un grand nombre de petits fichiers ralentit le traitement des données en raison de la taille globale des fichiers. Par exemple, des centaines de fichiers de quelques centaines de kilo-octets chacun peuvent considérablement ralentir la vitesse de traitement des données pour vos tâches AWS Glue. Cela est dû au fait qu'AWS Glue doit exécuter des fonctions de liste internes sur Amazon Simple Storage Service (Amazon S3) et YARN (Yet Another Resource Negotiator) doit stocker une grande quantité de métadonnées. Pour améliorer les vitesses de traitement des données, vous pouvez utiliser le regroupement pour permettre à vos tâches ETL de lire un groupe de fichiers d'entrée sur une seule partition en mémoire. La partition regroupe automatiquement les petits fichiers. Vous pouvez également utiliser un code personnalisé pour ajouter une logique de traitement par lots à vos fichiers existants.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une ou plusieurs tâches AWS Glue
- Une ou plusieurs charges de travail Big Data ou Apache Spark
- Compartiment S3

Architecture

Le modèle suivant montre comment les données de différents formats sont traitées par une tâche AWS Glue, puis stockées dans un compartiment S3 pour obtenir une visibilité sur les performances.

Le schéma suivant illustre le flux de travail suivant :

1.
> **Note**
>
> Une tâche AWS Glue convertit de petits fichiers au format CSV, JSON et Parquet en cadres dynamiques. : La taille du fichier d'entrée a l'impact le plus significatif sur les performances de la tâche AWS Glue.

2. La tâche AWS Glue exécute des fonctions de liste internes dans un compartiment S3.

Outils

- AWS Glue est un service ETL entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Épopées

Utilisez le regroupement pour optimiser l'ingestion d'ETL pendant la lecture

Tâche	Description	Compétences requises
Spécifiez la taille du groupe.	Si vous avez plus de 50 000 fichiers, le regroupement est effectué par défaut. Toutefois, vous pouvez également utiliser le regroupement pour moins de 50 000 fichiers en spécifiant la taille du groupe dans le `connectionOptions` paramètre. Le `connectionOptions` paramètre se trouve dans la `create_dynamic_frame.from_options` méthode.	Ingénieur de données

Tâche	Description	Compétences requises
Écrivez le code de regroupement.	Utilisez `create_dynamic_frame` cette méthode pour créer un cadre dynamique. Par exemple : `S3bucket_node1 = glueContext.create_dynamic_frame.from_options(format_options={"multiline": False}, connection_type="s3", format="json", connection_options={ "paths": ["s3://bucket/prefix/file.json"], "recurse": True, "groupFiles": 'inPartition', "groupSize": 1048576 }, transformation_ctx="S3bucket_node1",)`  **Note** `groupFiles` À utiliser pour regrouper des fichiers dans un groupe de partitions Amazon S3. Permet `groupSize` de	Ingénieur de données

Tâche	Description	Compétences requises
	définir la taille cible du groupe à lire en mémoire. Spécifiez `groupSize` en octets (1048576 = 1 Mo).	
Ajoutez le code au flux de travail.	Ajoutez le code de regroupement à votre flux de travail dans AWS Glue.	Ingénieur de données

Utilisez une logique personnalisée pour optimiser l'ingestion d'ETL

Tâche	Description	Compétences requises
Choisissez la langue et la plateforme de traitement.	Choisissez le langage de script et la plate-forme de traitement adaptés à votre cas d'utilisation.	Architecte du cloud
Écrivez le code.	Écrivez la logique personnalisée pour regrouper vos fichiers.	Architecte du cloud
Ajoutez le code au flux de travail.	Ajoutez le code à votre flux de travail dans AWS Glue. Cela permet d'appliquer votre logique personnalisée à chaque exécution de la tâche.	Ingénieur de données

Répartition lors de l'écriture de données après transformation

Tâche	Description	Compétences requises
Analysez les habitudes de consommation.	Découvrez comment les applications en aval utiliseront les données que vous écrivez. Par exemple, s'ils interroge nt des données chaque jour et que vous partitionnez uniquement les données par région ou que vous avez de très petits fichiers de sortie, tels que 2,5 Ko par fichier, cela n'est pas optimal en termes de consommation.	DBA
Répartissez les données avant de les écrire.	Répartition basée sur les jointures ou les requêtes pendant le traitement (selon la logique de traitement) et après le traitement (en fonction de la consommation). Par exemple, une répartition basée sur la taille des octets, telle que `.repartition(100000)` , ou une répartition basée sur des colonnes, telle que. `.repartition("column_name")`	Ingénieur de données

Ressources connexes

- Lecture de fichiers d'entrée dans des groupes plus importants
- Surveillance d'AWS Glue
- Surveillance d'AWS Glue à l'aide CloudWatch des métriques Amazon

- Surveillance et débogage des tâches
- Commencer à utiliser l'ETL sans serveur sur AWS Glue

Informations supplémentaires

Détermination de la taille du fichier

Il n'existe aucun moyen simple de déterminer si la taille d'un fichier est trop grande ou trop petite. L'impact de la taille du fichier sur les performances de traitement dépend de la configuration de votre cluster. Dans le noyau de Hadoop, nous vous recommandons d'utiliser des fichiers de 128 Mo ou 256 Mo pour tirer le meilleur parti de la taille des blocs.

Pour la plupart des charges de travail de fichiers texte sur AWS Glue, nous recommandons une taille de fichier comprise entre 100 Mo et 1 Go pour un cluster de 5 à 10 DPU. Pour déterminer la taille optimale des fichiers d'entrée, surveillez la section de prétraitement de votre tâche AWS Glue, puis vérifiez l'utilisation du processeur et de la mémoire de la tâche.

Considérations supplémentaires

Si les performances au cours des premières étapes de l'ETL constituent un obstacle, envisagez de regrouper ou de fusionner les fichiers de données avant le traitement. Si vous contrôlez totalement le processus de génération de fichiers, il peut être encore plus efficace d'agréger les points de données sur le système source lui-même avant que les données brutes ne soient envoyées à AWS.

Orchestrez un pipeline ETL avec validation, transformation et partitionnement à l'aide d'AWS Step Functions

Créée par Sandip Gangapadhyay (AWS)

Récapitulatif

Ce modèle décrit comment créer un pipeline d'extraction, de transformation et de chargement (ETL) sans serveur pour valider, transformer, compresser et partitionner un ensemble de données CSV volumineux afin d'optimiser les performances et les coûts. Le pipeline est orchestré par AWS Step Functions et inclut des fonctionnalités de gestion des erreurs, de relance automatique et de notification aux utilisateurs.

Lorsqu'un fichier CSV est chargé dans un dossier source du bucket Amazon Simple Storage Service (Amazon S3), le pipeline ETL commence à s'exécuter. Le pipeline valide le contenu et le schéma du fichier CSV source, transforme le fichier CSV au format Apache Parquet compressé, partitionne le jeu de données par année, mois et jour, et le stocke dans un dossier distinct pour que les outils d'analyse puissent le traiter.

Le code qui automatise ce modèle est disponible sur GitHub, dans le référentiel ETL Pipeline with AWS Step Functions.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- L'interface de ligne de commande AWS (AWS CLI) est installée et configurée avec votre compte AWS, afin que vous puissiez créer des ressources AWS en déployant une pile CloudFormation AWS. La version 2 de l'interface de ligne de commande AWS est recommandée. Pour les instructions d'installation, consultez la section Installation, mise à jour et désinstallation de la version 2 de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS. Pour les instructions de configuration de l'AWS CLI, consultez la section Configuration et paramètres des fichiers d'identification dans la documentation de l'AWS CLI.
- Un compartiment Amazon S3.
- Un jeu de données CSV avec le schéma correct. (Le référentiel de code inclus dans ce modèle fournit un exemple de fichier CSV contenant le schéma et le type de données appropriés que vous pouvez utiliser.)

- Un navigateur Web compatible avec l'AWS Management Console. (Consultez la liste des navigateurs pris en charge.)
- Accès à la console AWS Glue.
- Accès à la console AWS Step Functions.

Limites

- Dans AWS Step Functions, la durée maximale de conservation des journaux d'historique est de 90 jours. Pour plus d'informations, consultez la section Quotas et quotas pour les flux de travail standard dans la documentation AWS Step Functions.

Versions du produit

- Python 3.11 pour AWS Lambda
- AWS Glue version 2.0

Architecture

Le flux de travail illustré dans le diagramme comprend les étapes de haut niveau suivantes :

1. L'utilisateur télécharge un fichier CSV dans le dossier source d'Amazon S3.
2. Un événement de notification Amazon S3 lance une fonction AWS Lambda qui démarre la machine d'état Step Functions.
3. La fonction Lambda valide le schéma et le type de données du fichier CSV brut.
4. En fonction des résultats de validation :
   a. Si la validation du fichier source aboutit, le fichier est transféré dans le dossier de stage pour un traitement ultérieur.
   b. Si la validation échoue, le fichier est transféré dans le dossier des erreurs et une notification d'erreur est envoyée via Amazon Simple Notification Service (Amazon SNS).
5. Un robot d'exploration AWS Glue crée le schéma du fichier brut à partir du dossier stage dans Amazon S3.
6. Une tâche AWS Glue transforme, compresse et partitionne le fichier brut au format Parquet.
7. La tâche AWS Glue déplace également le fichier vers le dossier de transformation d'Amazon S3.

8. Le robot d'exploration AWS Glue crée le schéma à partir du fichier transformé. Le schéma obtenu peut être utilisé par n'importe quelle tâche d'analyse. Vous pouvez également utiliser Amazon Athena pour exécuter des requêtes ad hoc.
9. Si le pipeline se termine sans erreur, le fichier de schéma est déplacé vers le dossier d'archive. En cas d'erreur, le fichier est plutôt déplacé vers le dossier des erreurs.
10. Amazon SNS envoie une notification indiquant le succès ou l'échec en fonction de l'état d'achèvement du pipeline.

Toutes les ressources AWS utilisées dans ce modèle sont sans serveur. Il n'y a aucun serveur à gérer.

Outils

Services AWS

- AWS Glue — AWS Glue est un service ETL entièrement géré qui permet aux clients de préparer et de charger facilement leurs données à des fins d'analyse.
- AWS Step Functions — AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise. La console graphique AWS Step Functions vous permet de voir le flux de travail de votre application comme une série d'étapes pilotées par des événements.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service de messagerie Pub/Sub hautement disponible, durable, sécurisé et entièrement géré qui vous permet de dissocier les microservices, les systèmes distribués et les applications sans serveur.
- AWS Lambda — AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. AWS Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.

Code

Le code de ce modèle est disponible sur GitHub, dans le référentiel ETL Pipeline with AWS Step Functions. Le référentiel de code contient les fichiers et dossiers suivants :

- `template.yml`— CloudFormation Modèle AWS pour créer le pipeline ETL avec AWS Step Functions.
- `parameter.json`— Contient tous les paramètres et valeurs de paramètres. Vous mettez à jour ce fichier pour modifier les valeurs des paramètres, comme décrit dans la section Epics.
- `myLayer/python`dossier — Contient les packages Python nécessaires pour créer la couche AWS Lambda requise pour ce projet.
- `lambda`dossier — Contient les fonctions Lambda suivantes :
  - `move_file.py`— Déplace le jeu de données source vers le dossier d'archive, de transformation ou d'erreur.
  - `check_crawler.py`— Vérifie l'état du robot d'exploration AWS Glue autant de fois que configuré par la variable d'`RETRYLIMIT` environnement avant qu'il n'envoie un message d'échec.
  - `start_crawler.py`— Démarre le robot d'exploration AWS Glue.
  - `start_step_function.py`— Démarre AWS Step Functions.
  - `start_codebuild.py`— Démarre le CodeBuild projet AWS.
  - `validation.py`— Valide le jeu de données brut en entrée.
  - `s3object.py`— Crée la structure de répertoire requise dans le compartiment S3.
  - `notification.py`— Envoie des notifications de réussite ou d'erreur à la fin du pipeline.

Pour utiliser l'exemple de code, suivez les instructions de la section Epics.

Épopées

Préparez les fichiers sources

Tâche	Description	Compétences requises
Clonez le référentiel d'exemples de code.	1. Ouvrez le pipeline ETL avec le référentiel AWS Step Functions. 2. Choisissez Code sur la page principale du référentiel, au-dessus de la liste des fichiers, et copiez l'URL	Developer

Tâche	Description	Compétences requises
	répertoriée sous Cloner avec HTTPS. 3. Remplacez votre répertoire de travail par l'emplacement où vous souhaitez stocker les fichiers d'exemple. 4. Sur un terminal ou une invite de commande, tapez la commande suivante : `git clone <repoURL>` où `<repoURL>` fait référence à l'URL que vous avez copiée à l'étape 2.	

Tâche	Description	Compétences requises
Mettez à jour les valeurs des paramètres.	Dans votre copie locale du référentiel, modifiez le `parameter.json` fichier et mettez à jour les valeurs des paramètres par défaut comme suit : • `pS3BucketName` — Le nom du compartiment S3 pour stocker les ensembles de données. Le modèle créera ce compartiment pour vous. Le nom du compartiment doit être globalement unique. • `pSourceFolder` — Le nom du dossier dans le compartiment S3 qui sera utilisé pour télécharger le fichier CSV source. • `pStageFolder` — Le nom du dossier dans le compartiment S3 qui sera utilisé comme zone intermédiaire pendant le processus. • `pTransformFolder` — Le nom du dossier dans le compartiment S3 qui sera utilisé pour stocker les ensembles de données transformés et partitionnés. • `pErrorFolder` — Le dossier du compartiment S3	Developer

Tâche	Description	Compétences requises
	dans lequel le fichier CSV source sera déplacé s'il ne peut pas être validé. • `pArchiveFolder` — Le nom du dossier dans le compartiment S3 qui sera utilisé pour archiver le fichier CSV source. • `pEmailforNotification` — Une adresse e-mail valide pour recevoir les notifications de succès/d' erreur. • `pPrefix`— Chaîne de préfixe qui sera utilisée dans le nom du crawler AWS Glue. • `pDatasetSchema` — Le schéma de jeu de données par rapport auquel le fichier source sera validé. Le package Python Cerberus est utilisé pour la validation du jeu de données source. Pour plus d'informations, consultez le site Web de Cerberus.	

Tâche	Description	Compétences requises
Téléchargez le code source dans le compartiment S3.	Avant de déployer le CloudFormation modèle qui automatise le pipeline ETL, vous devez empaqueter les fichiers source du CloudFormation modèle et les télécharger dans un compartiment S3. Pour ce faire, exécutez la commande AWS CLI suivante avec votre profil préconfiguré : `aws cloudformation package --template-file template.yml --s3-bucket <bucket_name> --output-template-file packaged.template --profile <profile_name>` où : • `<bucket_name>` est le nom d'un compartiment S3 existant dans la région AWS où vous souhaitez déployer la pile. Ce compartiment est utilisé pour stocker le package de code source du CloudFormation modèle. • `<profile_name>` est un profil d'interface de ligne de commande AWS valide que vous avez préconfiguré lors de la configuration	Developer

Tâche	Description	Compétences requises
	de l'interface de ligne de commande AWS.	

Créez la pile .

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Pour déployer le CloudFormation modèle, exécutez la commande AWS CLI suivante : `aws cloudformation deploy --stack-name <stack_name> --template-file packaged.template --parameter-overrides file://parameter.json --capabilities CAPABILITY_IAM --profile <profile_name>` où : • `<stack_name>` est un identifiant unique pour la CloudFormation pile. • `<profile-name>` est votre profil d'interface de ligne de commande AWS préconfiguré.	Developer
Vérifiez les progrès.	Sur la CloudFormation console AWS, vérifiez la progression du développe	Developer

Tâche	Description	Compétences requises
	ment de la pile. Lorsque le statut est définiCREATE_COMPLETE , la pile a été déployée avec succès.	
Notez le nom de la base de données AWS Glue.	L'onglet Outputs de la pile affiche le nom de la base de données AWS Glue. Le nom de la clé estGlueDBOutput .	Developer

Testez le pipeline

Tâche	Description	Compétences requises
Démarrez le pipeline ETL.	1. Accédez au dossier source (sourceou au nom du dossier que vous avez défini dans le parameter.json fichier) dans le compartiment S3. 2. Téléchargez un exemple de fichier CSV dans ce dossier. (Le référentiel de code fournit un exemple de fichier appelé Sample_Bank_Transaction_Raw_Dataset.csv que vous pouvez utiliser.) Le téléchargement du fichier lancera le pipeline ETL via Step Functions. 3. Sur la console Step Functions, vérifiez l'état du pipeline ETL.	Developer

Tâche	Description	Compétences requises
Vérifiez la présence du jeu de données partitionné.	Lorsque le pipeline ETL est terminé, vérifiez que l'ensemble de données partitionné est disponible dans le dossier de transformation Amazon S3 (`transform` ou dans le nom du dossier que vous avez défini dans le `parameter.json` fichier).	Developer
Vérifiez la base de données AWS Glue partitionnée.	1. Sur la console AWS Glue, sélectionnez la base de données AWS Glue créée par la pile (il s'agit de la base de données que vous avez mentionnée dans l'épopée précédente). 2. Vérifiez que la table partitionnée est disponible dans le catalogue de données AWS Glue.	Developer
Exécutez des requêtes.	(Facultatif) Utilisez Amazon Athena pour exécuter des requêtes ad hoc sur la base de données partitionnée et transformée. Pour obtenir des instructions, consultez la section Exécution de requêtes SQL à l'aide d'Amazon Athena dans la documentation AWS.	analyste de base de données

Résolution des problèmes

Problème	Solution
Autorisations AWS Identity and Access Management (IAM) pour le job et le crawler AWS Glue	Si vous personnalisez davantage la tâche AWS Glue ou le robot d'exploration, veillez à accorder les autorisations IAM appropriées dans le rôle IAM utilisé par la tâche AWS Glue, ou à fournir des autorisations de données à AWS Lake Formation. Pour plus d'informations, consultez la documentation AWS.

Ressources connexes

Documentation des services AWS

- AWS Step Functions
- AWS Glue
- AWS Lambda
- Amazon S3
- Amazon SNS

Informations supplémentaires

Le schéma suivant montre le flux de travail AWS Step Functions pour un pipeline ETL réussi, à partir du panneau Step Functions Inspector.

Le schéma suivant montre le flux de travail AWS Step Functions pour un pipeline ETL qui échoue en raison d'une erreur de validation des entrées, depuis le panneau Step Functions Inspector.

Effectuez des analyses avancées à l'aide d'Amazon Redshift ML

Créée par Po Hong (AWS) et Chyanna Antonio (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), vous pouvez utiliser l'apprentissage automatique Amazon Redshift (Amazon Redshift ML) pour effectuer des analyses de machine learning sur les données stockées dans un cluster Amazon Redshift ou sur Amazon Simple Storage Service (Amazon S3). Amazon Redshift ML prend en charge l'apprentissage supervisé, qui est généralement utilisé pour des analyses avancées. Les cas d'utilisation d'Amazon Redshift ML incluent les prévisions de revenus, la détection des fraudes par carte de crédit, la valeur à vie du client (CLV) ou les prévisions de désabonnement des clients.

Amazon Redshift ML permet aux utilisateurs de bases de données de créer, d'entraîner et de déployer facilement des modèles de ML à l'aide de commandes SQL standard. Amazon Redshift ML utilise Amazon SageMaker Autopilot pour entraîner et ajuster automatiquement les meilleurs modèles de ML à des fins de classification ou de régression en fonction de vos données, tout en conservant le contrôle et la visibilité.

Toutes les interactions entre Amazon Redshift, Amazon S3 et Amazon SageMaker sont supprimées et automatisées. Une fois le modèle ML formé et déployé, il devient disponible en tant que fonction définie par l'utilisateur (UDF) dans Amazon Redshift et peut être utilisé dans les requêtes SQL.

Ce modèle complète les modèles de création, d'entraînement et de déploiement de modèles de machine learning dans Amazon Redshift en utilisant SQL avec Amazon Redshift ML du blog AWS, ainsi que le didacticiel sur la création, l'entraînement et le déploiement d'un modèle de machine learning avec SageMaker Amazon du Getting Started Resource Center.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Données existantes dans une table Amazon Redshift

Compétences

- Connaissance des termes et concepts utilisés par Amazon Redshift ML, notamment l'apprentissage automatique, la formation et les prédictions. Pour plus d'informations à ce sujet, consultez la section Training ML models dans la documentation Amazon Machine Learning (Amazon ML).
- Expérience de la configuration utilisateur d'Amazon Redshift, de la gestion des accès et de la syntaxe SQL standard. Pour plus d'informations à ce sujet, consultez Getting started with Amazon Redshift dans la documentation Amazon Redshift.
- Connaissance et expérience d'Amazon S3 et d'AWS Identity and Access Management (IAM).
- L'expérience de l'exécution de commandes dans l'interface de ligne de commande AWS (AWS CLI) est également utile, mais elle n'est pas obligatoire.

Limites

- Le cluster Amazon Redshift et le compartiment S3 doivent être situés dans la même région AWS.
- L'approche de ce modèle ne prend en charge que les modèles d'apprentissage supervisé tels que la régression, la classification binaire et la classification multiclasse.

Architecture

Les étapes suivantes expliquent comment Amazon Redshift ML fonctionne SageMaker pour créer, entraîner et déployer un modèle de ML :

1. Amazon Redshift exporte les données d'entraînement vers un compartiment S3.
2. SageMaker Le pilote automatique prétraite automatiquement les données d'entraînement.
3. Une fois l'`CREATE MODEL`instruction invoquée, Amazon Redshift ML l'utilise SageMaker pour l'entraînement.
4. SageMaker Le pilote automatique recherche et recommande l'algorithme ML et les hyperparamètres optimaux qui optimisent les métriques d'évaluation.
5. Amazon Redshift ML enregistre le modèle ML de sortie en tant que fonction SQL dans le cluster Amazon Redshift.
6. La fonction du modèle ML peut être utilisée dans une instruction SQL.

Pile technologique

- Amazon Redshift
- SageMaker
- Amazon S3

Outils

- Amazon Redshift — Amazon Redshift est un service d'entreposage de données entièrement géré au niveau de l'entreprise, à l'échelle du pétaoctet.
- Amazon Redshift ML — Amazon Redshift Machine Learning (Amazon Redshift ML) est un service robuste basé sur le cloud qui permet aux analystes et aux data scientists de tous niveaux d'utiliser facilement la technologie ML.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.
- Amazon SageMaker — SageMaker est un service de machine learning entièrement géré.
- Amazon SageMaker Autopilot — Le SageMaker pilote automatique est un ensemble de fonctionnalités qui automatise les tâches clés d'un processus d'apprentissage automatique (AutoML).

Code

Vous pouvez créer un modèle de machine learning supervisé dans Amazon Redshift à l'aide du code suivant :

```
“CREATE MODEL customer_churn_auto_model
FROM (SELECT state,
             account_length,
             area_code,
             total_charge/account_length AS average_daily_spend,
             cust_serv_calls/account_length AS average_daily_cases,
             churn
      FROM customer_activity
      WHERE  record_date < '2020-01-01'
     )
TARGET churn
FUNCTION ml_fn_customer_churn_auto
IAM_ROLE 'arn:aws:iam::XXXXXXXXXXXX:role/Redshift-ML'
SETTINGS (
```

```
  S3_BUCKET 'your-bucket'
);")
```

> **Note**
>
> L'SELECTétat peut faire référence aux tables standard Amazon Redshift, aux tables externes Amazon Redshift Spectrum, ou aux deux.

Épopées

Préparer un ensemble de données de formation et de test

Tâche	Description	Compétences requises
Préparez un ensemble de données de formation et de test.	Connectez-vous à l'AWS Management Console et ouvrez la SageMaker console Amazon. Suivez les instructions du didacticiel sur la création, l'entraînement et le déploiement d'un modèle d'apprentissage automatique pour créer un fichier .csv ou Apache Parquet comportant une colonne d'étiquette (formation supervisée) et aucun en-tête. **Note** Nous vous recommandons de mélanger et de diviser le jeu de données brut en un ensemble d'apprentissage pour l'entraînement du	Spécialiste des données

Tâche	Description	Compétences requises
	modèle (70 %) et un ensemble de test pour l'évaluation des performances du modèle (30 %).	

Préparation et configuration de la pile technologique

Tâche	Description	Compétences requises
Créez et configurez un cluster Amazon Redshift.	Sur la console Amazon Redshift, créez un cluster en fonction de vos besoins. Pour plus d'informations à ce sujet, consultez la section Créer un cluster dans la documentation Amazon Redshift. **Important** Les clusters Amazon Redshift doivent être créés avec le suivi de `SQL_PREVIEW` maintenance. Pour plus d'informations sur les pistes de prévisualisation, consultez Choisir les pistes de maintenance du cluster dans la documentation Amazon Redshift.	DBA, architecte cloud

Tâche	Description	Compétences requises
Créez un compartiment S3 pour stocker les données d'entraînement et les artefacts du modèle.	Sur la console Amazon S3, créez un compartiment S3 pour les données d'entraînement et de test. Pour plus d'informations sur la création d'un compartiment S3, consultez Créer un compartiment S3 à partir d'AWS Quick Starts. **⚠ Important** Assurez-vous que votre cluster Amazon Redshift et votre compartiment S3 se trouvent dans la même région.	DBA, architecte cloud
Créez et associez une politique IAM au cluster Amazon Redshift.	Créez une politique IAM pour autoriser le cluster Amazon Redshift à SageMaker accéder à Amazon S3. Pour obtenir des instructions et des étapes, consultez la section Configuration du cluster pour l'utilisation d'Amazon Redshift ML dans la documentation Amazon Redshift.	DBA, architecte cloud

Tâche	Description	Compétences requises
Autorisez les utilisateurs et les groupes Amazon Redshift à accéder aux schémas et aux tables.	Accordez des autorisations pour permettre aux utilisateurs et aux groupes d'Amazon Redshift d'accéder aux schémas et aux tables internes et externes. Pour connaître les étapes et les instructions, consultez la section Gestion des autorisations et de la propriété dans la documentation Amazon Redshift.	DBA

Créez et entraînez le modèle ML dans Amazon Redshift

Tâche	Description	Compétences requises
Créez et entraînez le modèle ML dans Amazon Redshift.	Créez et entraînez votre modèle de machine learning dans Amazon Redshift ML. Pour plus d'informations, consultez la `CREATE MODEL` déclaration contenue dans la documentation Amazon Redshift.	Développeur, data scientist

Effectuer des inférences et des prédictions par lots dans Amazon Redshift

Tâche	Description	Compétences requises
Effectuez une inférence à l'aide de la fonction de modèle ML générée.	Pour plus d'informations sur l'inférence à l'aide de la fonction de modèle ML	Data scientist, utilisateur de business intelligence

Tâche	Description	Compétences requises
	générée, consultez Predictio n dans la documentation Amazon Redshift.	

Ressources connexes

Préparer un ensemble de données de formation et de test

- Création, formation et déploiement d'un modèle d'apprentissage automatique avec Amazon SageMaker

Préparation et configuration de la pile technologique

- Création d'un cluster Amazon Redshift
- Choisir les pistes de maintenance du cluster Amazon Redshift
- Création d'un compartiment S3
- Configuration d'un cluster Amazon Redshift pour utiliser Amazon Redshift ML
- Gestion des autorisations et de la propriété dans Amazon Redshift

Créez et entraînez le modèle ML dans Amazon Redshift

- Déclaration CREATE MODEL dans Amazon Redshift

Effectuer des inférences et des prédictions par lots dans Amazon Redshift

- Prédiction dans Amazon Redshift

Autres ressources

- Commencer à utiliser Amazon Redshift ML

- Création, formation et déploiement de modèles de machine learning dans Amazon Redshift à l'aide de SQL avec Amazon Redshift ML
- Partenaires Amazon Redshift
- Partenaires de compétences AWS en apprentissage automatique

Interrogez les tables Amazon DynamoDB avec SQL à l'aide d'Amazon Athena

Créée par Gavin Perrie (AWS), Ajit Ambike (AWS) et Brad Yates (AWS)

Récapitulatif

Si vos données incluent des sources autres qu'Amazon Simple Storage Service (Amazon S3), vous pouvez utiliser des requêtes fédérées pour accéder à ces sources de données relationnelles, non relationnelles, objets ou personnalisées. Ce modèle montre comment configurer l'accès aux requêtes fédérées via Amazon Athena vers Amazon DynamoDB à l'aide d'un connecteur de source de données SQL.

À l'aide de ce modèle, vous pouvez effectuer les opérations suivantes :

- Interrogez les tables DynamoDB à l'aide de SQL.
- Exécutez des requêtes SQL fédérées dans Athena et associez des tables DynamoDB à d'autres sources de données prises en charge.

Conditions préalables et limitations

Prérequis

- Une table DynamoDB.
- Un groupe de travail Athena configuré pour utiliser la version 2 du moteur Athena. Pour obtenir des instructions, consultez la documentation d'Athena.
- Un compartiment S3 dans lequel la `AthenaDynamoDBConnector` AWS Lambda fonction peut diffuser les données. Le compartiment S3 et la fonction Lambda doivent se trouver dans la même région AWS.

Si c'est la première fois que vous accédez à Athena, vous aurez besoin d'un compartiment S3 supplémentaire à utiliser comme emplacement des résultats de requête. Pour obtenir des instructions, consultez la documentation d'Athena.

Limites

- Les opérations d'écriture telles que INSERT INTO ne sont pas prises en charge.

Versions du produit

- Athena Query Federation sort sur GitHub

Architecture

Architecture cible

Le schéma suivant montre le flux de connexion une fois le schéma établi. L'utilisateur se connecte à Amazon Athena pour fournir la requête. Athena transmet la requête et la cible à la fonction Lambda du connecteur de source de données DynamoDB, qui récupère et renvoie les données à Athena. Si de grandes quantités de données sont renvoyées, Athena stocke les résultats temporaires dans le seau avant de conditionner et de renvoyer l'ensemble de données complet.

Outils

Services AWS

- Amazon Athena est un service de requêtes interactif qui vous permet d'analyser les données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du langage SQL standard. Ce modèle utilise le connecteur Amazon Athena DynamoDB, un outil créé à l'aide du SDK Amazon Athena Query Federation et installé en tant qu'application via le. AWS Lambda AWS Serverless Application Repository
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Athena Query Federation.

Épopées

Configuration et test du connecteur de source de données DynamoDB

Tâche	Description	Compétences requises
Déployez AthenaDynamoDBConnector l'application.	Pour effectuer AthenaDynamoDBConnecter le déploiement, procédez comme suit : 1. Connectez-vous au AWS Management Console et choisissez Région AWS celui que vous utilisez pour la table DynamoDB et le bucket spill. 2. Ouvrez le Serverless Application Repository https://console.aws.amazon.com/serverlessrepo/ à l'adresse. 3. Dans le volet de navigation, sélectionnez Applications disponibles. 4. Pour l'accès AWS Identity and Access Management (IAM), sous la barre de recherche, cochez la case Afficher les applications qui créent des rôles ou des politiques de ressources IAM personnalisés. 5. Recherchez AthenaDynamoDBConnector, sélectionnez et assurez-vous que	AWS DevOps

Tâche	Description	Compétences requises
	l'auteur répertorié est Amazon Athena Federation. 6. Dans Paramètres de l'application, entrez les valeurs suivantes : • SpillBucket– Emplacement vers lequel la fonction peut envoyer des données. • AthenaCatalogName– Nom de la fonction Lambda qui sera créée. Le nom sera également utilisé comme nom de source de données dans Athena. 7. Cochez la case pour accuser réception de la création de rôles et de politiques IAM. 8. Choisissez Déployer.	

Tâche	Description	Compétences requises
Créez une source de données pour Athena.	Pour créer la source de données, procédez comme suit : 1. Ouvrez la console Athena à https://console.aws.amazon.com/athena/. 2. Développez le volet de navigation et choisissez Sources de données. 3. Choisissez Create data source. 4. Choisissez Amazon DynamoDB. 5. Entrez le nom de la source de données. 6. Sélectionnez la fonction Lambda que vous avez créée. 7. Passez en revue les détails, puis choisissez Créer une source de données.	AWS DevOps

Tâche	Description	Compétences requises
Utilisez Athena pour interroger la table DynamoDB.	Pour interroger la table DynamoDB, procédez comme suit : 1. Sur la console Athena, développez le volet de navigation et choisissez l'éditeur de requêtes. 2. Dans la liste déroulant e Source de données, sélectionnez la source de données que vous avez créée. 3. Vérifiez que les tables DynamoDB sont répertori ées sous Tables. 4. Exécutez la requête.	Développeur d’applications

Résolution des problèmes

Problème	Solution
La requête échoue avec `GENERIC_I NTERNAL_ERROR: The bucket is in this region: <region>`.	Assurez-vous que le godet de déversement Athena et la fonction Lambda sont créés de la même manière. Région AWS
La source de données nouvellement créée n'est pas visible sur la console Athena.	Les catalogues de données Athena sont régionaux. Assurez-vous `AthenaDyn amoDBConnector` qu'il a été déployé dans la région où vous essayez d'utiliser Athéna.
Vous ne pouvez pas exécuter la requête sur la source de données nouvellement créée.	Vérifiez que l'emplacement des résultats de la requête a été défini.

Ressources connexes

- Connecteur Amazon Athena DynamoDB
- Requête fédérée Amazon Athena

Accédez aux tables Amazon DynamoDB, interrogez-les et joignez-les à l'aide d'Athena

Créée par Moinul Al-Mamun (AWS)

Récapitulatif

Ce modèle explique comment configurer une connexion entre Amazon Athena et Amazon DynamoDB à l'aide du connecteur Amazon Athena DynamoDB. Le connecteur utilise une fonction AWS Lambda pour interroger les données dans DynamoDB. Vous n'avez pas besoin d'écrire de code pour configurer la connexion. Une fois la connexion établie, vous pouvez accéder rapidement aux tables DynamoDB et les analyser en utilisant Athena Federated Query pour exécuter des commandes SQL depuis Athena. Vous pouvez également joindre une ou plusieurs tables DynamoDB entre elles ou à d'autres sources de données, telles qu'Amazon Redshift ou Amazon Aurora.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif autorisé à gérer les tables DynamoDB, les sources de données Athena, Lambda et les rôles AWS Identity and Access Management (IAM)
- Un bucket Amazon Simple Storage Service (Amazon S3) dans lequel Athena peut stocker les résultats des requêtes
- Un compartiment S3 dans lequel le connecteur Athena DynamoDB peut enregistrer les données à court terme
- Une région AWS qui prend en charge la version 2 du moteur Athena
- Autorisations IAM pour accéder à Athena et aux compartiments S3 requis
- Connecteur Amazon Athena DynamoDB, installé

Limites

L'interrogation des tables DynamoDB entraîne un coût. Les tailles de table supérieures à quelques gigaoctets (GBs) peuvent entraîner des coûts élevés. Nous vous recommandons de tenir compte des coûts avant d'effectuer une opération de numérisation complète de la table. Pour plus d'informations, consultez Tarification Amazon DynamoDB. Pour réduire les coûts et atteindre des performances élevées, nous vous recommandons de toujours utiliser LIMIT dans votre requête (par exemple,`SELECT * FROM table1 LIMIT 10`). Par ailleurs, avant d'exécuter une requête JOIN

ou GROUP BY dans un environnement de production, tenez compte de la taille de vos tables. Si vos tables sont trop volumineuses, envisagez d'autres options, telles que la migration de la table vers Amazon S3.

Architecture

Le schéma suivant montre comment un utilisateur peut exécuter une requête SQL sur une table DynamoDB à partir d'Athena.

Le schéma suivant illustre le flux de travail suivant :

1. Pour interroger une table DynamoDB, un utilisateur exécute une requête SQL depuis Athena.
2. Athena lance une fonction Lambda.
3. La fonction Lambda interroge les données demandées dans la table DynamoDB.
4. DynamoDB renvoie les données demandées à la fonction Lambda. Ensuite, la fonction transfère les résultats de la requête à l'utilisateur via Athena.
5. La fonction Lambda stocke les données dans le compartiment S3.

Pile technologique

- Amazon Athena
- Amazon DynamoDB
- Amazon S3
- AWS Lambda

Outils

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- Le connecteur Amazon Athena DynamoDB est un outil AWS qui permet à Athena de se connecter à DynamoDB et d'accéder à vos tables à l'aide de requêtes SQL.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire

et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Épopées

Création d'exemples de tables DynamoDB

Tâche	Description	Compétences requises
Créez le premier exemple de table.	1. Connectez-vous à la console de gestion AWS et ouvrez la console DynamoDB. 2. Choisissez Créer un tableau. 3. Dans le champ Nom de la table, entrez dydbtable1. 4. Pour Clé de partition, entrez PK1. 5. Pour la touche de tri, entrez SK1. 6. Dans la section Paramètres du tableau, choisissez Personnaliser les paramètres. 7. Dans la section Classe de table, sélectionnez DynamoDB Standard. 8. Dans la section Paramètres de capacité de lecture/écriture, pour le mode Capacité, sélectionnez À la demande. 9. Dans la section Chiffrement au repos, sélection	Developer

Tâche	Description	Compétences requises
	nez Owned by Amazon DynamoDB. 10. Choisissez Créer un tableau.	

Tâche	Description	Compétences requises

Insérez des exemples de données dans le premier tableau.	1. Ouvrez la console DynamoDB.
	2. Dans le volet de navigation, choisissez Table, puis choisissez votre table dans la colonne Nom.
	3. Choisissez Actions, puis sélectionnez Créer un élément.
	4. Choisissez la vue JSON.
	5. Dans la barre de titre de l'éditeur d'attributs, désactivez View DynamoDB JSON.
	6. Dans l'éditeur d'attributs, entrez les exemples de données suivants un par un :
	
	`{ "PK1": "1234", "SK1": "info", "Salary": "5000" }`
	
	`{ "PK1": "1235", "SK1": "info", "Salary": "5200" }`
		Developer

Tâche	Description	Compétences requises
Créez le deuxième exemple de table.	1. Ouvrez la console DynamoDB. 2. Choisissez Créer un tableau. 3. Dans le champ Nom de la table, entrez dydbtable2. 4. Pour Clé de partition, saisissez PK2. 5. Pour la touche de tri, entrez SK2. 6. Dans la section Paramètres du tableau, choisissez Personnaliser les paramètres. 7. Dans la section Classe de table, sélectionnez DynamoDB Standard. 8. Dans la section Paramètres de capacité de lecture/écriture, pour le mode Capacité, sélectionnez À la demande. 9. Dans la section Chiffrement au repos, sélectionnez Owned by Amazon DynamoDB. 10. Choisissez Créer un tableau.	Developer

Tâche	Description	Compétences requises

Insérez des exemples de données dans le deuxième tableau.	1. Ouvrez la console DynamoDB.
	2. Dans le volet de navigation, choisissez Table, puis choisissez votre table dans la colonne Nom.
	3. Choisissez Actions, puis sélectionnez Créer un élément.
	4. Dans la barre de titre de l'éditeur d'attributs, désactivez View DynamoDB JSON.
	5. Dans l'éditeur d'attributs, entrez les exemples de données suivants un par un :
	
	`{ "PK2": "1234", "SK2": "bonus", "Bonus": "500" }`
	
	`{ "PK2": "1235", "SK2": "bonus", "Bonus": "1000" }`
		Developer

Création d'une source de données dans Athena pour DynamoDB

Tâche	Description	Compétences requises
Configurez le connecteur de source de données.	Créez une source de données pour DynamoDB, puis créez une fonction Lambda pour vous connecter à cette source de données. 1. Connectez-vous à l'AWS Management Console et ouvrez la console Athena. 2. Dans le volet de navigation, choisissez Sources de données, puis sélectionnez Créer une source de données. 3. Choisissez la source de données Amazon DynamoDB, puis cliquez sur Next. 4. Dans la section Détails de la source de données, pour Nom de la source de données, entrez TestDynamoDB. 5. Dans la section Détails de la connexion, sélectionnez une fonction Lambda déjà déployée ou choisissez Create Lambda function si vous n'avez pas de fonction Lambda à utiliser pour ce modèle. Remarque : Pour plus d'informations sur la	Developer

Tâche	Description	Compétences requises
	création d'une fonction Lambda, consultez Getting started with Lambda dans le guide du développeur Lambda. 6. (Facultatif) Si vous choisissez la fonction Create Lambda, vous devez configurer le CloudFormation modèle AWS inclus par l'application Java avant de déployer cette pile. Le modèle inclut ApplicationName, SpillBucket AthenaCatalogName, et d'autres paramètres de l'application. Remarque : Après avoir déployé cette application Java, la pile crée une fonction Lambda qui permet à Athena de communiquer avec DynamoDB. Cela rend vos tables accessibles par le biais de commandes SQL. 7. Déployez votre fonction Lambda. 8. Choisissez Suivant.	

Tâche	Description	Compétences requises
Vérifiez que la fonction Lambda peut accéder au compartiment de déversement S3.	1. Ouvrez la console Lambda. 2. Dans le volet de navigation, choisissez Functions, puis choisissez la fonction que vous avez créée précédemment. 3. Cliquez sur l'onglet Configuration. 4. Dans le volet gauche, choisissez Variables d'environnement, puis vérifiez que la valeur de la clé est `spill_bucket` . 5. Dans le volet gauche, choisissez Permissions, puis dans la section Rôle d'exécution, choisissez le rôle IAM attaché. Remarque : Vous êtes dirigé vers le rôle IAM associé à votre fonction Lambda dans la console IAM. 6. Vérifiez que vous disposez d'une autorisation d'écriture sur le `spill_bucket` bucket. Si vous rencontrez des erreurs, consultez la section Informations supplémentaires de ce modèle pour obtenir des conseils.	Developer

Accédez aux tables DynamoDB depuis Athena

Tâche	Description	Compétences requises
Interrogez les tables DynamoDB.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Athena. 2. Dans le volet de navigation, choisissez Sources de données, puis sélectionnez Créer une source de données. 3. Dans le panneau de navigation, choisissez Query Editor (Éditeur de requête). 4. Dans l'onglet Éditeur, dans la section Données, pour Source de données, choisissez votre source de données pour Source de données. 5. Pour Database (Base de données), choisissez votre base de données. 6. Pour la requête 1, entrez la requête suivante : `SELECT * FROM dydbtable1 t1;` 7. Choisissez Exécuter, puis vérifiez le résultat dans le tableau. 8. Pour la requête 2, entrez la requête suivante : `SELECT`	Developer

Tâche	Description	Compétences requises
	`* FROM dydbtable2 t2;` 9. Choisissez Exécuter, puis vérifiez le résultat dans le tableau.	
Joignez les deux tables DynamoDB.	DynamoDB est un magasin de données NoSQL qui ne prend pas en charge l'opération de jointure SQL. Par conséquent, vous devez effectuer une opération de jointure sur deux tables DynamoDB : 1. Cliquez sur l'icône plus pour créer une autre requête. 2. Pour la requête 3, entrez la requête suivante : `SELECT pk1, salary, bonus FROM dydbtable1 t1 JOIN dydbtable2 t2 ON t1.pk1 = t2.pk2;`	Developer

Ressources connexes

- Connecteur Amazon Athena DynamoDB (AWS Labs)
- Interrogez n'importe quelle source de données avec la nouvelle requête fédérée d'Amazon Athena (blog AWS Big Data)
- Référence de version du moteur Athena (Guide de l'utilisateur Athena)
- Simplifiez l'extraction et l'analyse des données Amazon DynamoDB à l'aide d'AWS Glue et d'Amazon Athena (blog de base de données AWS)

Informations supplémentaires

Si vous exécutez une requête dans Athena `spill_bucket` au `{bucket_name}/folder_name/` format, le message d'erreur suivant peut s'afficher :

```
"GENERIC_USER_ERROR: Encountered an exception[java.lang.RuntimeException] from your
 LambdaFunction[arn:aws:lambda:us-east-1:xxxxxx:function:testdynamodb] executed in
 context[retrieving meta-data] with message[You do NOT own the spill bucket with the
 name: s3://amzn-s3-demo-bucket/athena_dynamodb_spill_data/]
This query ran against the "default" database, unless qualified by the query. Please
 post the error message on our forum  or contact customer support with Query Id:
 [query-id]"
```

Pour résoudre cette erreur, mettez à jour la variable d'environnement de la fonction Lambda `spill_bucket` vers`{bucket_name_only}`, puis mettez à jour la politique Lambda IAM suivante pour l'accès en écriture au bucket :

```
{
            "Action": [
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketLocation",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::spill_bucket",
                "arn:aws:s3:::spill_bucket/*"
            ],
            "Effect": "Allow"
        }
```

Vous pouvez également supprimer le connecteur de source de données Athena que vous avez créé précédemment et le recréer en utilisant uniquement pour. `{bucket_name}` `spill_bucket`

Configurez un espace de données minimum viable pour partager les données entre les organisations

Créé par Ramy Hcini (Think-it), Ismail Abdellaoui (Think-it), Malte Gasseling (Think-it), Jorge Hernandez Suarez (AWS) et Michael Miller (AWS)

Récapitulatif

Les espaces de données sont des réseaux fédérés pour l'échange de données, la confiance et le contrôle des données étant des principes fondamentaux. Ils permettent aux entreprises de partager, d'échanger et de collaborer sur des données à grande échelle en proposant une solution rentable et indépendante de la technologie.

Les espaces de données ont le potentiel de stimuler de manière significative les efforts en faveur d'un futur durable en utilisant la résolution de problèmes basée sur les données avec une end-to-end approche impliquant toutes les parties prenantes concernées.

Ce modèle vous montre comment deux entreprises peuvent utiliser la technologie de l'espace de données sur Amazon Web Services (AWS) pour faire avancer leur stratégie de réduction des émissions de carbone. Dans ce scénario, l'entreprise X fournit des données sur les émissions de carbone, que l'entreprise Y consomme. Consultez la section Informations supplémentaires pour obtenir les détails suivants sur les spécifications de l'espace de données :

- Les participants
- Affaire de cas
- Autorité de l'espace de données
- Composants de l'espace de données
- Services d'espace de données
- Données à échanger
- Modèle de données
- Connecteur Tractus-X EDC

Le modèle inclut les étapes suivantes :

- Déploiement de l'infrastructure nécessaire à un espace de données de base avec deux participants AWS.

- Échange de données sur l'intensité des émissions de carbone en utilisant les connecteurs de manière sécurisée.

Ce modèle déploie un cluster Kubernetes qui hébergera les connecteurs d'espace de données et leurs services via Amazon Elastic Kubernetes Service (Amazon EKS).

Le plan de contrôle et le plan de données Eclipse Dataspace Components (EDC) sont tous deux déployés sur Amazon EKS. Le graphique officiel de Tractus-X Helm déploie les services PostgreSQL et Vault en tant que dépendances HashiCorp .

En outre, le service d'identité est déployé sur Amazon Elastic Compute Cloud (Amazon EC2) pour reproduire un scénario réel d'espace de données minimum viable (MVDS).

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS pour déployer l'infrastructure de votre choix Région AWS
- Un utilisateur AWS Identity and Access Management (IAM) ayant accès à Amazon S3 qui sera utilisé temporairement en tant qu'utilisateur technique (le connecteur EDC ne prend actuellement pas en charge l'utilisation de rôles). Nous vous recommandons de créer un utilisateur IAM spécifiquement pour cette démo et de lui attribuer des autorisations limitées.)
- AWS Command Line Interface (AWS CLI) installé et configuré dans la configuration de votre choix Région AWS
- AWS informations d'identification de sécurité
- eksctl sur votre poste de travail
- Git sur votre poste de travail
- kubectl
- Casque
- facteur
- Un certificat SSL/TLS AWS Certificate Manager (ACM)
- Un nom DNS qui pointera vers un Application Load Balancer (le nom DNS doit être couvert par le certificat ACM)
- HashiCorp Vault (pour plus d'informations sur l'utilisation AWS Secrets Manager pour gérer les secrets, consultez la section Informations supplémentaires.)

Versions du produit

- AWS CLI version 2+
- Collection Postman v2.1

Limites

- Sélection du connecteur – Ce déploiement utilise un connecteur basé sur EDC. Cependant, assurez-vous de prendre en compte les points forts et les fonctionnalités des connecteurs EDC et FIWARE True afin de prendre une décision éclairée qui correspond aux besoins spécifiques du déploiement.
- Conception du connecteur EDC – La solution de déploiement choisie repose sur le tableau de bord du connecteur EDC de Tractus-X, une option de déploiement bien établie et largement testée. La décision d'utiliser ce tableau est motivée par son utilisation courante et par l'inclusion d'extensions essentielles dans la version fournie. Bien que PostgreSQL HashiCorp et Vault soient des composants par défaut, vous avez la possibilité de personnaliser votre propre version de connecteur si nécessaire.
- Accès au cluster privé – L'accès au cluster EKS déployé est limité aux canaux privés. L'interaction avec le cluster s'effectue exclusivement à l'aide `kubectl` d'un IAM. L'accès public aux ressources du cluster peut être activé à l'aide d'équilibreurs de charge et de noms de domaine, qui doivent être mis en œuvre de manière sélective pour exposer des services spécifiques à un réseau plus large. Cependant, nous ne recommandons pas de fournir un accès public.
- Concentration sur la sécurité – L'accent est mis sur l'abstraction des configurations de sécurité par rapport aux spécifications par défaut afin que vous puissiez vous concentrer sur les étapes de l'échange de données du connecteur EDC. Bien que les paramètres de sécurité par défaut soient conservés, il est impératif d'activer les communications sécurisées avant d'exposer le cluster au réseau public. Cette précaution garantit une base solide pour un traitement sécurisé des données.
- Coût de l'infrastructure – Une estimation du coût de l'infrastructure peut être obtenue à l'aide du Calculateur de tarification AWS. Un simple calcul montre que les coûts peuvent atteindre 162,92 USD par mois pour l'infrastructure déployée.

Architecture

L'architecture MVDS comprend deux clouds privés virtuels (VPCs), l'un pour le service d'identité DAPS (Dynamic Attribute Provisioning System) et l'autre pour Amazon EKS.

Architecture DAPS

Le schéma suivant montre le DAPS exécuté sur des EC2 instances contrôlées par un groupe Auto Scaling. Un Application Load Balancer et une table de routage exposent les serveurs DAPS. Amazon Elastic File System (Amazon EFS) synchronise les données entre les instances DAPS.

Architecture d'Amazon EKS

Les espaces de données sont conçus pour être des solutions indépendantes de la technologie, et plusieurs implémentations existent. Ce modèle utilise un cluster Amazon EKS pour déployer les composants techniques de l'espace de données. Le schéma suivant montre le déploiement du cluster EKS. Les nœuds de travail sont installés dans des sous-réseaux privés. Les pods Kubernetes accèdent à l'instance Amazon Relational Database Service (Amazon RDS) pour PostgreSQL qui se trouve également dans les sous-réseaux privés. Les pods Kubernetes stockent les données partagées dans Amazon S3.

Outils

AWS services

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le AWS Cloud.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les EC2 instances, les conteneurs et les adresses IP dans une ou plusieurs zones de disponibilité.

Autres outils

- eksctl est un utilitaire de ligne de commande permettant de créer et de gérer des clusters Kubernetes sur Amazon EKS.
- Git est un système de contrôle de version distribué et open source.
- HashiCorp Vault fournit un stockage sécurisé avec un accès contrôlé aux informations d'identification et autres informations sensibles.
- Helm est un gestionnaire de packages open source pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes.
- kubectl est une interface de ligne de commande qui vous permet d'exécuter des commandes sur des clusters Kubernetes.
- Postman est une plateforme d'API.

Référentiel de code

Les fichiers YAML de configuration Kubernetes et les scripts Python pour ce modèle sont disponibles dans le référentiel. GitHub aws-patterns-edc Le modèle utilise également le référentiel Tractus-X EDC.

Bonnes pratiques

Amazon EKS et isolation des infrastructures des participants

Dans Kubernetes, les espaces de noms sépareront l'infrastructure du fournisseur X de l'infrastructure du consommateur de l'entreprise Y selon ce schéma. Pour plus d'informations, consultez les guides des meilleures pratiques d'EKS.

Dans une situation plus réaliste, chaque participant disposerait d'un cluster Kubernetes distinct fonctionnant au sein de son propre cluster. Compte AWS L'infrastructure partagée (DAPS dans ce modèle) serait accessible aux participants à l'espace de données tout en étant complètement séparée des infrastructures des participants.

Épopées

Configuration de l'environnement et mise en service d'un cluster et d' EC2 instances EKS

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le référentiel sur votre poste de travail, exécutez la commande suivante : `git clone https://github.com/Think-iT-Labs/aws-patterns-edc` Le poste de travail doit avoir accès à votre Compte AWS.	DevOps ingénieur
Provisionnez le cluster Kubernetes et configurez des espaces de noms.	Pour déployer un cluster EKS simplifié par défaut dans votre compte, exécutez la `eksctl` commande suivante sur le poste de travail sur lequel vous avez cloné le dépôt : `eksctl create cluster` La commande crée le VPC et les sous-réseaux privés et publics qui s'étendent sur trois zones de disponibilité différentes. Une fois la couche réseau créée, la commande crée deux `m5.large` EC2 instances au sein d'un groupe Auto Scaling.	DevOps ingénieur

Tâche	Description	Compétences requises

	Pour plus d'informations et des exemples de sortie, consultez le guide eksctl.
	
	Après avoir provisionné le cluster privé, ajoutez le nouveau cluster EKS à votre configuration Kubernetes locale en exécutant la commande suivante :
	
	`aws eks update-kubeconfig --name <EKS CLUSTER NAME> --region <AWS REGION>`
	
	Ce modèle utilise le `eu-west-1` Région AWS pour exécuter toutes les commandes. Cependant, vous pouvez exécuter les mêmes commandes dans vos préférences Région AWS.
	
	Pour vérifier que vos nœuds EKS fonctionnent et sont prêts, exécutez la commande suivante :
	
	`kubectl get nodes`	

Tâche	Description	Compétences requises

Configurez les espaces de noms.	Pour créer des espaces de noms pour le fournisseur et le consommateur, exécutez les commandes suivantes :
	`kubectl create ns provider`
	`kubectl create ns consumer`
	Dans ce modèle, il est important d'utiliser `provider` et d'utiliser `consumer` comme espaces de noms pour adapter les configurations aux étapes suivantes.
		DevOps ingénieur

Déployer le service d'identité

Tâche	Description	Compétences requises
Déployez le DAPS en utilisant AWS CloudFormation.	Pour faciliter la gestion des opérations DAPS, le serveur DAPS est installé sur les EC2 instances. Pour installer DAPS, utilisez le AWS CloudFormation modèle. Vous aurez besoin du certificat ACM et du nom DNS indiqués dans la section Prérequis. Le modèle déploie et configure les éléments suivants : • Application Load Balancer	DevOps ingénieur

Tâche	Description	Compétences requises
	• Groupe Auto Scaling • EC2 instances configurées avec les données utilisateur pour installer tous les packages nécessaires • Rôles IAM • DAPS Vous pouvez déployer le AWS CloudFormation modèle en vous connectant à la AWS CloudFormation console AWS Management Console et en utilisant celle-ci. Vous pouvez également déployer le modèle à l'aide d'une AWS CLI commande telle que la suivante : `aws cloudformation create-stack --stack-name daps \ --template-body file://aws-patterns-edc/cloudformation.yml --parameters \ ParameterKey=CertificateARN,ParameterValue=<ACM Certificate ARN> \ ParameterKey=DNSName,ParameterValue=<DNS name> \ ParameterKey=InstanceType,ParameterValue=<EC2 instance type> \`	

Tâche	Description	Compétences requises
	`ParameterKey=Environmentname,ParameterValue=<Environment Name> --capabilities CAPABILITY_NAMED_IAM` C'est à vous de choisir le nom de l'environnement. Nous vous recommandons d'utiliser un terme significatif, tel que`DapsInfrastructure`, car il sera reflété dans les balises de AWS ressources. Pour ce modèle, `t3.small` il est suffisamment grand pour exécuter le flux de travail DAPS, qui comporte trois conteneurs Docker. Le modèle déploie les EC2 instances dans des sous-réseaux privés. Cela signifie que les instances ne sont pas directement accessibles via SSH (Secure Shell) depuis Internet. Les instances sont dotées du rôle IAM et de l'AWS Systems Manager agent nécessaires pour permettre l'accès aux instances en cours d'exécution via le gestionnaire de session, une fonctionnalité de. AWS Systems Manager	

Tâche	Description	Compétences requises

	Nous vous recommandons d'utiliser le gestionnaire de session pour y accéder. Vous pouvez également configurer un hôte bastion pour autoriser l'accès SSH depuis Internet. Lorsque vous utilisez l'approche bastion host, l'exécution de l' EC2 instance peut prendre quelques minutes supplémentaires.
	
	Une fois le AWS CloudFormation modèle déployé avec succès, pointez le nom DNS sur le nom DNS de votre Application Load Balancer. Pour confirmer cela, exécutez la commande suivante :
	
	`dig <DNS NAME>`
	
	La sortie doit ressembler à ce qui suit :
	
	`; <<>> DiG 9.16.1-Ubuntu <<>> edc-pattern.think-it.io`
	`;; global options: +cmd`
	`;; Got answer:`
	`;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42344`
	`;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1`	

Tâche	Description	Compétences requises
	;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ;; QUESTION SECTION: ;edc-pattern.think- it.io. IN A ;; ANSWER SECTION: edc-pattern.think- it.io. 276 IN CNAME daps- alb-iap9zmwy3kn8-13287 73120.eu-west-1.el b.amazonaws.com. daps-alb-iap9zmwy3k n8-1328773120.eu-w est-1.elb.amazonaw s.com. 36 IN A 52.208.240.129 daps-alb-iap9zmwy3kn8 -1328773120.eu-wes t-1.elb.amazonaws. com. 36 IN A 52.210.15 5.124	

Tâche	Description	Compétences requises

Enregistrez les connecteurs des participants au service DAPS.	À partir de l'une des EC2 instances configurées pour le DAPS, enregistrez les participants :
	1. Exécutez le script disponible sur l' EC2 instance en utilisant l'utilisateur root :
	`cd /srv/mvds/omejdn-daps`
	2. Enregistrez le fournisseur :
	`bash scripts/register_connector.sh <provider_name>`
	3. Enregistrez le consommateur :
	`bash scripts/register_connector.sh <consumer_name>`
	Le choix des noms n'a aucune incidence sur les prochaines étapes. Nous vous recommandons d'utiliser soit `provider` et `consumer` soit `companyx` et`companyy`.
	Les commandes d'enregistrement configureront également automatiquement le service DAPS avec les
		DevOps ingénieur

Tâche	Description	Compétences requises
	informations nécessaires extraites des certificats et des clés créés. Lorsque vous êtes connecté à un serveur DAPS, collectez les informations nécessaires pour les étapes ultérieures de l'installation : 1. De `omejdn-daps/config/clients.yml` get the `client id` pour le fournisseur et le consommateur. Les `client id` valeurs sont de longues chaînes de chiffres hexadécimaux. 2. Dans le `omejdn-daps/keys` répertoire, copiez le contenu des `provider.key` fichiers `consumer.cert` `consumer.key` `provider.cert` ,, et. Nous vous recommandons de copier-coller le texte dans des fichiers portant le même nom et préfixés par le préfixe `daps-` sur votre poste de travail. Vous devez avoir le client IDs pour le fournisseur et le	

Tâche	Description	Compétences requises
	consommateur et vous devez avoir quatre fichiers dans votre répertoire de travail sur votre poste de travail : • Le nom du fichier source `consumer.cert` devient le nom du fichier du poste de travail`daps-consumer.cert` . • Le nom du fichier source `consumer.key` devient le nom du fichier du poste de travail`daps-consumer.key` . • Le nom du fichier source `provider.cert` devient le nom du fichier du poste de travail`daps-provider.cert` . • Le nom du fichier source `provider.key` devient le nom du fichier du poste de travail`daps-provider.key` .	

Déployez les connecteurs des participants

Tâche	Description	Compétences requises
Clonez le référentiel Tractus-X EDC et utilisez la version 0.4.1.	La version du connecteur Tractus-X EDC nécessite le déploiement et la disponibilité des services PostgreSQL	DevOps ingénieur

Tâche	Description	Compétences requises

	(base de données des actifs) et HashiCorp Vault (gestion des secrets).
	
	Il existe de nombreuses versions des cartes Tractus-X EDC Helm. Ce modèle spécifie la version 0.4.1 car il utilise le serveur DAPS.
	
	Les dernières versions utilisent le Managed Identity Wallet (MIW) avec une implémentation distribuée du service d'identité.
	
	Sur le poste de travail où vous avez créé les deux espaces de noms Kubernetes, clonez le référentiel tractusx-edc et consultez la branche. `release/0.4.1`
	
	`git clone https://github.com/eclipse-tractusx/tractusx-edc`
	
	`cd tractusx-edc`
	
	`git checkout release/0.4.1`	

Tâche	Description	Compétences requises

Configurez le graphique Tractus-X EDC Helm.	Modifiez la configuration du modèle de graphique Tractus-X Helm pour permettre aux deux connecteurs d'interagir ensemble.
	
	Pour ce faire, vous devez ajouter l'espace de noms au nom DNS du service afin qu'il puisse être résolu par les autres services du cluster. Ces modifications doivent être apportées au `charts/tractusx-connector/templates/_helpers.tpl` fichier. Ce modèle fournit une version finale modifiée de ce fichier que vous pouvez utiliser. Copiez-le et placez-le dans la `daps` section du fichier`charts/tractusx-connector/templates/_helpers.tpl` .
	
	Assurez-vous de commenter toutes les dépendances DAPS dans `charts/tractusx-connector/Chart.yaml` :
	
	`dependencies:`
	`  # IDS Dynamic Attribute Provisioning Service (IAM)`
	`  #  - name: daps`
		DevOps ingénieur

Tâche	Description	Compétences requises

	<pre># version: 0.0.1
	# repository:
	"file://./subcharts/
	omejdn"
	# alias: daps
	# condition:
	install.daps</pre>	

Tâche	Description	Compétences requises

Configurez les connecteurs pour utiliser PostgreSQL sur Amazon RDS.	(Facultatif) L'instance Amazon Relational Database Service (Amazon RDS) n'est pas requise dans ce modèle. Cependant, nous vous recommandons vivement d'utiliser Amazon RDS ou Amazon Aurora, car ils fournissent des fonctionn alités telles que la haute disponibilité, la sauvegarde et la restauration.
	
	Pour remplacer PostgreSQL sur Kubernetes par Amazon RDS, procédez comme suit :
	
	1. Provisionnez l'instance Amazon RDS for PostgreSQL.
	2. Dans `Chart.yaml` , commentez la `PostgreSQL` section.
	3. Dans `provider_values.yml` et `consumer_values.yml` , configurez la `postgresql` section comme suit :
	
	`postgresql:`
	`  auth:`
	`  database: edc`
	`  password: <RDS PASSWORD>`
		DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>username: <RDS Username>
	jdbcUrl: jdbc:postgresql://<RDS DNS NAME>:5432/edc
	username: <RDS Username>
	password: <RDS PASSWORD>
	primary:
	persistence:
	enabled: false
	readReplicas:
	persistence:
	enabled: false</pre>	

Tâche	Description	Compétences requises
Configurez et déployez le connecteur du fournisseur et ses services.	Pour configurer le connecteur du fournisseur et ses services, procédez comme suit : 1. Pour télécharger le `provider_edc.yaml` fichier depuis le `edc_helm_configs` répertoire vers le dossier du graphique Helm actuel, exécutez la commande suivante : `wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/provider_edc.yaml> -P charts/tractusx-connector/` 2. Remplacez les variables suivantes (également marquées dans le fichier) par leurs valeurs : • `CLIENT_ID` – L'identifiant généré par le DAPS. `CLIENT_ID` Il doit se trouver `/srv/mvds/omejdn-daps/config/clients.yml/config/clients.yml` sur le serveur DAPS. Il doit s'agir d'une	DevOps ingénieur

Tâche	Description	Compétences requises
	chaîne de caractères hexadécimaux. • `DAPS_URL`– URL du serveur DAPS. Il doit `https://{DNS name}` utiliser le nom DNS que vous avez défini lorsque vous avez exécuté le AWS CloudFormation modèle. • `VAULT_TOKEN` – Le jeton à utiliser pour l'autorisation du coffre-fort. Choisissez n'importe quelle valeur. • `vault.fullnameOverride` – `vault-provider` . • `vault.hashicorp.url` – `http://vault-provider:8200/` . Les valeurs précédentes supposent que le nom du déploiement et le nom de l'espace de noms sont le fournisseur. 3. Pour exécuter le graphique Helm depuis votre poste de travail, utilisez les commandes suivantes : `cd charts/tractusx-connector`	

Tâche	Description	Compétences requises

	`helm dependency build`
	
	`helm upgrade --install provider ./ -f provider_edc.yaml -n provider`	

Tâche	Description	Compétences requises

Ajoutez le certificat et les clés dans le coffre du fournisseur.	Pour éviter toute confusion, produisez les certificats suivants en dehors du `tractusx-edc/charts` répertoire.
	
	Par exemple, exécutez la commande suivante pour accéder à votre répertoire de base :
	
	`cd ~`
	
	Vous devez maintenant ajouter les secrets dont le fournisseur a besoin dans le coffre.
	
	Les noms des secrets contenus dans le coffre sont les valeurs des clés figurant dans la `secretNames:` section du `provider_edc.yml` fichier. Par défaut, ils sont configurés comme suit :
	
	`secretNames:`
	`transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key`
	`transferProxyTokenSignerPublicKey: transfer-`
		DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>proxy-token-signer-public-key
	transferProxyTokenEncryptionAesKey: transfer-proxy-token-encryption-aes-key
	dapsPrivateKey: daps-private-key
	dapsPublicKey: daps-public-key</pre>
	Une clé AES (Advanced Encryption Standard), une clé privée, une clé publique et un certificat autosigné sont initialement générés. Ils sont ensuite ajoutés en tant que secrets au coffre.
	
	De plus, ce répertoire doit contenir les `daps-provider.key` fichiers `daps-provider.cert` et que vous avez copiés depuis le serveur DAPS.
	
	1. Exécutez les commandes suivantes :
	
	<pre># generate a private key
	openssl ecparam -name prime256v1 -genkey -noout -out provider-private-key.pem
	# generate corresponding public key</pre>	

Tâche	Description	Compétences requises

	`openssl ec -in provider-private-key.pem -pubout -out provider-public-key.pem`
	`# create a self-signed certificate`
	`openssl req -new -x509 -key provider-private-key.pem -out provider-cert.pem -days 360`
	`# generate aes key`
	`openssl rand -base64 32 > provider-aes.key`
	2. Avant d'ajouter les secrets au coffre, convertissez-les de plusieurs lignes en lignes simples en remplaçant les sauts de ligne par \n :
	`cat provider-private-key.pem | sed 's/$/\\\n/'|tr -d '\n' > provider-private-key.pem.line`
	`cat provider-public-key.pem | sed 's/$/\\\n/'|tr -d '\n' > provider-public-key.pem.line`
	`cat provider-cert.pem | sed 's/$/\\\n/'|tr -d '\n' > provider-cert.pem.line`
	`cat provider-aes.key | sed 's/$/\\\n/'|tr -d '\n' > provider-aes.key.line`	

Tâche	Description	Compétences requises
	n/'|tr -d '\\n' > provider-aes.key.line ## The following block is for daps certificate and key openssl x509 -in daps-provider.cert -outform PEM | sed 's/$/\\\\n/'\|tr -d '\\n' > daps-provider.cert.line cat daps-provider.key \| sed 's/$/\\\\n/'|tr -d '\\n' > daps-provider.key.line	
	3. Pour formater les secrets qui seront ajoutés à Vault, exécutez les commandes suivantes : JSONFORMAT='{"content": "%s"}' #create a single line in JSON format printf "${JSONFORMAT}\\n" "`cat provider-private-key.pem.line`" > provider-private-key.json printf "${JSONFORMAT}\\n" "`cat provider-public-key.pem.line`" > provider-public-key.json printf "${JSONFORMAT}\\n" "`cat	

Tâche	Description	Compétences requises
	provider-cert.pem.line`" > provider-cert.json printf "${JSONFORMAT}\\n" "`cat provider-aes.key.line`" > provider-aes.json  printf "${JSONFORMAT}\\n" "`cat daps-provider.key.line`" > daps-provider.key.json printf "${JSONFORMAT}\\n" "`cat daps-provider.cert.line`" > daps-provider.cert.json  Les secrets sont désormais au format JSON et sont prêts à être ajoutés au coffre. 4. Pour obtenir le nom du module pour le coffre, exécutez la commande suivante : `kubectl get pods -n provider|egrep "vault|NAME"`  Le nom du module sera similaire à`"vault-provider-0"` . Ce nom est utilisé lors de la création d'un port de redirection vers	

Tâche	Description	Compétences requises
	le coffre. Le port forward vous permet d'accéder au coffre pour y ajouter le secret. Vous devez l'exécuter à partir d'un poste de travail sur lequel les informations d'identification AWS sont configurées. 5. Pour accéder au coffre-fort, utilisez `kubectl` pour configurer un port de redirection : `kubectl port-forward <VAULT_POD_NAME> 8200:8200 -n provider` Vous devriez maintenant être en mesure d'accéder au coffre par le biais de votre navigateur ou de la CLI. Navigateur 1. À l'aide du navigateur, accédez à http://127.0.0.1:8200, qui utilisera le port de redirection que vous avez configuré. 2. Connectez-vous à l'aide du jeton que vous avez configuré précédemm entprovider_edc.yml . Dans le moteur de secrets, créez trois secrets. Chaque	

Tâche	Description	Compétences requises
	secret aura une `Path for this secret` valeur, qui est le nom du secret indiqué dans la liste suivante. Dans la `secret data` section, le nom de la clé sera `content` et la valeur sera la seule ligne de texte du fichier correspondant nommé `.line`. 3. Les noms secrets proviennent de la `secretNames` section du `provider_edc.yml` fichier. 4. Créez les secrets suivants : • Secret `transfer-proxy-token-signer-private-key` avec nom de fichier `provider-private-key.pem.line` • Secret `transfer-proxy-token-signer-public-key` avec nom de fichier `provider-cert.pem.line` • Secret `transfer-proxy-token-encryption-aes-key` avec nom de fichier `provider-aes.key.line`	

Tâche	Description	Compétences requises
	• Secret `daps-private-key` avec nom de fichier `daps-provider.key.line` • Secret `daps-public-key` avec nom de fichier `daps-provider.cert.line` CLI Vault La CLI utilisera également le port forward que vous avez configuré. 1. Sur votre poste de travail, installez la CLI Vault en suivant les instructions de la documentation de HashiCorp Vault. 2. Pour vous connecter au coffre-fort à l'aide du jeton que vous avez configuré `provider_edc.yml` , exécutez la commande suivante : `vault login -address=http://127.0.0.1:8200` Avec le bon jeton, vous devriez voir le message `"Success! You are now authenticated."`	

Tâche	Description	Compétences requises

	3. Pour créer les secrets à l'aide des fichiers au format JSON que vous avez créés précédemment, exécutez le code suivant :
	
	`vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-signer-private-key @provider-private-key.json`
	`vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-signer-public-key @provider-cert.json`
	`vault kv put -address=http://127.0.0.1:8200 secret/transfer-proxy-token-encryption-aes-key @provider-aes.json`
	
	`vault kv put -address=http://127.0.0.1:8200 secret/daps-private-key @daps-provider.key.json`
	`vault kv put -address=http://127.0.0.1:8200 secret/daps-public-key @daps-provider.cert.json`	

Tâche	Description	Compétences requises

Configurez et déployez le connecteur grand public et ses services.	Les étapes de configuration et de déploiement du client sont similaires à celles que vous avez effectuées pour le fournisseur :
	
	1. Pour copier le `consumer_edc.yaml` depuis le aws-patterns-edcdépôt dans le dossier `tractusx-edc/charts/tractusx-connecto r`, exécutez les commandes suivantes :
	
	`cd tractusx-edc`
	
	`wget -q https://raw.githubusercontent.com/Think-iT-Labs/aws-patterns-edc/main/edc_helm_configs/consumer_edc.yaml -P charts/tractusx-connector/`
	
	2. Mettez à jour les variables suivantes avec leurs valeurs réelles :
	• `CONSUMER_CLIENT_ID` – L'identifiant généré par le DAPS. `CONSUMER_CLIENT_ID` Il doit se trouver `config/clients.yml` sur le serveur DAPS.	

Tâche	Description	Compétences requises

	• `DAPS_URL`– La même URL DAPS que celle que vous avez utilisée pour le fournisseur.
	• `VAULT_TOKEN` – Le jeton à utiliser pour l'autorisation du coffre-fort. Choisissez n'importe quelle valeur.
	• `vault.fullnameOverride` – `vault-consumer`
	• `vault.hashicorp.url` – `http://vault-provider:8200/`
	
	Les valeurs précédentes supposent que le nom du déploiement et le nom de l'espace de noms sont`consumer`.
	3. Pour exécuter le graphique Helm, utilisez les commandes suivantes :
	
	`cd charts/tractusx-connector`
	
	`helm upgrade --install consumer ./ -f consumer_edc.yaml -n consumer`	

Tâche	Description	Compétences requises

Ajoutez le certificat et les clés dans le coffre du consommateur.	Du point de vue de la sécurité, nous recommandons de régénérer les certificats et les clés pour chaque participant à l'espace de données. Ce modèle régénère les certificats et les clés pour le consommateur.
	
	Les étapes sont très similaires à celles du fournisseur. Vous pouvez vérifier les noms secrets contenus dans le `consumer_edc.yml` fichier.
	
	Les noms des secrets contenus dans le coffre sont les valeurs des clés figurant dans la `secretNames:` section du`consumer_edc.yml file` . Par défaut, ils sont configurés comme suit :
	
	`secretNames:`
	`transferProxyTokenSignerPrivateKey: transfer-proxy-token-signer-private-key`
	`transferProxyTokenSignerPublicKey: transfer-proxy-token-signer-public-key`
	`transferProxyTokenEncryptio`
		DevOps ingénieur

Tâche	Description	Compétences requises

	`nAesKey: transfer-proxy-token-encryption-aes-key`
	`dapsPrivateKey: daps-private-key`
	`dapsPublicKey: daps-public-key`	

	Les `daps-consumer.key` fichiers `daps-consumer.cert` et que vous avez copiés depuis le serveur DAPS devraient déjà exister dans ce répertoire.	

	1. Exécutez les commandes suivantes :
	`# generate a private key`
	`openssl ecparam -name prime256v1 -genkey -noout -out consumer-private-key.pem`
	`# generate corresponding public key`
	`openssl ec -in consumer-private-key.pem -pubout -out consumer-public-key.pem`
	`# create a self-signed certificate`
	`openssl req -new -x509 -key consumer-private-key.pem -out consumer-cert.pem -days 360`
	`# generate aes key`	

Tâche	Description	Compétences requises
	`openssl rand -base64 32 > consumer-aes.key`	

	2. Modifiez les fichiers manuellement pour remplacer les sauts de ligne par\n, ou utilisez trois commandes similaires aux suivantes :
	`cat consumer-private-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-private-key.pem.line`
	`cat consumer-public-key.pem | sed 's/$/\\\n/'|tr -d '\\n' > consumer-public-key.pem.line`
	`cat consumer-cert.pem | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-cert.pem.line`
	`cat consumer-aes.key | sed 's/$/\\\\n/'|tr -d '\\n' > consumer-aes.key.line`
	`cat daps-consumer.cert | sed 's/$/\\\\n/'|tr -d '\\n' > daps-consumer.cert.line`
	`cat daps-consumer.key | sed 's/$/\\\\n/'| tr -d '\\n' > daps-consumer.key.line`	

Tâche	Description	Compétences requises

	3. Pour formater les secrets qui seront ajoutés à Vault, exécutez les commandes suivantes :
	
	`JSONFORMAT='{"content": "%s"}'`
	
	`#create a single line in JSON format`
	
	`printf "${JSONFORMAT}\\n" "`cat consumer-private-key.pem.line`" > consumer-private-key.json`
	`printf "${JSONFORMAT}\\n" "`cat consumer-public-key.pem.line`" > consumer-public-key.json`
	`printf "${JSONFORMAT}\\n" "`cat consumer-cert.pem.line`" > consumer-cert.json`
	`printf "${JSONFORMAT}\\n" "`cat consumer-aes.key.line`" > consumer-aes.json`
	
	`printf "${JSONFORMAT}\\n" "`cat daps-consumer.key.line`" > daps-consumer.key.json`
	`printf "${JSONFORMAT}\\n" "`cat daps-`	

Tâche	Description	Compétences requises
	`consumer.cert.line`" > daps-consumer.cert.json`  Les secrets sont désormais au format JSON et sont prêts à être ajoutés au coffre.  4. Pour obtenir le nom du module pour le coffre du consommateur, exécutez la commande suivante :  `kubectl get pods -n consumer | egrep "vault|NAME"`  Le nom du module sera similaire à `"vault-consumer-0"` . Ce nom est utilisé lors de la création d'un port de redirection vers le coffre. Le port forward vous permet d'accéder au coffre pour y ajouter le secret. Vous devez l'exécuter à partir d'un poste de travail dont les AWS informations d'identification sont configurées. 5. Pour accéder au coffre-fort, utilisez `kubectl` pour configurer un port de redirection :	

Tâche	Description	Compétences requises
	`kubectl port-forward <VAULT_POD_NAME> 8201:8200 -n consumer` Le port local est cette fois le 8201, ce qui vous permet de mettre en place des redirecti ons pour le producteur et le consommateur. Navigateur Vous pouvez utiliser votre navigateur pour vous connecter à http://localhost:8201/ afin d'accéder au coffre du consommateur et de créer les secrets avec les noms et le contenu tels que décrits. Les secrets et les fichiers contenant le contenu sont les suivants : • Secret `transfer-proxy-token-signer-private-key` avec nom de fichier `consumer-private-key.pem.line` • Secret `transfer-proxy-token-signer-public-key` avec	

Tâche	Description	Compétences requises
	nom de fichier `consumer-cert.pem.line` • Secret `transfer-proxy-token-encryption-aes-key` avec nom de fichier `consumer-aes.key.line` CLI Vault À l'aide de la CLI de Vault, vous pouvez exécuter les commandes suivantes pour vous connecter au coffre-fort et créer les secrets : 1. Connectez-vous au coffre-fort en utilisant le jeton que vous avez configuré dans `consumer_edc.yml` : ``` vault login -address=http://127.0.0.1:8201 ``` Avec le bon jeton, vous devriez voir le message `"Success! You are now authenticated."` 2. Pour créer les secrets à l'aide des fichiers au format JSON que vous avez créés précédemment, exécutez le code suivant :	

Tâche	Description	Compétences requises

	`vault kv put -address= http://127.0.0.1:8 201 secret/transfer- proxy-token-signer-p rivate-key @consumer -private-key.json`
	`vault kv put - address=http://12 7.0.0.1:8201 secret/ transfer-proxy-token -signer-public-key @consumer-cert.json`
	`vault kv put -address= http://127.0.0.1:8 201 secret/transfer- proxy-token-encrypti on-aes-key @consumer -aes.json`
	`vault kv put -address= http://127.0.0.1:8 201 secret/daps- private-key @daps-con sumer.key.json`
	`vault kv put - address=http://12 7.0.0.1:8201 secret/ daps-public-key @daps-consumer.cer t.json`	

Configurer un client HTTP pour interagir avec l'API de gestion des connecteurs

Tâche	Description	Compétences requises
Configurez la redirection de port.	1. Pour vérifier l'état des pods, exécutez les commandes suivantes :	DevOps ingénieur

Tâche	Description	Compétences requises

	`kubectl get pods -n provider`
	`kubectl get pods -n consumer`
	2. Pour vous assurer que les déploiements de Kubernetes ont réussi, consultez les journaux des pods Kubernetes du fournisseur et du consommateur en exécutant les commandes suivantes :
	`kubectl logs -n provider <producer control plane pod name>`
	`kubectl logs -n consumer <consumer control plane pod name>`
	Le cluster est privé et n'est pas accessible au public. Pour interagir avec les connecteurs, utilisez la fonction de transfert de port Kubernetes pour transférer le trafic généré par votre machine vers le plan de contrôle des connecteurs.
	1. Sur le premier terminal, transmettez les demandes du consommateur à l'API de gestion via le port 8300 :	

Tâche	Description	Compétences requises

	`kubectl port-forward deployment/consumer-tractusx-connector-controlplane 8300:8081 -n consumer`
	2. Sur le deuxième terminal, transmettez les demandes du fournisseur à l'API de gestion via le port 8400 :
	`kubectl port-forward deployment/provider-tractusx-connector-controlplane 8400:8081 -n provider`	

Tâche	Description	Compétences requises
Créez des compartiments S3 pour le fournisseur et le consommateur.	Le connecteur EDC n'utilise actuellement pas d'informations d'identification AWS temporaires, telles que celles fournies en assumant un rôle. L'EDC ne prend en charge que l'utilisation d'une combinaison de clé d'accès IAM et de clé d'accès secrète. Deux compartiments S3 sont nécessaires pour les étapes ultérieures. Un compartiment S3 est utilisé pour stocker les données mises à disposition par le fournisseur. L'autre compartiment S3 est destiné aux données reçues par le consommateur. L'utilisateur IAM doit être autorisé à lire et à écrire des objets uniquement dans les deux compartiments nommés. Une paire d'identifiant de clé d'accès et de clé d'accès secrète doit être créée et conservée en toute sécurité. Après la mise hors service de ce MVDS, l'utilisateur IAM doit être supprimé. Le code suivant est un exemple de politique IAM pour l'utilisateur :	DevOps ingénieur

Tâche	Description	Compétences requises

	{
	  "Version": "2012-10-17",
	  "Statement": [
	  {
	  "Sid": "Stmt1708699805237",
	  "Action": [
	  "s3:GetObject",
	  "s3:GetObjectVersion",
	  "s3:ListAllMyBuckets",
	  "s3:ListBucket",
	  "s3:ListBucketMultipartUploads",
	  "s3:ListBucketVersions",
	  "s3:PutObject"
	  ],
	  "Effect": "Allow",
	  "Resource": [
	  "arn:aws:s3:::<S3 Provider Bucket>",
	  "arn:aws:s3:::<S3 Consumer Bucket>",
	  "arn:aws:s3:::<S3 Provider Bucket>/*",
	  "arn:aws:s3:::<S3 Consumer Bucket>/*"
	  ] }
	  ]
	}	

Tâche	Description	Compétences requises
Configurez Postman pour qu'il interagisse avec le connecteur.	Vous pouvez désormais interagir avec les connecteurs via votre EC2 instance. Utilisez Postman comme client HTTP et fournissez des collections Postman pour les connecteurs fournisseur et consommateur. Importez les collections du `aws-pattern-edc` référentiel dans votre instance Postman. Ce modèle utilise les variables de collection Postman pour fournir des informations à vos demandes.	Développeur d'applications, ingénieur de données

Fournissez les données d'empreinte carbone de l'entreprise X via le connecteur

Tâche	Description	Compétences requises
Préparez les données d'intensité des émissions de carbone à partager.	Vous devez d'abord choisir la ressource de données à partager. Les données de l'entreprise X représentent l'empreinte carbone de son parc de véhicules. Le poids est le poids brut du véhicule (PTC) en tonnes, et les émissions sont exprimées en grammes CO2 par tonne-kilomètre (g CO2 e/t-km) selon	Ingénieur de données, développeur d'applications

Tâche	Description	Compétences requises
	la Wheel-to-Well mesure (WTW) : • Type de véhicule : fourgonnette ; poids : < 3,5 ; émissions : 800 • Type de véhicule : camion urbain ; poids : 3,5 à 7,5 ; émissions : 315 • Type de véhicule : véhicule utilitaire moyen (MGV) ; poids : 7,5 à 20 ; émissions : 195 • Type de véhicule : poids lourd (poids lourd) ; poids : > 20 ; émissions : 115 Les données d'exemple se trouvent dans le `carbon_emissions_data.json` fichier du `aws-patterns-edc` référentiel. L'entreprise X utilise Amazon S3 pour stocker des objets. Créez le compartiment S3 et stockez-y l'exemple d'objet de données. Les commandes suivantes créent un compartiment S3 avec des paramètres de sécurité par défaut. Nous vous recommandons vivement de consulter les meilleures	

Tâche	Description	Compétences requises

	pratiques de sécurité pour Amazon S3.
	
	`aws s3api create-bucket <BUCKET_NAME> --region <AWS_REGION>`
	`# You need to add '--create-bucket-configuration # LocationConstraint=<AWS_REGION>' if you want to create # the bucket outside of us-east-1 region`
	
	`aws s3api put-object --bucket <BUCKET_NAME> \ --key <S3 OBJECT NAME> \ --body <PATH OF THE FILE TO UPLOAD>`
	
	Le nom du compartiment S3 doit être unique au monde. Pour plus d'informations sur les règles de dénomination, consultez la documentation AWS.	

Tâche	Description	Compétences requises
Enregistrez la ressource de données sur le connecteur du fournisseur à l'aide de Postman.	Une ressource de données du connecteur EDC contient le nom des données et leur emplacement. Dans ce cas, la ressource de données du connecteur EDC pointera vers l'objet créé dans le compartiment S3 : • Connecteur : Provider • Demande : créer un actif • Variables de collection : mise à jour`ASSET_NAME` . Choisissez un nom significatif qui représente l'actif. • Corps de la demande : mettez à jour le corps de la demande avec le compartiment S3 que vous avez créé pour le fournisseur. `"dataAddress": { "edc:type": "AmazonS3", "name": "Vehicle Carbon Footprint", "bucketName": "<REPLACE WITH THE SOURCE BUCKET NAME>", "keyName": "<REPLACE WITH YOUR OBJECT NAME>", "region": "<REPLACE WITH THE BUCKET REGION>",`	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises
	<pre>"accessKeyId": "<REPLACE WITH YOUR ACCESS KEY ID>", "secretAccessKey": "<REPLACE WITH SECRET ACCESS KEY>" }</pre> • Réponse : Une demande réussie renvoie l'heure de création et l'ID de l'actif nouvellement créé. <pre>{ "@id": "c89aa31c-ec4c-44ed-9e8c-1647f19d7583" }</pre> • Variable de collection ASSET_ID : mettez à jour la variable de collection Postman `ASSET_ID` avec l'ID généré automatiquement par le connecteur EDC après sa création.	

Tâche	Description	Compétences requises

Définissez la politique d'utilisation de l'actif.	Un actif de données EDC doit être associé à des politiques d'utilisation claires. Créez d'abord la définition de la politique dans le connecteur du fournisseur.
	
	La politique de l'entreprise X est de permettre aux participants de l'espace de données d'utiliser les données d'empreinte carbone.
	
	• Organisme de la demande :
	  • Connecteur : Provider
	  • Demande : créer une politique
	  • Variables de collection : mettez à jour la `Policy Name` variable avec le nom de la politique.
	• Réponse : Une demande réussie renvoie l'heure de création et l'ID de politique de la nouvelle politique. Mettez à jour la variable de collection `POLICY_ID` avec l'ID de la politique générée par le connecteur EDC après sa création.
		Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises
Définissez une offre de contrat EDC pour l'actif et sa politique d'utilisation.	Pour permettre aux autres participants de demander l'accès à vos données, proposez-les dans le cadre d'un contrat qui précise les conditions d'utilisation et les autorisations : • Connecteur : Provider • Demande : Création d'une définition de contrat • Variables de collection : mettez à jour la `Contract Name` variable avec un nom pour l'offre ou la définition du contrat.	Développeur d'applications, ingénieur de données

Découvrez les actifs et parvenez à un accord sur les contrats définis

Tâche	Description	Compétences requises
Demandez le catalogue de données partagé par l'entreprise X.	En tant que consommateur de données dans le domaine des données, l'entreprise Y doit d'abord découvrir les données partagées par les autres participants. Dans cette configuration de base, vous pouvez le faire en demandant au connecteur consommateur de demander le catalogue des actifs	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises

	disponibles directement au connecteur fournisseur.
	• Connecteur : Consumer
	• Demande : Demande de catalogue
	• Réponse : Toutes les ressources de données disponibles auprès du fournisseur, ainsi que leurs politiques d'utilisation associées. En tant que consommateur de données, recherchez le contrat qui vous intéresse et mettez à jour les variables de collecte suivantes en conséquence.
	  • `CONTRACT_OFFER_ID` – L'identifiant de l'offre contractuelle que le consommateur souhaite négocier
	  • `ASSET_ID`– L'identifiant de l'actif que le consommateur souhaite négocier
	  • `PROVIDER_CLIENT_ID` – L'ID du connecteur du fournisseur avec lequel négocier	

Tâche	Description	Compétences requises
Lancer une négociation contractuelle pour les données sur l'intensité des émissions de carbone de l'entreprise X.	Maintenant que vous avez identifié l'actif que vous souhaitez consommer, lancez un processus de négociation de contrat entre les connecteurs consommateur et fournisseur. • Connecteur : Consumer • Demande : Négociation de contrat • Variables de collection : mettez à jour la `CONSUMER_CLIENT_ID` variable avec l'ID du connecteur consommateur avec lequel négocier. Le processus peut prendre un certain temps avant d'atteindre l'état VÉRIFIÉ. Vous pouvez vérifier l'état de la négociation du contrat et l'ID de contrat correspondant en utilisant la `Get Negotiation` demande.	Développeur d'applications, ingénieur de données

Consommez les données en utilisant le contrat

Tâche	Description	Compétences requises
Consommez les données des points de terminaison HTTP.	(Option 1) Pour utiliser le plan de données HTTP afin de	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises
	consommer les données de l'espace de données, vous pouvez utiliser webhook.site pour émuler un serveur HTTP et lancer le processus de transfert dans le connecteur consommateur : • Connecteur : Consumer • Demande : Négociation de contrat • Variables de collection : mettez à jour la `Contract Agreement ID` variable avec l'ID de l'accord contractuel généré par le connecteur EDC. • Corps de la demande : mettez à jour le corps de la demande pour HTTP le spécifier à `dataDestination` côté de l'URL du webhook : `{ "dataDestination": { "type": "HttpProxy" }, "privateProperties": { "receiverHttpEndpoint": "<WEBHOOK URL>" }`	

Tâche	Description	Compétences requises

	<pre>}</pre>
	Le connecteur enverra les informations nécessaires pour télécharger le fichier directement sur l'URL du webhook.
	
	La charge utile reçue est similaire à ce qui suit :
	
	<pre>{
	  "id": "dcc90391
	-3819-4b54-b401-1a
	005a029b78",
	  "endpoint":
	 "http://consumer-t
	ractusx-connector-
	dataplane.consumer
	:8081/api/public",
	  "authKey":
	 "Authorization",
	  "authCode": "<AUTH
	 CODE YOU RECEIVE IN
	 THE ENDPOINT>",
	  "properties": {
	  "https://
	w3id.org/edc/v0.0.
	1/ns/cid": "vehicle-
	carbon-footprint-c
	ontract:4563abf7-5
	dc7-4c28-bc3d-97f4
	5e32edac:b073669b-
	db20-4c83-82df-46b
	583c4c062"
	  }
	}</pre>	

Tâche	Description	Compétences requises
	Utilisez les informations d'identification reçues pour obtenir la ressource S3 partagée par le fournisseur. Dans cette dernière étape, vous devez envoyer la demande au plan de données du consommateur (ports de transfert correctement), comme indiqué dans la charge utile (`endpoint`).	

Tâche	Description	Compétences requises
Consommez directement les données des compartiments S3.	(Option 2) Utilisez l'intégration Amazon S3 avec le connecteur EDC et pointez directement vers le compartiment S3 de l'infrastructure grand public comme destination : • Corps de la demande : mettez à jour le corps de la demande pour spécifier le compartiment S3 en tant que DataDestination. Il doit s'agir du compartiment S3 que vous avez créé précédemment pour stocker les données reçues par le consommateur. `{ "dataDestination": { "type": "AmazonS3", "bucketName": "{{ REPLACE WITH THE DESTINATION BUCKET NAME }}", "keyName": "{{ REPLACE WITH YOUR OBJECT NAME }}", "region": "{{ REPLACE WITH THE BUCKET REGION }}", "accessKeyId": "{{ REPLACE WITH YOUR ACCESS KEY ID }}",`	Ingénieur de données, développeur d'applications

Tâche	Description	Compétences requises

	<pre>"secretAc
	cessKey": "{{ REPLACE
	 WITH SECRET ACCESS
	 KEY }}"
	}
	 }
	}</pre>	

Résolution des problèmes

Problème	Solution
Le connecteur peut soulever un problème concernant le format PEM du certificat.	Concaténez le contenu de chaque fichier sur une seule ligne en ajoutant. \n

Ressources connexes

- DSSC
- Création d'espaces de données pour les cas d'utilisation liés au développement durable (stratégie AWS Prescriptive Guidance de Think-it)
- AWS pour les espaces de données
- Documentation sur Tractus-X
- DAPS
- Permettre le partage de données via les espaces de données et AWS (article de blog)

Informations supplémentaires

Spécifications de l'espace de données

Les participants

Participant	Description de l'entreprise	Objectif de l'entreprise

Entreprise X	Exploite une flotte de véhicules en Europe et en Amérique du Sud pour transporter diverses marchandises.	Vise à prendre des décisions basées sur les données afin de réduire l'intensité de son empreinte carbone.
Entreprise Y	Une autorité de régulation environnementale	Applique les réglement ations et politiques environne mentales conçues pour surveiller et atténuer l'impact environnemental des entrepris es et des industries, y compris l'intensité des émissions de carbone.

Affaire de cas

L'entreprise X utilise la technologie de l'espace de données pour partager les données d'empreinte carbone avec un auditeur de conformité, la société Y, afin d'évaluer et de prendre en compte l'impact environnemental des opérations logistiques de l'entreprise X.

Autorité de l'espace de données

L'autorité de l'espace de données est un consortium des organisations qui régissent l'espace de données. Dans ce modèle, les entreprises X et Y forment l'organe de gouvernance et représentent une autorité fédérée en matière d'espace de données.

Composants de l'espace de données

Composant	Implémentation choisie	Informations supplémentaires
Protocole d'échange de données	Protocole Dataspace version 0.8	• JSON-LD • Vocabulaire du catalogue de données (DCAT)
Connecteur d'espace de données	Connecteur Tractus-X EDC version 0.4.1	• Extensions EDC

Politiques d'échange de données	Politique d'utilisation par défaut	• Langage ouvert des droits numériques (ODRL)

Services d'espace de données

Service	Mise en œuvre	Informations supplémentaires
Service d'identité	Système de provisionnement dynamique des attributs (DAPS)	« Un système de provision nement dynamique des attributs (DAPS) a pour but de vérifier certains attributs des organisations et des connecteurs. Les tiers n'ont donc pas besoin de faire confiance à ces derniers à condition qu'ils fassent confiance aux assertions du DAPS. » — ROBINETS Pour se concentrer sur la logique du connecteur, l'espace de données est déployé sur une EC2 machine Amazon à l'aide de Docker Compose.
Le service de découverte	Catalogue fédéré Gaia-X	« Le catalogue fédéré constitue un référentiel indexé des auto-descriptions de Gaia-X afin de permettre la découverte et la sélection des fournisseurs et de leurs offres de services. Les auto-descriptions sont les informati ons fournies par les participa nts sur eux-mêmes et sur

		leurs services sous forme de propriétés et de réclamations. » — Kickstarter de l'écosystème Gaia-X

Données à échanger

Ressources de données	Description	Format
Données sur les émissions de carbone	Valeurs d'intensité pour différents types de véhicules dans la région spécifiée (Europe et Amérique du Sud) pour l'ensemble du parc de véhicules	Fichier JSON

Modèle de données

```
{
  "region": "string",
  "vehicles": [
// Each vehicle type has its Gross Vehicle Weight (GVW) category and its emission
 intensity in grams of CO2 per Tonne-Kilometer (g CO2 e/t-km) according to the "Well-
to-Wheel" (WTW) measurement.
    {
      "type": "string",
      "gross_vehicle_weight": "string",
      "emission_intensity": {
        "CO2": "number",
        "unit": "string"
      }
    }
  ]
}
```

Connecteur Tractus-X EDC

Pour la documentation de chaque paramètre EDC de Tractus-X, consultez le fichier de valeurs d'origine.

Le tableau suivant répertorie tous les services, ainsi que leurs ports exposés et points de terminaison correspondants à titre de référence.

Nom du service	Port et chemin
Plan de contrôle	• Gestion : – Port : 8081 Chemin : `/management` • contrôle – Port : 8083 Trajet : `/control` • Port du protocole : 8084 Chemin : `/api/v1/dsp` • métriques – Port : 9090 Trajet : `/metrics` • observabilité – Port : 8085 Trajet : `/observability`
Plan de données	par défaut – Port : 8080 Chemin : `/api` public – Port : 8081 Trajet : `/api/dataplane/control` proxy – Port : 8186 Chemin : `/proxy` métriques – Port : 9090 Trajet : `/metrics` observabilité – Port : 8085 Trajet : `/observability`
Coffre-fort	Hafen : 8200
PostgreSQL	Hafen : 5432

Utilisation AWS Secrets Manager du gestionnaire

Il est possible d'utiliser Secrets Manager au lieu de HashiCorp Vault comme gestionnaire de secrets. Pour ce faire, vous devez utiliser ou créer l'extension AWS Secrets Manager EDC.

Vous serez responsable de la création et de la maintenance de votre propre image, car Tractus-X ne fournit pas de support pour Secrets Manager.

Pour ce faire, vous devez modifier les fichiers Gradle de génération du plan de contrôle et du plan de données du connecteur en introduisant votre extension AWS Secrets Manager EDC (voir cet artefact maven par exemple), puis créer, maintenir et référencer l'image Docker.

Pour plus d'informations sur la refactorisation de l'image Docker du connecteur Tractus-X, consultez les diagrammes Refactor Tractus-X EDC Helm.

Pour des raisons de simplicité, nous évitons de reconstruire l'image du connecteur selon ce modèle et utilisons HashiCorp Vault.

Configurer un tri spécifique à la langue pour les résultats des requêtes Amazon Redshift à l'aide d'un UDF Python scalaire

Créée par Ethan Stark (AWS)

Récapitulatif

Ce modèle fournit des étapes et un exemple de code pour utiliser une UDF (fonction définie par l'utilisateur) Python scalaire afin de configurer un tri linguistique insensible aux majuscules et minuscules pour les résultats des requêtes Amazon Redshift. Il est nécessaire d'utiliser un UDF Python scalaire car Amazon Redshift renvoie des résultats basés sur l'ordre binaire UTF-8 et ne prend pas en charge le tri spécifique à une langue. Un UDF Python est un code de traitement non SQL basé sur un programme Python 2.7 et exécuté dans un entrepôt de données. Vous pouvez exécuter du code UDF Python avec une instruction SQL dans une seule requête. Pour plus d'informations, consultez le billet de blog consacré à l'introduction à Python UDFs dans Amazon Redshift AWS Big Data.

Les données d'échantillon de ce modèle sont basées sur l'alphabet turc à des fins de démonstration. Le scalaire Python UDF utilisé dans ce modèle est conçu pour que les résultats de requête par défaut d'Amazon Redshift soient conformes à l'ordre linguistique des caractères en turc. Pour plus d'informations, voir l'exemple de langue turque dans la section Informations supplémentaires de ce modèle. Vous pouvez modifier l'UDF Python scalaire dans ce modèle pour d'autres langages.

Conditions préalables et limitations

Prérequis

- Cluster Amazon Redshift avec base de données, schéma et tables
- Utilisateur Amazon Redshift avec autorisations CREATE TABLE et CREATE FUNCTION
- Python 2.7 ou version ultérieure

Limites

Le tri linguistique utilisé par les requêtes dans ce modèle ne fait pas la distinction majuscules/minuscules.

Architecture

Pile technologique

- Amazon Redshift
- UDF en Python

Outils

Services AWS

- Amazon Redshift est un service d'entrepôt de données géré à l'échelle du pétaoctet dans le cloud AWS. Amazon Redshift est intégré à votre lac de données, ce qui vous permet d'utiliser vos données pour acquérir de nouvelles informations pour votre entreprise et vos clients.

Autres outils

- Les fonctions définies par l'utilisateur Python (UDFs) sont des fonctions que vous pouvez écrire en Python puis appeler dans des instructions SQL.

Épopées

Développez du code pour trier les résultats des requêtes par ordre linguistique

Tâche	Description	Compétences requises

Créez un tableau pour vos exemples de données.	Pour créer une table dans Amazon Redshift et y insérer vos exemples de données, utilisez les instructions SQL suivantes :
	`CREATE TABLE my_table (first_name varchar(30));`
	`INSERT INTO my_table (first_name)`
		Ingénieur de données

Tâche	Description	Compétences requises

```
VALUES
    ('ali'),
    ('Ali'),
    ('ırmak'),
    ('IRMAK'),
    ('irem'),
    ('İREM'),
    ('oğuz'),
    ('OĞUZ'),
    ('ömer'),
    ('ÖMER'),
    ('sedat'),
    ('SEDAT'),
    ('şule'),
```

> **Note**
>
> Les prénoms figurant dans les échantillons de données incluent des caractères spéciaux de l'alphabet turc. Pour plus d'informations sur les considérations relatives à la langue turque pour cet exemple, voir l'exemple de langue turque dans la section Informations supplémentaires de ce modèle.

Tâche	Description	Compétences requises

Vérifiez le tri par défaut des échantillons de données.	Pour voir le tri par défaut de vos exemples de données dans Amazon Redshift, exécutez la requête suivante :
	`SELECT first_name FROM my_table ORDER BY first_name;`
	La requête renvoie la liste des prénoms de la table que vous avez créée précédemment :
	`first_name`
	`---------------`
	`Ali`
	`IRMAK`
	`OĞUZ`
	`SEDAT`
	`ali`
	`irem`
	`oğuz`
	`sedat`
	`ÖMER`
	`ömer`
	`İREM`
	`ırmak`
	`ŞULE`
	`şule`
	Les résultats de la requête ne sont pas dans le bon ordre car l'ordre binaire UTF-8 par défaut ne correspond pas à l'ordre linguistique des caractères spéciaux turcs.
		Ingénieur de données

Tâche	Description	Compétences requises
Créez un UDF Python scalaire.	Pour créer un UDF Python scalaire, utilisez le code SQL suivant : `CREATE OR REPLACE FUNCTION collate_sort (value varchar) RETURNS varchar IMMUTABLE AS $$ def sort_str(val): import string dictionary = { 'I': 'ı', 'ı': 'h~', 'İ': 'i', 'Ş': 's~', 'ş': 's~', 'Ğ': 'g~', 'ğ': 'g~', 'Ü': 'u~', 'ü': 'u~', 'Ö': 'o~', 'ö': 'o~', 'Ç': 'c~', 'ç': 'c~' } for key, value in dictionary.items(): val = val.replace(key, value) return val.lower()`	Ingénieur de données

Tâche	Description	Compétences requises

	`    return sort_str( value)`
	
	`$$ LANGUAGE plpythonu;`	

Interrogez les exemples de données.	Pour interroger les exemples de données à l'aide de l'UDF Python, exécutez la requête SQL suivante :
	
	`SELECT first_name FROM my_table ORDER BY collate_order(firs t_name);`
	
	La requête renvoie désormais les exemples de données dans l'ordre linguistique turc :
	
	`first_name`
	`---------------`
	`ali`
	`Ali`
	`ırmak`
	`IRMAK`
	`irem`
	`İREM`
	`oğuz`
	`OĞUZ`
	`ömer`
	`Ömer`
	`sedat`
	`SEDAT`
	`şule`
	`ŞULE`
		Ingénieur de données

Ressources connexes

- Clause ORDER BY (documentation Amazon Redshift)
- Création d'un UDF Python scalaire (documentation Amazon Redshift)

Informations supplémentaires

Exemple de langue turque

Amazon Redshift renvoie les résultats des requêtes sur la base d'un ordre de tri binaire UTF-8, et non d'un ordre de tri spécifique à une langue. Cela signifie que si vous interrogez une table Amazon Redshift contenant des caractères turcs, les résultats de la requête ne sont pas triés selon l'ordre linguistique de la langue turque. La langue turque contient six caractères spéciaux (ç, ı, ğ, ö, ş et ü) qui n'apparaissent pas dans l'alphabet latin. Ces caractères spéciaux sont placés à la fin d'un ensemble de résultats triés en fonction de l'ordre binaire UTF-8, comme le montre le tableau suivant.

Ordre binaire UTF-8	Ordre linguistique turc
a	a
b	b
c	c
d	mois (*)
e	d
f	e
g	f
h	g
i	ğ (*)
j	h
k	Oui (*)

l	i
m	j
n	k
o	l
p	m
r	n
s	o
t	île (*)
u	p
v	r
y	s
z	Oui (*)
mois (*)	t
ğ (*)	u
Oui (*)	ü (*)
île (*)	v
Oui (*)	y
ü (*)	z

> **Note**
>
> L'astérisque (*) indique un caractère spécial dans la langue turque.

Comme l'illustre le tableau ci-dessus, le caractère spécial ç se situe entre c et d dans l'ordre linguistique turc, mais apparaît après z dans l'ordre binaire UTF-8. Dans ce modèle, le scalaire Python UDF utilise le dictionnaire de remplacement de caractères suivant pour remplacer les caractères spéciaux turcs par des caractères équivalents en latin correspondants.

Caractère spécial turc	Caractère équivalent en latin
ç	c~
ı	h~
ğ	g~
ö	o~
ş	s~
ü	u~

> **Note**
>
> Un tilde (~) est ajouté à la fin des caractères latins pour remplacer les caractères spéciaux turcs correspondants.

Modifier une fonction UDF Python scalaire

Pour modifier la fonction UDF scalaire de Python à partir de ce modèle afin qu'elle accepte un paramètre de localisation et prenne en charge un dictionnaire de transactions multiples, utilisez le code SQL suivant :

```
CREATE OR REPLACE FUNCTION collate_sort (value varchar, locale varchar)
RETURNS varchar
IMMUTABLE
AS
$$
    def sort_str(val):
       import string
       # Turkish Dictionary
       if locale == 'tr-TR':
```

```
            dictionary = {
               'I': 'ı',
               'ı': 'h~',
               'İ': 'i',
               'Ş': 's~',
               'ş': 's~',
               'Ğ': 'g~',
               'ğ': 'g~',
               'Ü': 'u~',
               'ü': 'u~',
               'Ö': 'o~',
               'ö': 'o~',
               'Ç': 'c~',
               'ç': 'c~'
        }
        # German Dictionary
        if locale == 'de-DE':
            dictionary = {
               ....
               ....
        }

        for key, value in dictionary.items():
            val = val.replace(key, value)

        return val.lower()

    return sort_str(value)

$$ LANGUAGE plpythonu;
```

L'exemple de code suivant montre comment interroger l'UDF Python modifié :

```
SELECT first_name FROM my_table ORDER BY collate_order(first_name, 'tr-TR');
```

Abonnement d'une fonction Lambda aux notifications d'événements provenant de compartiments S3 dans différentes régions AWS

Créée par Suresh Konathala, Andrew Preston et Arindom Sarkar

Récapitulatif

Les notifications d'événements Amazon Simple Storage Service (Amazon S3) publient des notifications pour certains événements de votre compartiment S3 (par exemple, les événements créés, les événements de suppression d'objets ou les événements de restauration d'objets). Vous pouvez utiliser une fonction AWS Lambda pour traiter ces notifications conformément aux exigences de votre application. Cependant, la fonction Lambda ne peut pas s'abonner directement aux notifications provenant de compartiments S3 hébergés dans différentes régions AWS.

L'approche de ce modèle déploie un scénario de fanout pour traiter les notifications Amazon S3 provenant de compartiments S3 interrégionaux en utilisant une rubrique Amazon Simple Notification Service (Amazon SNS) pour chaque région. Ces rubriques SNS régionales envoient les notifications d'événements Amazon S3 à une file d'attente Amazon Simple Queue Service (Amazon SQS) située dans une région centrale qui contient également votre fonction Lambda. La fonction Lambda s'abonne à cette file d'attente SQS et traite les notifications d'événements conformément aux exigences de votre organisation.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Des compartiments S3 existants dans plusieurs régions, y compris une région centrale pour héberger la file d'attente Amazon SQS et la fonction Lambda.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée. Pour plus d'informations à ce sujet, consultez la section Installation, mise à jour et désinstallation de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS.
- Connaissance du scénario de fanout dans Amazon SNS. Pour plus d'informations à ce sujet, consultez les scénarios Amazon SNS courants dans la documentation Amazon SNS.

Architecture

Le schéma suivant montre l'architecture de l'approche de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Amazon S3 envoie des notifications d'événements concernant les compartiments S3 (par exemple, un objet créé, un objet supprimé ou un objet restauré) à une rubrique SNS de la même région.
2. La rubrique SNS publie l'événement dans une file d'attente SQS de la région centrale.
3. La file d'attente SQS est configurée comme source d'événements pour votre fonction Lambda et met en mémoire tampon les messages d'événement de la fonction Lambda.
4. La fonction Lambda interroge la file d'attente SQS à la recherche de messages et traite les notifications d'événements Amazon S3 conformément aux exigences de votre application.

Pile technologique

- Lambda
- Amazon SNS
- Amazon SQS
- Amazon S3

Outils

- AWS CLI — L'interface de ligne de commande AWS (AWS CLI) est un outil open source permettant d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande. Avec une configuration minimale, vous pouvez exécuter des commandes de l'interface de ligne de commande AWS qui mettent en œuvre des fonctionnalités équivalentes à celles fournies par la console de gestion AWS basée sur un navigateur à partir d'une invite de commande.
- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les

ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.

- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.
- Amazon SQS — Amazon Simple Queue Service (Amazon SQS) propose une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués. Amazon SQS prend en charge les files d'attente standard et FIFO.

Épopées

Créez la file d'attente SQS et la fonction Lambda dans votre région centrale

Tâche	Description	Compétences requises
Créez une file d'attente SQS avec un déclencheur Lambda.	Connectez-vous à l'AWS Management Console et suivez les instructions du didacticiel Using Lambda with Amazon SQS de la documentation AWS Lambda pour créer les ressources suivantes dans votre région centrale : • Un rôle d'exécution Lambda • Une fonction Lambda pour traiter les événements Amazon S3	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
	• Une file d'attente SQS **Note** Assurez-vous de configurer la file d'attente SQS comme source d'événements pour votre fonction Lambda.	

Créez une rubrique SNS et configurez des notifications d'événements pour les compartiments S3 dans chaque région requise

Tâche	Description	Compétences requises
Créez une rubrique SNS pour recevoir des notifications d'événements Amazon S3.	Créez une rubrique SNS dans une région à partir de laquelle vous souhaitez recevoir des notifications d'événements Amazon S3. Pour plus d'informations à ce sujet, consultez la rubrique Création d'un réseau SNS dans la documentation Amazon SNS. **Important** Assurez-vous d'enregistrer le nom de ressource Amazon (ARN) de votre rubrique SNS.	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
Abonnez la rubrique SNS à la file d'attente SQS centrale.	Abonnez votre rubrique SNS à la file d'attente SQS hébergée par votre région centrale. Pour plus d'informations à ce sujet, consultez la section Abonnement à une rubrique SNS dans la documentation Amazon SNS.	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
Mettez à jour la politique d'accès de la rubrique SNS.	1. Ouvrez la console Amazon SNS, choisissez Rubriques , puis choisissez la rubrique SNS que vous avez créée précédemment. 2. Choisissez Modifier, puis développez la section Politique d'accès - facultative. 3. Joignez la politique d'accès suivante à votre rubrique SNS pour `sns:publish` autoriser Amazon S3, puis choisissez Enregistrer : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "0", "Effect": "Allow", "Principal": { "Service": "s3.amazonaws.com" }, "Action": "sns:Publish", "Resource": "arn:aws:sns:us-west-2::s3Events-SNSTopic-us-west-2" } ] }`	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
Configurez des notifications pour chaque compartiment S3 de la région.	Configurez des notifications d'événements pour chaque compartiment S3 de la région. Pour plus d'informations à ce sujet, consultez la section Activation et configuration des notifications d'événements à l'aide de la console Amazon S3 dans la documentation Amazon S3. **Note** Dans la section Destination, choisissez le sujet SNS et spécifiez l'ARN du sujet SNS que vous avez créé précédemment.	AWS DevOps, architecte du cloud
Répétez cette épopée pour toutes les régions requises.	**Important** Répétez les tâches de cette épopée pour chaque région dont vous souhaitez recevoir des notifications d'événements Amazon S3, y compris votre région centrale.	AWS DevOps, architecte du cloud

Ressources connexes

- Configuration d'une politique d'accès (documentation Amazon SQS)
- Configuration d'une file d'attente SQS en tant que source d'événements (documentation AWS Lambda)
- Configuration d'une file d'attente SQS pour lancer une fonction Lambda (documentation Amazon SQS)
- AWS::Lambda::Function ressource (CloudFormation documentation AWS)

Trois types de tâches ETL AWS Glue pour convertir des données vers Apache Parquet

Créée par Adnan Alvee (AWS), Karthikeyan Ramachandran (AWS) et Nith Govindasivan (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. AWS Glue permet de classer vos données, de les nettoyer, de les enrichir et de les déplacer de manière fiable entre différents magasins de données et flux de données à moindre coût.

Ce modèle fournit différents types de tâches dans AWS Glue et utilise trois scripts différents pour illustrer la création de tâches ETL.

Vous pouvez utiliser AWS Glue pour écrire des tâches ETL dans un environnement shell Python. Vous pouvez également créer des tâches ETL par lots et en streaming en utilisant Python (PySpark) ou Scala dans un environnement Apache Spark géré. Pour vous aider à créer des tâches ETL, ce modèle se concentre sur les tâches ETL par lots à l'aide du shell Python et de Scala. PySpark Les jobs shell Python sont destinés aux charges de travail nécessitant une puissance de calcul moindre. L'environnement Apache Spark géré est destiné aux charges de travail nécessitant une puissance de calcul élevée.

Apache Parquet est conçu pour prendre en charge des schémas de compression et d'encodage efficaces. Il peut accélérer vos charges de travail d'analyse car il stocke les données en colonnes. La conversion de données au format Parquet peut vous faire économiser de l'espace de stockage, de l'argent et du temps à long terme. Pour en savoir plus sur Parquet, consultez le billet de blog Apache Parquet : comment être un héros avec le format de données colonnaire open source.

Conditions préalables et limitations

Prérequis

- Rôle AWS Identity and Access Management (IAM) (si vous n'avez pas de rôle, consultez la section Informations supplémentaires.)

Architecture

Pile technologique cible

- AWS Glue
- Amazon Simple Storage Service (Amazon S3)
- Apache Parquet

Automatisation et mise à l'échelle

- Les flux de travail AWS Glue prennent en charge l'automatisation complète d'un pipeline ETL.
- Vous pouvez modifier le nombre d'unités de traitement des données (DPUs), ou les types de travailleurs, pour qu'ils soient redimensionnés horizontalement et verticalement.

Outils

Services AWS

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Glue est un service ETL entièrement géré qui permet de catégoriser, de nettoyer, d'enrichir et de déplacer vos données entre différents magasins de données et flux de données.

Autres outils

- Apache Parquet est un format de fichier de données open source orienté colonne conçu pour le stockage et la récupération.

Configuration

Utilisez les paramètres suivants pour configurer la puissance de calcul d'AWS Glue ETL. Pour réduire les coûts, utilisez les paramètres minimaux lorsque vous exécutez la charge de travail fournie dans ce modèle.

- Shell Python — Vous pouvez utiliser 1 DPU pour utiliser 16 Go de mémoire ou 0,0625 DPU pour utiliser 1 Go de mémoire. Ce modèle utilise 0,0625 DPU, qui est la valeur par défaut dans la console AWS Glue.
- Python ou Scala pour Spark : si vous choisissez les types de tâches liés à Spark dans la console, AWS Glue utilise par défaut 10 travailleurs et le type de travail G-1X. Ce modèle utilise deux

travailleurs, qui est le nombre minimum autorisé, avec le type de travailleur standard, qui est suffisant et rentable.

Le tableau suivant présente les différents types de travailleurs AWS Glue pour l'environnement Apache Spark. Comme une tâche shell Python n'utilise pas l'environnement Apache Spark pour exécuter Python, elle n'est pas incluse dans le tableau.

	Standard	G.1X	G.2X
vCPU	4	4	8
Mémoire	16 Go	16 Go	32 GO
Espace disque	50 Go	64 Go	128 Go
Exécuteur par travailleur	2	1	1

Code

Pour le code utilisé dans ce modèle, y compris le rôle IAM et la configuration des paramètres, consultez la section Informations supplémentaires.

Épopées

Téléchargez les données

Tâche	Description	Compétences requises
Téléchargez les données dans un compartiment S3 nouveau ou existant.	Créez ou utilisez un compartiment S3 existant dans votre compte. Téléchargez le fichier sample_data.csv depuis la section Pièces jointes et notez l'emplacement du compartiment S3 et du préfixe.	AWS général

Création et exécution de la tâche AWS Glue

Tâche	Description	Compétences requises
Créez la tâche AWS Glue.	Dans la section ETL de la console AWS Glue, ajoutez une tâche AWS Glue. Sélectionnez le type de tâche approprié, la version d'AWS Glue, le type de DPU/trava illeur et le nombre de travaille urs correspondants. Pour plus de détails, consultez la section Configuration.	Développeur, cloud ou données
Modifiez les emplacements d'entrée et de sortie.	Copiez le code correspon dant à votre tâche AWS Glue et modifiez l'emplacement d'entrée et de sortie indiqué dans l'épisode Upload the data.	Développeur, cloud ou données
Configurez les paramètres.	Vous pouvez utiliser les extraits fournis dans la section Informations supplémentaires pour définir les paramètres de votre tâche ETL. AWS Glue utilise quatre noms d'argumen ts en interne : • `--conf` • `--debug` • `--mode` • `--JOB_NAME` Le `--JOB_NAME` paramètre doit être saisi explicitement	Développeur, cloud ou données

Tâche	Description	Compétences requises
	sur la console AWS Glue. Choisissez Tâches, Modifier la tâche, Configuration de sécurité, bibliothèques de scripts et paramètres de tâche (facultatif). Entrez `--JOB_NAME` comme clé et saisissez une valeur. Vous pouvez également utiliser l'interface de ligne de commande AWS (AWS CLI) ou l'API AWS Glue pour définir ce paramètre. Le `--JOB_NAME` paramètre est utilisé par Spark et n'est pas nécessaire dans une tâche d'environnement shell Python. Vous devez en ajouter `--` avant chaque nom de paramètre, sinon le code ne fonctionnera pas. Par exemple, pour les extraits de code, les paramètres de localisation doivent être invoqués par `--input_loc` et. `--output_loc`	
Exécutez le job ETL.	Exécutez votre tâche et vérifiez le résultat. Notez combien d'espace a été réduit par rapport au fichier d'origine.	Développeur, cloud ou données

Ressources connexes

Références

- Apache Spark
- AWS Glue : comment ça marche
- Tarification d'AWS Glue

Tutoriels et vidéos

- Qu'est-ce qu'AWS Glue ?

Informations supplémentaires

Rôle IAM

Lorsque vous créez les tâches AWS Glue, vous pouvez utiliser soit un rôle IAM existant doté des autorisations indiquées dans l'extrait de code suivant, soit un nouveau rôle.

Pour créer un nouveau rôle, utilisez le code YAML suivant.

```
# (c) 2022 Amazon Web Services, Inc. or its affiliates. All Rights Reserved. This AWS
 Content is provided subject to the terms of the AWS Customer
# Agreement available at https://aws.amazon.com/agreement/ or other written agreement
 between Customer and Amazon Web Services, Inc.

AWSTemplateFormatVersion: "2010-09-09"

Description: This template will setup IAM role for AWS Glue service.

Resources:
  rGlueRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "glue.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole
```

```
      Policies:
        - PolicyName: !Sub "${AWS::StackName}-s3-limited-read-write-inline-policy"
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - "s3:PutObject"
                  - "s3:GetObject"
                Resource: "arn:aws:s3:::*/*"
      Tags:
        - Key  : "Name"
          Value : !Sub "${AWS::StackName}"

Outputs:
  oGlueRoleName:
    Description: AWS Glue IAM role
    Value:
      Ref: rGlueRole
    Export:
      Name: !Join [ ":", [ !Ref "AWS::StackName", rGlueRole ] ]
```

Coque Python AWS Glue

Le code Python utilise les Pandas et les PyArrow bibliothèques pour convertir les données en Parquet. La bibliothèque Pandas est déjà disponible. La PyArrow bibliothèque est téléchargée lorsque vous exécutez le modèle, car il s'agit d'une exécution unique. Vous pouvez utiliser des fichiers wheel pour les PyArrow convertir en bibliothèque et fournir le fichier sous forme de package de bibliothèque. Pour plus d'informations sur l'empaquetage des fichiers Wheel, consultez Fournir votre propre bibliothèque Python.

Paramètres du shell AWS Glue Python

```
from awsglue.utils import getResolvedOptions

args = getResolvedOptions(sys.argv, ["input_loc", "output_loc"])
```

Code du shell AWS Glue Python

```
from io import BytesIO
import pandas as pd
import boto3
```

```
import os
import io
import site
from importlib import reload
from setuptools.command import easy_install
install_path = os.environ['GLUE_INSTALLATION']
easy_install.main( ["--install-dir", install_path, "pyarrow"] )
reload(site)
import pyarrow


input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"


input_bucket = input_loc.split('/', 1)[0]
object_key = input_loc.split('/', 1)[1]


output_loc_bucket = output_loc.split('/', 1)[0]
output_loc_prefix = output_loc.split('/', 1)[1]


s3 = boto3.client('s3')
obj = s3.get_object(Bucket=input_bucket, Key=object_key)
df = pd.read_csv(io.BytesIO(obj['Body'].read()))


parquet_buffer = BytesIO()
s3_resource = boto3.resource('s3')
df.to_parquet(parquet_buffer, index=False)
s3_resource.Object(output_loc_bucket, output_loc_prefix +  'data' +
 '.parquet').put(Body=parquet_buffer.getvalue())
```

Tâche AWS Glue Spark avec Python

Pour utiliser un type de tâche AWS Glue Spark avec Python, choisissez Spark comme type de tâche. Choisissez Spark 3.1, Python 3 avec un temps de démarrage des tâches amélioré (Glue Version 3.0) comme version AWS Glue.

Paramètres Python d'AWS Glue

```
from awsglue.utils import getResolvedOptions
```

```
args = getResolvedOptions(sys.argv, ["JOB_NAME", "input_loc", "output_loc"])
```

Tâche AWS Glue Spark avec du code Python

```
import sys
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.transforms import *
from awsglue.dynamicframe import DynamicFrame
from awsglue.utils import getResolvedOptions
from awsglue.job import Job


sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session
job = Job(glueContext)

input_loc = "s3://bucket-name/prefix/sample_data.csv"
output_loc = "s3://bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(\
    connection_type = "s3", \
    connection_options = {
        "paths": [input_loc]}, \
    format = "csv",
    format_options={
        "withHeader": True,
        "separator": ","
    })


outputDF = glueContext.write_dynamic_frame.from_options(\
    frame = inputDyf, \
    connection_type = "s3", \
    connection_options = {"path": output_loc \
        }, format = "parquet")
```

Pour un grand nombre de gros fichiers compressés (par exemple, 1 000 fichiers d'environ 3 Mo chacun), utilisez le `compressionType` paramètre associé au `recurse` paramètre pour lire tous les fichiers disponibles dans le préfixe, comme indiqué dans le code suivant.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Pour un grand nombre de petits fichiers compressés (par exemple, 1 000 fichiers d'environ 133 Ko chacun), utilisez le `groupFiles` paramètre, ainsi que les `recurse` paramètres `compressionType` et. Le `groupFiles` paramètre regroupe les petits fichiers en plusieurs gros fichiers et contrôle le regroupement selon la taille spécifiée en octets (par exemple, 1 Mo). `groupSize` L'extrait de code suivant fournit un exemple d'utilisation de ces paramètres dans le code.

```
input_loc = "bucket-name/prefix/"
output_loc = "bucket-name/prefix/"

inputDyf = glueContext.create_dynamic_frame_from_options(
                    connection_type = "s3",
                    connection_options = {"paths": [input_loc],
                                          "compressionType":"gzip","recurse" :"True",
                                           "groupFiles" :"inPartition",
 "groupSize" :"1048576",
                                          },
                    format = "csv",
                    format_options={"withHeader": True,"separator": ","}
                    )
```

Sans aucune modification des nœuds de travail, ces paramètres permettent à la tâche AWS Glue de lire plusieurs fichiers (grands ou petits, avec ou sans compression) et de les écrire sur la cible au format Parquet.

Tâche AWS Glue Spark avec Scala

Pour utiliser un type de tâche AWS Glue Spark avec Scala, choisissez Spark comme type de tâche et Language comme Scala. Choisissez Spark 3.1, Scala 2 avec un temps de démarrage des tâches amélioré (Glue Version 3.0) comme version AWS Glue. Pour économiser de l'espace de stockage,

l'exemple d'AWS Glue with Scala suivant utilise également `applyMapping` cette fonctionnalité pour convertir les types de données.

Paramètres d'AWS Glue Scala

```
import com.amazonaws.services.glue.util.GlueArgParser val args =
 GlueArgParser.getResolvedOptions(sysArgs, Seq("JOB_NAME", "inputLoc",
 "outputLoc").toArray)
```

Tâche AWS Glue Spark avec code Scala

```
import com.amazonaws.services.glue.GlueContext
import com.amazonaws.services.glue.MappingSpec
import com.amazonaws.services.glue.DynamicFrame
import com.amazonaws.services.glue.errors.CallSite
import com.amazonaws.services.glue.util.GlueArgParser
import com.amazonaws.services.glue.util.Job
import com.amazonaws.services.glue.util.JsonOptions
import org.apache.spark.SparkContext
import scala.collection.JavaConverters._


object GlueScalaApp {
  def main(sysArgs: Array[String]) {

    @transient val spark: SparkContext = SparkContext.getOrCreate()
    val glueContext: GlueContext = new GlueContext(spark)

    val inputLoc = "s3://bucket-name/prefix/sample_data.csv"
    val outputLoc = "s3://bucket-name/prefix/"

    val readCSV = glueContext.getSource("csv", JsonOptions(Map("paths" ->
 Set(inputLoc)))).getDynamicFrame()

    val applyMapping = readCSV.applyMapping(mappings = Seq(("_c0", "string", "date",
 "string"), ("_c1", "string", "sales", "long"),
    ("_c2", "string", "profit", "double")), caseSensitive = false)

    val formatPartition = applyMapping.toDF().coalesce(1)

    val dynamicFrame = DynamicFrame(formatPartition, glueContext)

    val dataSink = glueContext.getSinkWithFormat(
```

```
        connectionType = "s3",
        options = JsonOptions(Map("path" -> outputLoc )),
        transformationContext = "dataSink", format =
 "parquet").writeDynamicFrame(dynamicFrame)
  }
}
```

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Visualisez les journaux d'audit d'Amazon Redshift à l'aide d'Amazon Athena et Amazon QuickSight

Créée par Sanket Sirsikar (AWS) et Gopal Krishna Bhatia (AWS)

Récapitulatif

La sécurité fait partie intégrante des opérations de base de données sur le cloud Amazon Web Services (AWS). Votre organisation doit veiller à surveiller les activités et les connexions des utilisateurs de la base de données afin de détecter les incidents et les risques de sécurité potentiels. Ce modèle vous permet de surveiller vos bases de données à des fins de sécurité et de résolution des problèmes, un processus connu sous le nom d'audit des bases de données.

Ce modèle fournit un script SQL qui automatise la création d'une table et de vues Amazon Athena pour un tableau de bord de reporting dans Amazon qui vous aide à auditer les journaux QuickSight Amazon Redshift. Cela garantit que les utilisateurs chargés de surveiller les activités de la base de données ont un accès pratique aux fonctionnalités de sécurité des données.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un cluster Amazon Redshift existant. Pour plus d'informations à ce sujet, consultez la section Créer un cluster Amazon Redshift dans la documentation Amazon Redshift.
- Accès à un groupe de travail Athena existant. Pour plus d'informations, consultez Comment fonctionnent les groupes de travail dans la documentation Amazon Athena.
- Un compartiment source Amazon Simple Storage Service (Amazon S3) existant avec les autorisations AWS Identity and Access Management (IAM) requises. Pour plus d'informations, consultez la section Permissions des compartiments pour la journalisation des audits Amazon Redshift dans la section Journalisation des audits de base de données dans la documentation Amazon Redshift.

Architecture

Pile technologique

- Athena
- Amazon Redshift
- Amazon S3
- QuickSight

Outils

- Amazon Athena — Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide du SQL standard.
- Amazon QuickSight QuickSight est un service de business intelligence (BI) évolutif, sans serveur, intégrable et basé sur l'apprentissage automatique.
- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données entièrement géré au niveau de l'entreprise, à l'échelle du pétaoctet.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.

Épopées

Configuration du cluster Amazon Redshift

Tâche	Description	Compétences requises
Activez la journalisation des audits pour le cluster Amazon Redshift.	1. Connectez-vous à l'AWS Management Console, ouvrez la console Amazon Redshift, choisissez CLUSTERS, puis choisissez le cluster pour lequel vous souhaitez activer la journalisation. 2. Choisissez l'onglet Propriétés, puis activez l'audit en suivant les instructions de la section Configuration de l'audit à	DBA, ingénieur de données

Tâche	Description	Compétences requises
	l'aide de la console de la documentation Amazon Redshift.	

Tâche	Description	Compétences requises
Activez la journalisation dans le groupe de paramètres du cluster Amazon Redshift.	Vous pouvez activer l'audit des journaux de connexion, des journaux des utilisateurs et des journaux d'activité des utilisateurs en même temps à l'aide de l'AWS Managemen t Console, de la référence d'API Amazon Redshift ou de l'interface de ligne de commande AWS (AWS CLI). Pour auditer les journaux d'activité des utilisateurs, vous devez activer le paramètre `enable_user_activi ty_logging` de base de données. Si vous activez uniquement la fonctionn alité de journalisation des audits, mais pas le paramètre associé, l'audit de base de données enregistre les informations de journalis ation pour la connexion et les journaux utilisateur, mais pas pour les journaux d'activité des utilisateurs. Le `enable_us er_activity_loggin g` paramètre n'est pas activé par défaut, mais vous pouvez l'activer en le remplaçant `false` par`true`.	DBA, ingénieur de données

Tâche	Description	Compétences requises
	Important Vous devez créer un nouveau groupe de paramètres de cluster avec le `user_activity_logging` paramètre activé et l'associer à votre cluster Amazon Redshift. Pour plus d'informations à ce sujet, consultez la section Modification d'un cluster dans la documentation Amazon Redshift. Pour plus d'informations sur cette tâche, consultez les groupes de paramètres Amazon Redshift et Configuration de l'audit à l'aide de la console dans la documentation Amazon Redshift.	

Tâche	Description	Compétences requises
Configurez les autorisations du compartiment S3 pour la journalisation du cluster Amazon Redshift.	Lorsque vous activez la journalisation, Amazon Redshift collecte les informations de journalisation et les télécharge dans des fichiers journaux stockés dans un compartiment S3. Vous pouvez utiliser un compartiment S3 existant ou en créer un nouveau. **Important** Assurez-vous qu'Amazon Redshift dispose des autorisations IAM requises pour accéder au compartiment S3. Pour plus d'informations à ce sujet, consultez la section Permissions des compartiments pour la journalisation des audits Amazon Redshift dans la section Journalisation des audits de base de données de la documentation Amazon Redshift.	DBA, ingénieur de données

Création de la table et des vues Athena

Tâche	Description	Compétences requises
Créez la table et les vues Athena pour interroger les données du journal d'audit Amazon Redshift à partir du compartiment S3.	Ouvrez la console Amazon Athena et utilisez la requête DDL (Data Definitio n Language) du script `AuditLogging.sql` SQL (ci-joint) pour créer la table et les vues des journaux d'activité des utilisateurs, des journaux des utilisateurs et des journaux de connexion. Pour plus d'informations et d'instructions, consultez le didacticiel sur la création de tables et l'exécution de requêtes dans le cadre de l'atelier Amazon Athena.	Ingénieur de données

Configurer la surveillance des journaux dans le QuickSight tableau de bord

Tâche	Description	Compétences requises
Créez un QuickSight tableau de bord en utilisant Athena comme source de données.	Ouvrez la QuickSight console Amazon et créez un QuickSight tableau de bord en suivant les instructions du didacticiel Visualize with QuickSight using Athena du Amazon Athena Workshop.	DBA, ingénieur de données

Ressources connexes

- Création de tables et exécution de requêtes dans Athena
- Visualisez en QuickSight utilisant Athena

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Visualisez les rapports d'identification IAM pour tous les comptes AWS à l'aide d'Amazon QuickSight

Créée par Parag Nagwekar (AWS) et Arun Chanapillai (AWS)

Récapitulatif

> **Warning**
>
> Les utilisateurs IAM disposent d’informations d’identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu’elles ne sont plus nécessaires.

Vous pouvez utiliser les rapports d'identification d'AWS Identity and Access Management (IAM) pour vous aider à répondre aux exigences de sécurité, d'audit et de conformité de votre organisation. Les rapports d'identification fournissent une liste de tous les utilisateurs de vos comptes AWS et indiquent l'état de leurs informations d'identification, telles que les mots de passe, les clés d'accès et les dispositifs d'authentification multifactorielle (MFA). Vous pouvez utiliser les rapports d'identification pour plusieurs comptes AWS gérés par AWS Organizations.

Ce modèle inclut des étapes et du code pour vous aider à créer et à partager des rapports d'identification IAM pour tous les comptes AWS de votre organisation à l'aide des tableaux de bord Amazon QuickSight . Vous pouvez partager les tableaux de bord avec les parties prenantes de votre organisation. Les rapports peuvent aider votre organisation à atteindre les résultats commerciaux ciblés suivants :

- Identifier les incidents de sécurité liés aux utilisateurs IAM
- Suivez la migration en temps réel des utilisateurs IAM vers l'authentification unique (SSO)
- Suivez les régions AWS auxquelles les utilisateurs IAM ont accédé
- Restez en conformité
- Partagez des informations avec d'autres parties prenantes

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une organisation avec des comptes membres
- Un rôle IAM avec des autorisations d'accès aux comptes dans Organizations
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée
- Un abonnement à l'édition Amazon QuickSight Enterprise

Architecture

Pile technologique

- Amazon Athena
- Amazon EventBridge
- Amazon QuickSight
- Amazon Simple Storage Service (Amazon S3)
- AWS Glue
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Organizations

Architecture cible

Le schéma suivant montre une architecture permettant de configurer un flux de travail qui capture les données des rapports d'identification IAM provenant de plusieurs comptes AWS.

1. EventBridge invoque une fonction Lambda tous les jours.
2. La fonction Lambda assume un rôle IAM dans chaque compte AWS de l'organisation. La fonction crée ensuite le rapport d'informations d'identification IAM et stocke les données du rapport dans un compartiment S3 centralisé. Vous devez activer le chiffrement et désactiver l'accès public sur le compartiment S3.

3. Un robot d'exploration AWS Glue explore le compartiment S3 quotidiennement et met à jour la table Athena en conséquence.
4. QuickSight importe et analyse les données du rapport d'identification et crée un tableau de bord qui peut être visualisé et partagé avec les parties prenantes.

Outils

Services AWS

- Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide du langage SQL standard.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres comptes AWS.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Code

Le code de ce modèle est disponible dans le GitHub getiamcredsreport-allaccounts-orgréférentiel. Vous pouvez utiliser le code de ce référentiel pour créer des rapports d'identification IAM sur les comptes AWS dans Organizations et les stocker dans un emplacement central.

Épopées

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Configurez QuickSight l'édition Amazon Enterprise.	1. Activez l'édition Amazon QuickSight Enterprise dans votre compte AWS. Pour plus d'informations, consultez la section Gestion de l'accès des utilisateurs au sein d'Amazon QuickSight dans la QuickSight documentation. 2. Pour accorder des autorisations au tableau de bord, obtenez le nom de ressource Amazon (ARN) des QuickSight utilisateurs.	Administrateur AWS, AWS DevOps, administrateur du cloud, architecte du cloud
Intégrez Amazon QuickSight à Amazon S3 et Athena.	Vous devez QuickSight autoriser l'utilisation d'Amazon S3 et Athena avant de déployer la pile AWS CloudFormation .	Administrateur AWS, AWS DevOps, administrateur du cloud, architecte du cloud

Déployer l'infrastructure

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	1. Clonez le GitHub getiamcredsreport-allaccounts-orgdépôt sur votre machine locale en exécutant la commande suivante :	Administrateur AWS

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/getiamcredsreport-allaccounts-org`	

Tâche	Description	Compétences requises
Déployez l'infrastructure.	1. Connectez-vous à AWS Management Console et ouvrez la console CloudFormation . 2. Dans le volet de navigation, choisissez Create stack, puis sélectionnez With new resources (standard). 3. Sur la page Identifier les ressources, choisissez Next. 4. Sur la page Spécifier le modèle, pour Source du modèle, sélectionnez Télécharger un fichier modèle. 5. Choisissez Choisir un fichier, sélectionnez le `Cloudformation-createcredrepo.yaml` fichier dans votre GitHub référentiel cloné, puis cliquez sur Suivant. 6. Dans Paramètres, effectuez la mise à jour `IAMRoleName` avec votre rôle IAM. Il doit s'agir du rôle IAM que vous souhaitez que Lambda assume dans tous les comptes de l'organisation. Ce rôle crée le rapport d'identification. Remarque : Il n'est pas nécessaire que	Administrateur AWS

Tâche	Description	Compétences requises
	le rôle soit présent dans tous les comptes à cette étape de la création de la pile. 7. Dans Paramètres, mettez à jour `S3BucketName` avec le nom du compartiment S3 dans lequel Lambda peut stocker les informations d'identification de tous les comptes. 8. Dans Nom de la pile, entrez le nom de la pile. 9. Sélectionnez Envoyer. 10. Notez le nom du rôle de la fonction Lambda.	

Tâche	Description	Compétences requises
Créez une politique d'autorisation IAM.	Créez une politique IAM pour chaque compte AWS de votre organisation avec les autorisations suivantes : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "iam:GenerateCredentialReport", "iam:GetCredentialReport" ], "Resource": "*" } ] }`	AWS DevOps, administrateur de cloud, architecte de cloud, ingénieur de données

Tâche	Description	Compétences requises

Créez un rôle IAM avec une politique de confiance.	1. Créez un rôle IAM pour les comptes AWS et joignez la politique d'autorisation que vous avez créée à l'étape précédente.
	2. Associez la politique de confiance suivante au rôle IAM :
	
	`{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Principal":{ "AWS":[ "arn:aws:iam::<MasterAccountID>:role/<LambdaRole>" ] }, "Action": "sts:AssumeRole" } ] }`
	
	Important
	`arn:aws:iam::<MasterAccountID>:role/<LambdaRo`
		Administrateur cloud, architecte cloud, administrateur AWS

Tâche	Description	Compétences requises
	`le>` Remplacez-le par l'ARN du rôle Lambda que vous avez noté précédemment. **Note** Organisations utilisent généralement l'automatisation pour créer des rôles IAM pour leurs comptes AWS. Nous vous recommandons d'utiliser cette automatisation, si elle est disponible. Vous pouvez également utiliser le `CreateRoleforOrg.py` script depuis le référentiel de code. Le script nécessite un rôle administratif existant ou tout autre rôle IAM autorisé à créer une politique et un rôle IAM dans chaque compte AWS.	

Tâche	Description	Compétences requises
Configurez Amazon QuickSight pour visualiser les données.	1. Connectez-vous à l' QuickSightaide de vos informations d'identification. 2. Créez un jeu de données à l'aide d'Athena (à l'aide de la `iamcredreportdb` base de données et de la `“cfn_iamcredreport”` table), puis actualisez automatiquement le jeu de données. 3. Créez une analyse dans QuickSight. 4. Créez un QuickSight tableau de bord.	AWS DevOps, administrateur de cloud, architecte de cloud, ingénieur de données

Informations supplémentaires

Considérations supplémentaires

Éléments à prendre en compte :

- Après CloudFormation avoir déployé l'infrastructure, vous pouvez attendre que les rapports soient créés dans Amazon S3 et analysés par Athena jusqu'à ce que Lambda et AWS Glue soient exécutés conformément à leurs plannings. Vous pouvez également exécuter Lambda manuellement pour obtenir les rapports dans Amazon S3, puis exécuter le robot d'exploration AWS Glue pour obtenir la table Athena créée à partir des données.
- QuickSight est un outil puissant pour analyser et visualiser les données en fonction des besoins de votre entreprise. Vous pouvez utiliser des paramètres QuickSight pour contrôler les données du widget en fonction des champs de données que vous choisissez. Vous pouvez également utiliser une QuickSight analyse pour créer des paramètres (par exemple, des champs Compte, Date et Utilisateur tels que `partition_0partition_1`, et `user` respectivement) à partir de votre ensemble de données afin d'ajouter des contrôles pour les paramètres Compte, Date et Utilisateur.

- Pour créer vos propres QuickSight tableaux de bord, consultez les QuickSight ateliers sur le site Web d'AWS Workshop Studio.
- Pour voir des exemples de QuickSight tableaux de bord, consultez le référentiel de GitHub getiamcredsreport-allaccounts-orgcode.

Résultats commerciaux ciblés

Vous pouvez utiliser ce modèle pour obtenir les résultats commerciaux ciblés suivants :

- Identifiez les incidents de sécurité liés aux utilisateurs IAM : examinez chaque utilisateur de chaque compte AWS de votre organisation à l'aide d'un seul écran. Vous pouvez suivre la tendance des régions AWS les plus récemment consultées par un utilisateur IAM et des services qu'il a utilisés.
- Suivez la migration en temps réel des utilisateurs IAM vers l'authentification SSO : grâce à l'authentification unique, les utilisateurs peuvent se connecter une seule fois avec un seul identifiant et accéder à plusieurs comptes et applications AWS. Si vous envisagez de migrer vos utilisateurs IAM vers le SSO, ce modèle peut vous aider à passer au SSO et à suivre l'utilisation de toutes les informations d'identification des utilisateurs IAM (telles que l'accès à la console de gestion AWS ou l'utilisation des clés d'accès) sur tous les comptes AWS.
- Suivez les régions AWS auxquelles les utilisateurs IAM accèdent : vous pouvez contrôler l'accès des utilisateurs IAM aux régions à diverses fins, telles que la souveraineté des données et le contrôle des coûts. Vous pouvez également suivre l'utilisation des régions par n'importe quel utilisateur IAM.
- Restez en conformité : en suivant le principe du moindre privilège, vous ne pouvez accorder que les autorisations IAM spécifiques requises pour effectuer une tâche spécifique. Vous pouvez également suivre l'accès aux services AWS, à l'AWS Management Console et l'utilisation des informations d'identification à long terme.
- Partagez des informations avec d'autres parties prenantes : vous pouvez partager des tableaux de bord personnalisés avec d'autres parties prenantes, sans leur accorder l'accès aux rapports d'identification IAM ou aux comptes AWS.

Plus de modèles

- Authentifiez les utilisateurs existants de l'application React à l'aide d'Amazon Cognito et de l'interface utilisateur AWS Amplify
- Extrayez automatiquement le contenu de fichiers PDF à l'aide d'Amazon Textract
- Créez un modèle de prévision de démarrage à froid en utilisant DeePar pour les séries chronologiques dans Amazon SageMaker AI Studio Lab
- Créez des rapports détaillés sur les coûts et l'utilisation des clusters Amazon EMR à l'aide d'AWS Cost Explorer
- Créez des rapports détaillés sur les coûts et l'utilisation pour Amazon RDS et Amazon Aurora
- Créez des rapports détaillés sur les coûts et l'utilisation des tâches AWS Glue à l'aide d'AWS Cost Explorer
- Déployer une tâche AWS Glue avec un pipeline AWS CodePipeline CI/CD
- Intégrer un tableau de QuickSight bord Amazon dans une application Angular locale
- Assurez-vous qu'un cluster Amazon Redshift est chiffré lors de sa création
- Assurez-vous que le chiffrement des données Amazon EMR au repos est activé au lancement
- Estimation des coûts de stockage pour une table Amazon DynamoDB
- Exécutez des requêtes SQL Amazon Redshift à l'aide de Terraform
- Extraire et interroger AWS IoT SiteWise les attributs de métadonnées dans un lac de données
- Générez des informations sur les données en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight
- Générez des informations sur les données Db2 z/OS à l'aide d' AWS Mainframe Modernization Amazon Q dans QuickSight
- Donnez aux instances de SageMaker bloc-notes un accès temporaire à un CodeCommit référentiel dans un autre compte AWS
- Identifiez et alertez lorsque les ressources Amazon Data Firehose ne sont pas chiffrées à l'aide d'une clé AWS KMS
- Importez la bibliothèque psycopg2 pour interagir avec votre base AWS Lambda de données PostgreSQL
- Ingérez et analysez les journaux de sécurité AWS dans Microsoft Sentinel
- Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS

- Migrer une base de données Oracle vers Amazon RDS for Oracle à l'aide d'adaptateurs de GoldenGate fichiers plats Oracle
- Migrer une base de données Oracle vers Amazon Redshift à l'aide d'AWS DMS et d'AWS SCT
- Migrez les données d'un environnement Hadoop sur site vers Amazon S3 à l'aide d' DistCp AWS PrivateLink pour Amazon S3
- Migrer du serveur Couchbase vers Couchbase Capella sur AWS
- Migrez les charges de travail Cloudera sur site vers Cloudera Data Platform sur AWS
- Surveillez les clusters Amazon EMR pour le chiffrement en transit lors du lancement
- Gérez le basculement multi-AZ pour les clusters EMR à l'aide d'Application Recovery Controller
- Automatisez les déploiements bleu/vert des bases de données mondiales Amazon Aurora en utilisant les principes de l'IaC
- Provisionner AWS Service Catalog des produits basés sur AWS CloudFormation des modèles à l'aide d' GitHub actions
- Exécutez des tests unitaires pour les tâches ETL Python en AWS Glue utilisant le framework pytest
- Configurer un tableau de bord de surveillance Grafana pour AWS ParallelCluster
- Déchargez les données d'un cluster Amazon Redshift entre différents comptes vers Amazon S3
- Vérifiez que les nouveaux clusters Amazon Redshift ont besoin de points de terminaison SSL
- Vérifiez que les nouveaux clusters Amazon Redshift sont lancés dans un VPC
- Visualisez les résultats du modèle AI/ML à l'aide de Flask et AWS Elastic Beanstalk

Calcul

Rubriques

- Conteneurs et microservices
- sans serveur
- Réseaux
- Diffusion de contenu

Conteneurs et microservices

Rubriques

- Accédez à une base de données Amazon Neptune depuis un conteneur Amazon EKS
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS Fargate, d' PrivateLinkAWS et d'un Network Load Balancer
- Accédez à des applications de conteneur en privé sur Amazon EKS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Activez les MTL dans AWS App Mesh à l'aide d'AWS Private CA sur Amazon EKS
- Automatisez les sauvegardes pour les instances de base de données Amazon RDS for PostgreSQL à l'aide d'AWS Batch
- Automatisez le déploiement du gestionnaire de terminaison de nœuds dans Amazon EKS à l'aide d'un pipeline CI/CD
- Automatically build and deploy a Java application to Amazon EKS using a CI/CD pipeline
- Créez une définition de tâche Amazon ECS et montez un système de fichiers sur des EC2 instances à l'aide d'Amazon EFS
- Déployer des fonctions Lambda avec des images de conteneurs
- Déployez des microservices Java sur Amazon ECS à l'aide d'AWS Fargate
- Déployez des ressources et des packages Kubernetes à l'aide d'Amazon EKS et d'un référentiel de diagrammes Helm dans Amazon S3
- Déployez un exemple de microservice Java sur Amazon EKS et exposez le microservice à l'aide d'un Application Load Balancer
- Déployez une application en cluster sur Amazon ECS à l'aide d'AWS Copilot
- Déployez une application basée sur GRPC sur un cluster Amazon EKS et accédez-y à l'aide d'un Application Load Balancer
- Déploiement et débogage de clusters Amazon EKS
- Déployez des conteneurs à l'aide d'Elastic Beanstalk
- Générez une adresse IP sortante statique à l'aide d'une fonction Lambda, d'Amazon VPC et d'une architecture sans serveur
- Identifiez automatiquement les images de conteneur dupliquées lors de la migration vers un référentiel Amazon ECR

- Installation de l'agent SSM sur les nœuds de travail Amazon EKS à l'aide de Kubernetes DaemonSet
- Installez l'agent SSM et l' CloudWatch agent sur les nœuds de travail Amazon EKS à l'aide de preBootstrapCommands
- Migrer les contrôleurs d'entrée NGINX lors de l'activation du mode automatique Amazon EKS
- Migrez vos charges de travail de conteneurs d'Azure Red Hat OpenShift (ARO) vers Red Hat OpenShift Service on AWS (ROSA)
- Optimisation des images Docker générées par AWS App2Container
- Placez des pods Kubernetes sur Amazon EKS en utilisant l'affinité, les entorses et les tolérances des nœuds
- Répliquez les images filtrées des conteneurs Amazon ECR sur plusieurs comptes ou régions
- Rotation des informations d'identification de base de données sans redémarrer les conteneurs
- Exécutez des tâches Amazon ECS sur Amazon WorkSpaces avec Amazon ECS Anywhere
- Exécuter un conteneur Docker d'API Web ASP.NET Core sur une instance Amazon Linux EC2
- Exécutez des charges de travail basées sur les messages à grande échelle à l'aide d'AWS Fargate
- Exécutez des charges de travail dynamiques avec un stockage de données persistant en utilisant Amazon EFS sur Amazon EKS avec AWS Fargate
- Configurez le dimensionnement automatique piloté par les événements dans Amazon EKS à l'aide d'Amazon EKS Pod Identity et KEDA
- Simplifiez les déploiements de PostgreSQL sur Amazon EKS à l'aide de PGO
- Simplifiez l'authentification des applications avec le protocole TLS mutuel dans Amazon ECS en utilisant Application Load Balancer
- Plus de modèles

Accédez à une base de données Amazon Neptune depuis un conteneur Amazon EKS

Créée par Ramakrishnan Palaninathan (AWS)

Récapitulatif

Ce modèle établit une connexion entre Amazon Neptune, qui est une base de données de graphes entièrement gérée, et Amazon Elastic Kubernetes Service (Amazon EKS), un service d'orchestration de conteneurs, pour accéder à une base de données Neptune. Les clusters de base de données Neptune sont confinés dans un cloud privé virtuel (VPC) sur. AWS Pour cette raison, l'accès à Neptune nécessite une configuration minutieuse du VPC pour permettre la connectivité.

Contrairement à Amazon Relational Database Service (Amazon RDS) pour PostgreSQL, Neptune ne s'appuie pas sur les informations d'identification d'accès classiques à la base de données. Il utilise plutôt des rôles AWS Identity and Access Management (IAM) pour l'authentification. Par conséquent, la connexion à Neptune depuis Amazon EKS implique de configurer un rôle IAM doté des autorisations nécessaires pour accéder à Neptune.

De plus, les points de terminaison Neptune ne sont accessibles que dans le VPC où réside le cluster. Cela signifie que vous devez configurer les paramètres réseau pour faciliter la communication entre Amazon EKS et Neptune. En fonction de vos besoins spécifiques et de vos préférences réseau, il existe différentes approches pour configurer le VPC afin de permettre une connectivité fluide entre Neptune et Amazon EKS. Chaque méthode présente des avantages et des considérations distincts, qui offrent une certaine flexibilité dans la conception de l'architecture de votre base de données en fonction des besoins de votre application.

Conditions préalables et limitations

Prérequis

- Installez la dernière version de kubectl (voir les instructions). Pour vérifier votre version, exécutez :

```
kubectl version --short
```

- Installez la dernière version d'eksctl (voir les instructions). Pour vérifier votre version, exécutez :

```
eksctl info
```

- Installez la dernière version de AWS Command Line Interface (AWS CLI) version 2 (voir les instructions). Pour vérifier votre version, exécutez :

```
aws --version
```

- Créez un cluster de base de données Neptune (voir les instructions). Assurez-vous d'établir des communications entre le VPC du cluster et Amazon EKS via le peering VPC ou une autre méthode. AWS Transit Gateway Assurez-vous également que l'état du cluster est « disponible » et qu'il dispose d'une règle entrante sur le port 8182 pour le groupe de sécurité.
- Configurez un fournisseur IAM OpenID Connect (OIDC) sur un cluster Amazon EKS existant (voir les instructions).

Versions du produit

- Amazon EKS 1.27
- Version 1.3.0.0 du moteur Amazon Neptune (15/11/2023)

Architecture

Le schéma suivant montre la connexion entre les pods Kubernetes d'un cluster Amazon EKS et Neptune pour permettre l'accès à une base de données Neptune.

Automatisation et mise à l'échelle

Vous pouvez utiliser l'autoscaler horizontal Amazon EKS pour adapter cette solution.

Outils

Services

- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Neptune est un service de base de données graphique qui vous permet de créer et d'exécuter des applications qui fonctionnent avec des ensembles de données hautement connectés.

Bonnes pratiques

Pour connaître les meilleures pratiques, consultez Identity and Access Management dans les guides des meilleures pratiques Amazon EKS.

Épopées

Définir les variables d'environnement

Tâche	Description	Compétences requises
Vérifiez le contexte du cluster.	Avant d'interagir avec votre cluster Amazon EKS à l'aide de Helm ou d'autres outils de ligne de commande, vous devez définir des variables d'environnement qui encapsulent les détails de votre cluster. Ces variables sont utilisées dans les commandes suivantes pour garantir qu'elles ciblent le bon cluster et les bonnes ressources. Tout d'abord, vérifiez que vous opérez dans le bon contexte de cluster. Cela garantit que toutes les commandes suivantes sont envoyées au cluster Kubernetes prévu. Pour vérifier le contexte actuel, exécutez la commande suivante. `kubectl config current-context`	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
Définissez la `CLUSTER_NAME` variable.	Définissez la variable d'`CLUSTER_NAME` environnement pour votre cluster Amazon EKS. Dans la commande suivante, remplacez la valeur d'échantillon `us-west-2` par la valeur correcte Région AWS pour votre cluster. Remplacez la valeur d'échantillon `eks-workshop` par le nom de votre cluster existant. `export CLUSTER_NAME=$(aws eks describe-cluster --region us-west-2 --name eks-workshop --query "cluster.name" --output text)`	Administrateur AWS, administrateur du cloud
Validez la sortie.	Pour vérifier que les variables ont été correctement définies, exécutez la commande suivante. `echo $CLUSTER_NAME` Vérifiez que le résultat de cette commande correspond à l'entrée que vous avez spécifiée à l'étape précédente.	Administrateur AWS, administrateur du cloud

Créez un rôle IAM et associez-le à Kubernetes

Tâche	Description	Compétences requises
Création d'un compte de service .	Vous utilisez les rôles IAM pour les comptes de service afin de mapper vos comptes de service Kubernetes aux rôles IAM, afin de permettre une gestion précise des autorisations pour vos applications qui s'exécute nt sur Amazon EKS. Vous pouvez utiliser eksctl pour créer et associer un rôle IAM à un compte de service Kubernetes spécifique au sein de votre cluster Amazon EKS. La politique AWS gérée `NeptuneFullAccess` permet d'accéder en écriture et en lecture au cluster Neptune que vous avez spécifié. ⚠ Important Un point de terminais on OIDC doit être associé à votre cluster avant d'exécuter ces commandes. Créez un compte de service que vous souhaitez associer à une politique AWS gérée	Administrateur AWS, administr ateur du cloud

Tâche	Description	Compétences requises

	nomméeNeptuneFullAccess .
	
	`eksctl create iamserviceaccount --name eks-neptune-sa --namespace default --cluster $CLUSTER_NAME --attach-policy-arn arn:aws:iam::aws:policy/NeptuneFullAccess --approve --override-existing-serviceaccounts`
	
	où `eks-neptune-sa` est le nom du compte de service que vous souhaitez créer.
	
	Une fois terminée, cette commande affiche la réponse suivante :
	
	`2024-02-07 01:12:39 [#] created serviceaccount "default/eks-neptune-sa"`	

Tâche	Description	Compétences requises

Vérifiez que le compte est correctement configuré.	Assurez-vous que le compte de `eks-neptune-sa` service est correctement configuré dans l'espace de noms par défaut de votre cluster.
	`kubectl get sa eks-neptune-sa -o yaml`
	La sortie doit se présenter comme suit :
	`apiVersion: v1`
	`kind: ServiceAccount`
	`metadata:`
	`  annotations:`
	`  eks.amazonaws.com/role-arn: arn:aws:iam::123456789123:role/eksctl-eks-workshop-addon-iamserviceaccount-d-Role1-Q35yKgdQOlmM`
	`  creationTimestamp: "2024-02-07T01:12:39Z"`
	`  labels:`
	`  app.kubernetes.io/managed-by: eksctl`
	`  name: eks-neptune-sa`
	`  namespace: default`
	`  resourceVersion: "5174750"`
	`  uid: cd6ba2f7-a0f5-40e1-a6f4-4081e0042316`
		Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises

Vérifiez la connectivité.	Déployez un module d'échantillonnage appelé `pod-util` et vérifiez la connectivité avec Neptune.
	
	`apiVersion: v1`
	`kind: Pod`
	`metadata:`
	`  name: pod-util`
	`  namespace: default`
	`spec:`
	`  serviceAccountName: eks-neptune-sa`
	`  containers:`
	`  - name: pod-util`
	`  image: public.ecr.aws/patrickc/troubleshoot-util`
	`  command:`
	`  - sleep`
	`  - "3600"`
	`  imagePullPolicy: IfNotPresent`
	
	`kubectl apply -f pod-util.yaml`
	
	`kubectl exec --stdin --tty pod-util -- /bin/bash`
	`bash-5.1# curl -X POST -d '{"gremlin":"g.V().limit(1)"}' https://db-neptune-1.cluster-xxxxxxxxxxxx.us-west-2.neptune.amazonaws.com:8182/gremlin`
		Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
	{"requestId":"a4964f2d-12b1-4ed3-8a14-eff511431a0e","status":{"message":"","code":200,"attributes":{"@type":"g:Map","@value":[]},"result":{"data":{"@type":"g:List","@value":[]},"meta":{"@type":"g:Map","@value":[]}}} bash-5.1# exit exit	

Valider l'activité de connexion

Tâche	Description	Compétences requises
Activez l'authentification de base de données IAM.	Par défaut, l'authentification de base de données IAM est désactivée lorsque vous créez un cluster de base de données Neptune. Vous pouvez activer ou désactiver l'authentification de base de données IAM à l'aide du AWS Management Console. Suivez les étapes décrites dans la AWS documentation pour activer l'authentification de base de données IAM dans Neptune.	Administrateur AWS, administrateur du cloud
Vérifiez les connexions.	Au cours de cette étape, vous interagissez avec le pod-	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises

	`util` conteneur, qui est déjà en cours d'exécution, pour installer awscurl et vérifier la connexion.
	
	1. Exécutez la commande suivante pour trouver le pod.
	
	`kubectl get pods`
	
	La sortie doit se présenter comme suit :
	
	`NAME READY STATUS RESTARTS AGE pod-util 1/1 Running 0 50m`
	
	2. Exécutez la commande suivante pour installer awscurl.
	
	`kubectl exec --stdin --tty pod-util -- /bin/bash bash-5.1# pip3 install awscurl Installing collected packages: idna, configparser, configargparse, charset-normalizer, certifi, requests, awscurl Successfully installed awscurl-0.32 certifi-2024.2.2 charset-normalizer-3.3.2 configargparse-1.7 configpar`	

Tâche	Description	Compétences requises
	ser-6.0.0 idna-3.6 requests-2.31.0 bash-5.1# awscurl https://db-neptune -1.cluster-xxxxxxx xxxxx.us-west-2.ne ptune.amazonaws.co m:8182/status -- region us-west-2 -- service neptune-db {"status":"healthy ","startTime":"Thu Feb 08 01:22:14 UTC 2024","dbEngineVer sion":"1.3.0.0.R1" ,"role":"writer"," dfeQueryEngine":"v iaQueryHint","grem lin":{"version":"t inkerpop-3.6.4"}," sparql":{"version" :"sparql-1.1"},"op encypher":{"versio n":"Neptune-9.0.20 190305-1.0"},"labM ode":{"ObjectIndex ":"disabled","Read WriteConflictDetec tion":"enabled"}," features":{"SlowQu eryLogs":"disabled ","ResultCache":{" status":"disabled" },"IAMAuthenticati on":"enabled","Str eams":"disabled"," AuditLog":"disable d"},"settings":{"c lusterQueryTimeout InMs":"120000","Sl	

Tâche	Description	Compétences requises
	`owQueryLogsThresho ld":"5000"}}`	

Résolution des problèmes

Problème	Solution
Impossible d'accéder à la base de données Neptune.	Passez en revue la politique IAM associée au compte de service. Assurez-vous qu'il autorise les actions nécessaires (par exemple,`neptune:Connec,nep tune:DescribeDBInstances`) pour les opérations que vous souhaitez exécuter.

Ressources connexes

- Autoriser les charges de travail Kubernetes à AWS utiliser les comptes de service Kubernetes (documentation Amazon EKS)
- Rôles IAM pour les comptes de service (documentation Amazon EKS)
- Création d'un nouveau cluster de base de données Neptune (documentation Amazon Neptune)

Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS PrivateLink et d'un Network Load Balancer

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

Ce modèle décrit comment héberger en privé une application de conteneur Docker sur Amazon Elastic Container Service (Amazon ECS) derrière un Network Load Balancer et accéder à l'application via AWS. PrivateLink Vous pouvez ensuite utiliser un réseau privé pour accéder en toute sécurité aux services sur le cloud Amazon Web Services (AWS). Amazon Relational Database Service (Amazon RDS) héberge la base de données relationnelle de l'application exécutée sur Amazon ECS avec haute disponibilité (HA). Amazon Elastic File System (Amazon EFS) est utilisé si l'application nécessite un stockage permanent.

Le service Amazon ECS exécutant les applications Docker, avec un Network Load Balancer sur le front-end, peut être associé à un point de terminaison de cloud privé virtuel (VPC) pour un accès via AWS. PrivateLink Ce service de point de terminaison VPC peut ensuite être partagé avec d'autres utilisateurs VPCs en utilisant leurs points de terminaison VPC.

Vous pouvez également utiliser AWS Fargate au lieu d'un groupe Amazon Auto EC2 Scaling. Pour plus d'informations, consultez Accéder aux applications de conteneur de manière privée sur Amazon ECS à l'aide d'AWS Fargate, d' PrivateLinkAWS et d'un Network Load Balancer.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée sous Linux, macOS ou Windows
- Docker, installé et configuré sous Linux, macOS ou Windows
- Une application exécutée sur Docker

Architecture

Pile technologique

- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon EC2 Auto Scaling
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer
- VPC

Automatisation et mise à l'échelle

- Vous pouvez utiliser AWS CloudFormation pour créer ce modèle en utilisant l'infrastructure en tant que code.

Outils

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS.
- Amazon EC2 Auto Scaling — Amazon EC2 Auto Scaling vous aide à vous assurer que vous disposez du nombre correct d' EC2 instances Amazon disponibles pour gérer la charge de votre application.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif qui facilite l'exécution, l'arrêt et la gestion des conteneurs sur un cluster.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs AWS géré qui est sécurisé, évolutif et fiable.

- Amazon EFS — Amazon Elastic File System (Amazon EFS) fournit un système de fichiers NFS élastique simple, évolutif et entièrement géré à utiliser avec les services cloud AWS et les ressources sur site.
- AWS Lambda — Lambda est un service de calcul permettant d'exécuter du code sans provisionner ni gérer de serveurs.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud AWS.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle d'Internet pour les développeurs.
- AWS Secrets Manager — Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, en fournissant un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) vous aide à déployer des ressources AWS dans un réseau virtuel que vous avez défini.
- Elastic Load Balancing — Elastic Load Balancing distribue le trafic applicatif ou réseau entrant sur plusieurs cibles, telles que EC2 les instances Amazon, les conteneurs et les adresses IP, dans plusieurs zones de disponibilité.
- Docker — Docker aide les développeurs à emballer, expédier et exécuter n'importe quelle application sous la forme d'un conteneur léger, portable et autonome.

Épopées

Création de composants réseau

Tâche	Description	Compétences requises
Créez un VPC.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. Choisissez Create VPC, puis choisissez VPC et plus encore. 2. Entrez un nom pour votre VPC et choisissez une	Administrateur du cloud

Tâche	Description	Compétences requises
	plage de blocs CIDR appropriée. 3. Spécifiez deux zones de disponibilité, deux sous-réseaux publics, quatre sous-réseaux privés. Deux sous-réseaux privés sont destinés aux tâches Amazon ECS, et deux sous-réseaux privés sont destinés aux bases de données Amazon RDS. 4. Spécifiez une passerelle NAT pour chaque zone de disponibilité. 5. Sélectionnez Create VPC (Créer un VPC).	

Création des équilibreurs de charge

Tâche	Description	Compétences requises
Créez un Network Load Balancer.	1. Ouvrez la EC2 console Amazon et choisissez la région AWS qui contient votre VPC. 2. Sous Équilibrage de charge, choisissez Load balancers, puis Create load balancer. 3. Choisissez Network Load Balancer, puis Create.	Administrateur du cloud

Tâche	Description	Compétences requises
	4. Sur la page Configurer l'équilibreur de charge, configurez votre Network Load Balancer et votre écouteur. Important : Assurez-vous de choisir le schéma de votre Network Load Balancer comme Interne. 5. Choisissez les paramètre s de sécurité applicables, configurez un groupe de sécurité et un groupe cible. Choisissez Instance ou IP comme type de cible dans la section Configurer le routage. Assurez-vous de ne pas enregistrer de cible. 6. Lorsque vous avez configuré tous les paramètres, choisissez Next : Review, puis Create.	

Tâche	Description	Compétences requises
Créez un Application Load Balancer.	1. Sur la EC2 console Amazon, choisissez la même région que celle qui contient votre VPC. 2. Sous Équilibrage de charge, choisissez Load balancers, puis Create load balancer. 3. Choisissez Application Load Balancer, puis Create. 4. **Important** Configurez votre Application Load Balancer et son écouteur. Assurez-vous de choisir le schéma de votre équilibreur de charge d'application comme interne. 5. Choisissez les paramètre s de sécurité applicables, configurez un groupe de sécurité et un groupe cible. Choisissez Instance ou IP comme type de cible dans la section Configurer le routage. Assurez-vous de ne pas enregistrer de cible. 6. Lorsque vous avez configuré tous les	Administrateur du cloud

Tâche	Description	Compétences requises
	paramètres, choisissez Next : Review, puis Create.	

Créer un système de fichiers Amazon EFS

Tâche	Description	Compétences requises
Créez un système de fichiers Amazon EFS.	1. Ouvrez la console Amazon EFS et choisissez Create file system. 2. Dans la boîte de dialogue Créer un système de fichiers, entrez le nom de votre système de fichiers et choisissez votre VPC. 3. Choisissez Create pour créer le système de fichiers. 4. Configurez et configurez votre système de fichiers Amazon EFS.	Administrateur du cloud
Montez des cibles pour les sous-réseaux.	1. Retournez à la console Amazon EFS et choisisse z Systèmes de fichiers. La page Systèmes de fichiers affiche les systèmes de fichiers Amazon EFS de votre compte. 2. Choisissez le système de fichiers que vous avez créé, puis sélectionnez Gérer pour afficher les zones de disponibilité. Pour ajouter	Administrateur du cloud

Tâche	Description	Compétences requises
	une cible de montage, choisissez Ajouter une cible de montage et ajoutez les quatre sous-réseaux privés que vous avez créés.	
Vérifiez que les sous-réseaux sont montés en tant que cibles.	1. Sur la console Amazon EFS, sélectionnez Systèmes de fichiers. 2. Choisissez Réseau pour afficher la liste des cibles de montage existantes. Assurez-vous qu'ils incluent les quatre sous-réseaux que vous avez créés.	Administrateur du cloud

Création d’un compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	Ouvrez la console Amazon S3 et créez un compartiment S3 pour stocker les actifs statiques de votre application, si nécessaire.	Administrateur du cloud

Création d'un secret dans le Gestionnaire de Secrets

Tâche	Description	Compétences requises
Créez une clé AWS KMS pour chiffrer le secret du Secrets Manager.	Ouvrez la console AWS Key Management Service (AWS KMS) et créez une clé KMS.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un secret Secrets Manager pour stocker le mot de passe Amazon RDS.	1. Ouvrez la console AWS Secrets Manager et créez un nouveau secret en choisissant Stocker un nouveau secret. 2. Choisissez la clé KMS que vous avez créée et stockez votre nouveau secret.	Administrateur du cloud

Création d'une instance Amazon RDS

Tâche	Description	Compétences requises
Créez un groupe de sous-réseaux de base de données.	1. Ouvrez la console Amazon RDS et choisissez Subnet groups. 2. Choisissez Create DB subnet group, puis entrez un nom et une description pour votre groupe de sous-réseaux DB. 3. Choisissez le VPC que vous avez créé précédemment, puis choisissez les zones de disponibilité et les sous-réseaux. Ensuite, choisissez Créer.	Administrateur du cloud
Créez une instance Amazon RDS.	Créez et configurez une instance Amazon RDS dans les sous-réseaux privés. Assurez-vous que le mode Multi-AZ est activé pour HA.	Administrateur du cloud

Tâche	Description	Compétences requises
Chargez les données sur l'instance Amazon RDS.	Chargez les données relationnelles requises par votre application dans votre instance Amazon RDS. Ce processus varie en fonction des besoins de votre application, ainsi que de la façon dont le schéma de votre base de données est défini et conçu.	Administrateur cloud, DBA

Création des composants Amazon ECS

Tâche	Description	Compétences requises
Créez un cluster ECS.	1. Ouvrez la console Amazon ECS et choisissez Clusters. 2. Choisissez Créer des clusters, puis configurez un cluster ECS conformément à vos spécifications requises.	Administrateur du cloud
Créez les images Docker.	Créez les images Docker en suivant les instructions de la section Ressources associées.	Administrateur du cloud
Créez des référentiels Amazon ECR.	1. Sur la console Amazon ECR, sélectionnez Repositories. 2. Choisissez Créer un référentiel, puis entrez un nom unique pour votre référentiel.	Administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	3. Configurez le référenti el conformément à vos spécifications, y compris le chiffrement AWS KMS si nécessaire.	
Authentifiez votre client Docker pour le référentiel Amazon ECR.	Pour authentifier votre client Docker pour le référentiel Amazon ECR, exécutez la `aws ecr get-login-password` commande « dans l'AWS CLI.	Administrateur du cloud
Transférez les images Docker vers le référentiel Amazon ECR.	1. Identifiez l'image Docker que vous souhaitez envoyer et exécutez la `docker images` commande dans l'AWS CLI. 2. Marquez votre image à l'aide de la combinaison de noms de registre, de référentiel et de balises d'image facultative Amazon ECR. 3. Appuyez sur l'image Docker en exécutant la `docker push` commande. 4. Répétez ces étapes pour toutes les images requises.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez une définition de tâche Amazon ECS.	Une définition de tâche est requise pour exécuter des conteneurs Docker dans Amazon ECS. 1. Revenez à la console Amazon ECS, choisissez Définitions de tâches, puis choisissez Créer une nouvelle définition de tâche. 2. Sur la page Sélectionner les compatibilités, sélectionnez le type de lancement que votre tâche doit utiliser, puis choisissez Étape suivante. **Important** Pour obtenir de l'aide sur la configuration de votre définition de tâche, consultez la section « Création d'une définition de tâche » dans la section Ressources connexes. Assurez-vous de fournir les images Docker que vous avez transmises à Amazon ECR.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un service Amazon ECS service.	Créez un service Amazon ECS en utilisant le cluster ECS que vous avez créé précédemment. Assurez-v ous de choisir Amazon EC2 comme type de lancement, de choisir la définition de tâche créée à l'étape précédente, ainsi que le groupe cible de l'Application Load Balancer.	Administrateur du cloud

Création d'un groupe Amazon EC2 Auto Scaling

Tâche	Description	Compétences requises
Créez une configuration du lancement.	Ouvrez la EC2 console Amazon et créez une configuration de lancement. Assurez-vous que les données utilisateur contiennent le code permettant aux EC2 instances de rejoindre le cluster ECS souhaité. Pour un exemple du code requis, consultez la section Ressources connexes.	Administrateur du cloud
Créez un groupe Amazon EC2 Auto Scaling.	Revenez à la EC2 console Amazon et sous Auto Scaling, sélectionnez Auto Scaling groups. Configurez un groupe Amazon EC2 Auto Scaling. Assurez-vous de choisir les sous-réseaux privés et la configuration de	Administrateur du cloud

Tâche	Description	Compétences requises
	lancement que vous avez créés précédemment.	

Configuration d'AWS PrivateLink

Tâche	Description	Compétences requises
Configurez le point de PrivateLink terminaison AWS.	1. Sur la console Amazon VPC, créez un point de terminaison AWS PrivateLink . 2. Associez ce point de terminaison au Network Load Balancer, qui met l'application hébergée sur Amazon ECS à la disposition privée des clients. Pour plus d'informations, consultez la section Ressources connexes.	Administrateur du cloud

Création d'un point de terminaison de VPC

Tâche	Description	Compétences requises
Créez un point de terminaison de VPC.	Créez un point de terminaison VPC pour le point de PrivateLink terminaison AWS que vous avez créé précédemment. Le nom de domaine complet (FQDN) du point de terminaison VPC pointera vers le nom	Administrateur du cloud

Tâche	Description	Compétences requises
	de domaine complet du point de terminaison AWS PrivateLink . Cela crée une interface réseau élastique vers le service de point de terminaison VPC à laquelle les points de terminaison DNS peuvent accéder.	

Créer la fonction Lambda

Tâche	Description	Compétences requises
Créez la fonction Lambda.	Sur la console AWS Lambda, créez une fonction Lambda pour mettre à jour les adresses IP de l'Application Load Balancer en tant que cibles pour le Network Load Balancer. Pour plus d'informations à ce sujet, consultez le billet de blog Utiliser AWS Lambda pour activer les adresses IP statiques pour les équilibreurs de charge d'application.	Développeur d’applications

Ressources connexes

Créez les équilibreurs de charge :

- Utiliser un Network Load Balancer pour Amazon ECS
- Création d'un Network Load Balancer
- Utiliser un Application Load Balancer pour Amazon ECS

- Création d'un Application Load Balancer

Créez un système de fichiers Amazon EFS :

- Création d'un système de fichiers Amazon EFS
- Création de cibles de montage dans Amazon EFS

Créez un compartiment S3 :

- Création d'un compartiment S3

Créez un secret du Gestionnaire de Secrets :

- Création de clés dans AWS KMS
- Création d'un secret dans AWS Secrets Manager

Créez une instance Amazon RDS :

- Création d'une instance de base de données Amazon RDS

Créez les composants Amazon ECS :

- Création d'un cluster Amazon ECS
- Création d'une image Docker
- Création d'un référentiel Amazon ECR
- Authentifier Docker avec le référentiel Amazon ECR
- Transférer une image vers un référentiel Amazon ECR
- Création d'une définition de tâche Amazon ECS
- Création d'un service Amazon ECS

Créez un groupe Amazon EC2 Auto Scaling :

- Création d'une configuration de lancement
- Création d'un groupe Auto Scaling à l'aide d'une configuration de lancement

- Instances de conteneur Bootstrap avec données EC2 utilisateur Amazon

Configurez AWS PrivateLink :

- Services de point de terminaison VPC (AWS) PrivateLink

Créez un point de terminaison VPC :

- Points de terminaison VPC d'interface (AWS) PrivateLink

Créez la fonction Lambda :

- Création d'une fonction Lambda

Autres ressources :

- Utilisation d'adresses IP statiques pour les équilibreurs de charge d'application
- Accès sécurisé aux services via AWS PrivateLink

Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS Fargate, d' PrivateLinkAWS et d'un Network Load Balancer

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

Ce modèle décrit comment héberger en privé une application de conteneur Docker sur le cloud Amazon Web Services (AWS) en utilisant Amazon Elastic Container Service (Amazon ECS) avec un type de lancement AWS Fargate, derrière un Network Load Balancer, et accéder à l'application via AWS. PrivateLink Amazon Relational Database Service (Amazon RDS) héberge la base de données relationnelle de l'application exécutée sur Amazon ECS avec haute disponibilité (HA). Vous pouvez utiliser Amazon Elastic File System (Amazon EFS) si l'application nécessite un stockage permanent.

Ce modèle utilise un type de lancement Fargate pour le service Amazon ECS exécutant les applications Docker, avec un Network Load Balancer au niveau du front-end. Il peut ensuite être associé à un point de terminaison de cloud privé virtuel (VPC) pour y accéder via AWS. PrivateLink Ce service de point de terminaison VPC peut ensuite être partagé avec d'autres utilisateurs VPCs en utilisant leurs points de terminaison VPC.

Vous pouvez utiliser Fargate avec Amazon ECS pour exécuter des conteneurs sans avoir à gérer des serveurs ou des clusters d'instances Amazon Elastic Compute Cloud (EC2Amazon). Vous pouvez également utiliser un groupe Amazon EC2 Auto Scaling au lieu de Fargate. Pour plus d'informations, consultez Accéder aux applications de conteneur en privé sur Amazon ECS à l'aide d'AWS PrivateLink et d'un Network Load Balancer.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée sous Linux, macOS ou Windows
- Docker, installé et configuré sous Linux, macOS ou Windows
- Une application s'exécutant sur Docker

Architecture

Pile technologique

- Amazon CloudWatch
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- Amazon EFS
- Amazon RDS
- Amazon Simple Storage Service (Amazon S3)
- AWS Fargate
- AWS PrivateLink
- AWS Secrets Manager
- Application Load Balancer
- Network Load Balancer
- VPC

Automatisation et mise à l'échelle

- Vous pouvez utiliser AWS CloudFormation pour créer ce modèle en utilisant l'infrastructure en tant que code.

Outils

Services AWS

- Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs AWS géré qui est sécurisé, évolutif et fiable.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif qui facilite l'exécution, l'arrêt et la gestion des conteneurs sur un cluster.
- Amazon Elastic File System (Amazon EFS) fournit un système de fichiers NFS élastique simple, évolutif et entièrement géré à utiliser avec les services cloud AWS et les ressources sur site.
- AWS Fargateest une technologie que vous pouvez utiliser avec Amazon ECS pour exécuter des conteneurs sans avoir à gérer des serveurs ou des clusters d' EC2 instances Amazon.

- Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le. AWS Cloud
- Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle d'Internet pour les développeurs.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini.
- Elastic Load Balancing (ELB) distribue le trafic applicatif ou réseau entrant sur plusieurs cibles, telles que les EC2 instances, les conteneurs et les adresses IP, dans plusieurs zones de disponibilité.

Autres outils

- Docker aide les développeurs à emballer, expédier et exécuter facilement n'importe quelle application sous la forme d'un conteneur léger, portable et autonome.

Épopées

Création de composants réseau

Tâche	Description	Compétences requises
Créez un VPC.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. Choisissez Create VPC, puis choisissez VPC et plus encore. 2. Entrez un nom pour votre VPC et choisissez une plage de blocs CIDR appropriée.	Administrateur du cloud

Tâche	Description	Compétences requises
	3. Spécifiez deux zones de disponibilité, deux sous-réseaux publics, quatre sous-réseaux privés. Deux sous-réseaux privés sont destinés aux tâches Amazon ECS, et deux sous-réseaux privés sont destinés aux bases de données Amazon RDS. 4. Spécifiez une passerelle NAT pour chaque zone de disponibilité. 5. Sélectionnez Create VPC (Créer un VPC).	

Création des équilibreurs de charge

Tâche	Description	Compétences requises
Créez un Network Load Balancer.	1. Ouvrez la EC2 console Amazon et choisissez la région AWS qui contient votre VPC. 2. Sous Équilibrage de charge, choisissez Load balancers, puis Create load balancer. 3. Choisissez Network Load Balancer, puis Create. 4. Sur la page Configurer l'équilibreur de charge, configurez votre Network	Administrateur du cloud

Tâche	Description	Compétences requises
	Load Balancer et votre écouteur. Important : Assurez-vous de choisir le schéma de votre Network Load Balancer comme Interne. 5. Choisissez les paramètres de sécurité applicables, configurez un groupe de sécurité et un groupe cible. Choisissez IP comme type de cible dans la section Configurer le routage. Assurez-vous de ne pas enregistrer de cible. 6. Lorsque vous avez configuré tous les paramètres, choisissez Next : Review, puis Create. Pour obtenir de l'aide sur ce sujet et sur d'autres articles, consultez la section Ressources connexes.	

Tâche	Description	Compétences requises
Créez un Application Load Balancer.	1. Sur la EC2 console Amazon, choisissez la même région que celle qui contient votre VPC. 2. Sous Équilibrage de charge, choisissez Load balancers, puis Create load balancer. 3. Choisissez Application Load Balancer, puis Create. 4. **Important** Configurez votre Application Load Balancer et son écouteur. Assurez-vous de choisir le schéma de votre équilibreur de charge d'application comme interne. 5. Choisissez les paramètre s de sécurité applicables, configurez un groupe de sécurité et un groupe cible. Choisissez IP comme type de cible dans la section Configurer le routage. Assurez-vous de ne pas enregistrer de cible. 6. Lorsque vous avez configuré tous les	Administrateur du cloud

Tâche	Description	Compétences requises
	paramètres, choisissez Next : Review, puis Create.	

Créer un système de fichiers Amazon EFS

Tâche	Description	Compétences requises
Créez un système de fichiers Amazon EFS.	1. Ouvrez la console Amazon EFS, puis choisissez Create file system. 2. Dans la boîte de dialogue Créer un système de fichiers, entrez le nom de votre système de fichiers et choisissez votre VPC. 3. Choisissez Create pour créer le système de fichiers. 4. Configurez et configurez votre système de fichiers Amazon EFS.	Administrateur du cloud
Montez des cibles pour les sous-réseaux.	1. Retournez à la console Amazon EFS, puis sélectionnez Systèmes de fichiers. La page Systèmes de fichiers affiche les systèmes de fichiers Amazon EFS de votre compte. 2. Choisissez le système de fichiers que vous avez créé, puis sélectionnez Gérer pour afficher la zone de disponibilité.	Administrateur du cloud

Tâche	Description	Compétences requises
	3. Pour ajouter une cible de montage, choisissez Ajouter une cible de montage et ajoutez les quatre sous-réseaux privés que vous avez créés.	
Vérifiez que les sous-réseaux sont montés en tant que cibles.	1. Sur la console Amazon EFS, sélectionnez Systèmes de fichiers. 2. Choisissez Réseau pour afficher la liste des cibles de montage existantes. Assurez-vous qu'ils incluent les quatre sous-réseaux que vous avez créés.	Administrateur du cloud

Création d’un compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	Ouvrez la console Amazon S3 et créez un compartiment S3 pour stocker les actifs statiques de votre application, si nécessaire.	Administrateur du cloud

Création d'un secret dans le Gestionnaire de Secrets

Tâche	Description	Compétences requises
Créez une clé AWS KMS pour chiffrer le secret du Secrets Manager.	Ouvrez la console AWS Key Management Service (AWS KMS) et créez une clé KMS.	Administrateur du cloud
Créez un secret Secrets Manager pour stocker le mot de passe Amazon RDS.	1. Ouvrez la console AWS Secrets Manager et créez un nouveau secret en choisissant Stocker un nouveau secret. 2. Choisissez la clé KMS que vous avez créée et stockez votre nouveau secret.	Administrateur du cloud

Création d'une instance Amazon RDS

Tâche	Description	Compétences requises
Créez un groupe de sous-réseaux de base de données.	1. Ouvrez la console Amazon RDS et choisissez Subnet groups. 2. Choisissez Create DB subnet group, puis entrez un nom et une description pour votre groupe de sous-réseaux DB. 3. Choisissez le VPC que vous avez créé précédemment, puis choisissez les zones de disponibilité et les sous-réseaux. Ensuite, choisissez Créer.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez une instance Amazon RDS.	Créez et configurez une instance Amazon RDS dans les sous-réseaux privés. Assurez-vous que le mode Multi-AZ est activé pour une haute disponibilité (HA).	Administrateur du cloud
Chargez les données sur l'instance Amazon RDS.	Chargez les données relationn elles requises par votre application dans votre instance Amazon RDS. Ce processus varie en fonction des besoins de votre applicati on, ainsi que de la façon dont le schéma de votre base de données est défini et conçu.	DBA

Création des composants Amazon ECS

Tâche	Description	Compétences requises
Créez un cluster ECS.	1. Ouvrez la console Amazon ECS et choisissez Clusters. 2. Choisissez Créer des clusters, puis configurez un cluster ECS conformém ent à vos spécifications requises.	Administrateur du cloud
Créez les images Docker.	Créez les images Docker en suivant les instructions de la AWS documentation.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR.	1. Ouvrez la console Amazon ECR et choisissez Repositories. 2. Choisissez Créer un référentiel, puis entrez un nom unique pour votre référentiel. 3. Configurez le référenti el conformément à vos spécifications, y compris le chiffrement AWS KMS si nécessaire.	Administrateur cloud, DevOps ingénieur
Transférez les images Docker vers le référentiel Amazon ECR.	1. Identifiez l'image Docker que vous souhaitez envoyer et exécutez la `docker images` commande dans l'AWS CLI. 2. Marquez votre image à l'aide de la combinaison de noms de registre, de référentiel et de balises d'image facultative Amazon ECR. 3. Appuyez sur l'image Docker en exécutant la `docker push` commande. 4. Répétez ces étapes pour toutes les images requises.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez une définition de tâche Amazon ECS.	Une définition de tâche est requise pour exécuter des conteneurs Docker dans Amazon ECS. 1. Revenez à la console Amazon ECS, choisissez Définitions de tâches, puis choisissez Créer une nouvelle définition de tâche. 2. Sur la page Sélectionner les compatibilités, sélectionnez le type de lancement que votre tâche doit utiliser, puis choisissez Étape suivante. **Important** Pour obtenir de l'aide sur la configuration de votre définition de tâche, consultez la section « Création d'une définition de tâche » dans la section Ressources connexes. Assurez-vous de fournir les images Docker que vous avez transmises à Amazon ECR.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un service ECS et choisissez Fargate comme type de lancement.	1. Créez un service Amazon ECS en utilisant le cluster ECS que vous avez créé précédemment. Assurez-vous de choisir Fargate comme type de lancement. 2. Choisissez la définition de tâche créée à l'étape précédente et choisissez le groupe cible de l'Application Load Balancer.	Administrateur du cloud

Configuration d'AWS PrivateLink

Tâche	Description	Compétences requises
Configurez le point de PrivateLink terminaison AWS.	1. Ouvrez la console Amazon VPC et créez un AWS PrivateLink point de terminaison. 2. Associez ce point de terminaison au Network Load Balancer, qui met l'application hébergée sur Amazon ECS à la dispositi on privée des clients.	Administrateur du cloud

Création d'un point de terminaison de VPC

Tâche	Description	Compétences requises
Créez un point de terminaison de VPC.	Créez un point de terminaison VPC pour le point de PrivateLi	Administrateur du cloud

Tâche	Description	Compétences requises
	nk terminaison AWS que vous avez créé précédemment. Le nom de domaine complet (FQDN) du point de terminaison VPC pointera vers le nom de domaine complet du point de terminaison AWS PrivateLink . Cela crée une interface réseau élastique vers le service de point de terminaison VPC à laquelle les points de terminaison du service de noms de domaine peuvent accéder.	

Définissez la cible

Tâche	Description	Compétences requises
Ajoutez l'Application Load Balancer en tant que cible.	Pour ajouter l'Application Load Balancer en tant que cible pour le Network Load Balancer, suivez les instructions de la documentation.AWS	Développeur d’applications

Ressources connexes

Créez les équilibreurs de charge :

- Utiliser un Network Load Balancer pour Amazon ECS
- Création d'un Network Load Balancer
- Utiliser un Application Load Balancer pour Amazon ECS
- Création d'un Application Load Balancer

Créez un système de fichiers Amazon EFS :

- Création d'un système de fichiers Amazon EFS
- Création de cibles de montage dans Amazon EFS

Créez un secret du Gestionnaire de Secrets :

- Création de clés dans AWS KMS
- Création d'un secret dans AWS Secrets Manager

Créez une instance Amazon RDS :

- Création d'une instance de base de données Amazon RDS

Création des composants Amazon ECS

- Création d'un référentiel Amazon ECR
- Authentifier Docker avec le référentiel Amazon ECR
- Transférer une image vers un référentiel Amazon ECR
- Création d'une définition de tâche Amazon ECS
- Création d'un service Amazon ECS

Autres ressources :

- Accès sécurisé aux services via AWS PrivateLink

Accédez à des applications de conteneur en privé sur Amazon EKS à l'aide d'AWS PrivateLink et d'un Network Load Balancer

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

Ce modèle décrit comment héberger en privé une application de conteneur Docker sur Amazon Elastic Kubernetes Service (Amazon EKS) derrière un Network Load Balancer, et comment accéder à l'application via AWS. PrivateLink Vous pouvez ensuite utiliser un réseau privé pour accéder en toute sécurité aux services sur le cloud Amazon Web Services (AWS).

Le cluster Amazon EKS exécutant les applications Docker, avec un Network Load Balancer sur le front-end, peut être associé à un point de terminaison de cloud privé virtuel (VPC) pour un accès via AWS. PrivateLink Ce service de point de terminaison VPC peut ensuite être partagé avec d'autres utilisateurs VPCs en utilisant leurs points de terminaison VPC.

La configuration décrite par ce modèle est un moyen sécurisé de partager l'accès aux applications entre VPCs les comptes AWS. Il ne nécessite aucune configuration de connectivité ou de routage particulière, car la connexion entre les comptes client et fournisseur se fait sur le backbone mondial d'AWS et ne traverse pas l'Internet public.

Conditions préalables et limitations

Prérequis

- Docker, installé et configuré sous Linux, macOS ou Windows.
- Une application qui s'exécute sur Docker.
- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée sous Linux, macOS ou Windows.
- Un cluster Amazon EKS existant avec des sous-réseaux privés balisés et configuré pour héberger des applications. Pour plus d'informations, consultez la section Balisage des sous-réseaux dans la documentation Amazon EKS.
- Kubectl, installé et configuré pour accéder aux ressources de votre cluster Amazon EKS. Pour plus d'informations, consultez la section Installation de kubectl dans la documentation Amazon EKS.

Architecture

Pile technologique

- Amazon EKS
- AWS PrivateLink
- Network Load Balancer

Automatisation et mise à l'échelle

- Les manifestes Kubernetes peuvent être suivis et gérés sur un référentiel basé sur Git, puis déployés à l'aide de l'intégration continue et de la livraison continue (CI/CD) dans AWS. CodePipeline
- Vous pouvez utiliser AWS CloudFormation pour créer ce modèle en utilisant l'infrastructure en tant que code (IaC).

Outils

- AWS CLI — AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS à l'aide de commandes dans votre shell de ligne de commande.
- Elastic Load Balancing — Elastic Load Balancing distribue le trafic applicatif ou réseau entrant sur plusieurs cibles, telles que les instances Amazon Elastic Compute Cloud (Amazon EC2), les conteneurs et les adresses IP, dans une ou plusieurs zones de disponibilité.

- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré que vous pouvez utiliser pour exécuter Kubernetes sur AWS sans avoir à installer, exploiter et gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) vous aide à déployer des ressources AWS dans un réseau virtuel que vous avez défini.
- Kubectl — Kubectl est un utilitaire de ligne de commande permettant d'exécuter des commandes sur des clusters Kubernetes.

Épopées

Déployer les fichiers manifestes de déploiement et de service de Kubernetes

Tâche	Description	Compétences requises

Créez le fichier manifeste de déploiement de Kubernetes.	Créez un fichier manifeste de déploiement en modifiant le fichier d'exemple suivant en fonction de vos besoins.
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: sample-app`
	`spec:`
	`  replicas: 3`
	`  selector:`
	`  matchLabels:`
	`  app: nginx`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: nginx`
	`  spec:`
	`  containers:`
	`  - name: nginx`
	`  image:`
	`public.ecr.aws/z9d2n7e1/nginx:1.19.5`
	`  ports:`
	`  - name: http`
	`  containerPort: 80`
	
	Note
	Il s'agit d'un exemple de fichier de configuration NGINX déployé à l'aide de l'image
		DevOps ingénieur

Tâche	Description	Compétences requises
	Docker NGINX. Pour plus d'informations, consultez Comment utiliser l'image officielle de NGINX Docker dans la documentation Docker.	
Déployez le fichier manifeste de déploiement de Kubernetes.	Exécutez la commande suivante pour appliquer le fichier manifeste de déploiement à votre cluster Amazon EKS : `kubectl apply -f <your_deployment_file_name>`	DevOps ingénieur

Tâche	Description	Compétences requises

Créez le fichier manifeste du service Kubernetes.	Créez un fichier manifeste de service en modifiant le fichier d'exemple suivant en fonction de vos besoins.
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: sample-service`
	`  annotations:`
	`  service.beta.kubernetes.io/aws-load-balancer-type: nlb`
	`  service.beta.kubernetes.io/aws-load-balancer-internal: "true"`
	`spec:`
	`  ports:`
	`  - port: 80`
	`  targetPort: 80`
	`  protocol: TCP`
	`  type: LoadBalancer`
	`  selector:`
	`  app: nginx`
	
	⚠ Important
	Assurez-vous d'avoir inclus les éléments suivants `annotations` pour définir un Network Load Balancer interne :
		DevOps ingénieur

Tâche	Description	Compétences requises
	`service.beta.kubernetes.io/aws-load-balancer-type: nlb` `service.beta.kubernetes.io/aws-load-balancer-internal: "true"`	
Déployez le fichier manifeste du service Kubernetes.	Exécutez la commande suivante pour appliquer le fichier manifeste du service à votre cluster Amazon EKS : `kubectl apply -f <your_service_file_name>`	DevOps ingénieur

Création des points de terminaison

Tâche	Description	Compétences requises
Enregistrez le nom du Network Load Balancer.	Exécutez la commande suivante pour récupérer le nom du Network Load Balancer : `kubectl get svc sample-service -o wide` Enregistrez le nom du Network Load Balancer, qui est requis pour créer un point de PrivateLink terminaison AWS.	DevOps ingénieur

Tâche	Description	Compétences requises
Créez un point de PrivateLink terminaison AWS.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon VPC, puis créez un point de terminaison AWS PrivateLink . Associez ce point de terminaison au Network Load Balancer pour mettre l'application à la disposition privée des clients. Pour plus d'informations, consultez les services de point de terminaison VPC PrivateLink (AWS) dans la documentation Amazon VPC. **Important** Si le compte client nécessite l'accès à l'application, l'ID de compte AWS du compte consommateur doit être ajouté à la liste des principaux autorisés pour la configuration du point de PrivateLink terminaison AWS. Pour plus d'informations, consultez la section Ajouter et supprimer des autorisations pour votre service de point de terminaison dans	Administrateur du cloud

Tâche	Description	Compétences requises
	la documentation Amazon VPC.	
Créez un point de terminaison de VPC.	Sur la console Amazon VPC, choisissez Endpoint Services, puis Create Endpoint Service. Créez un point de terminaison VPC pour le point de terminaison AWS PrivateLink . Le nom de domaine complet (FQDN) du point de terminaison VPC pointe vers le nom de domaine complet du point de terminaison AWS. PrivateLink Cela crée une interface réseau élastique vers le service de point de terminaison VPC à laquelle les points de terminaison DNS peuvent accéder.	Administrateur du cloud

Ressources connexes

- Utilisation de l'image officielle de NGINX Docker
- Répartition de charge réseau sur Amazon EKS
- Création de services de point de terminaison VPC (AWS) PrivateLink
- Ajouter et supprimer des autorisations pour votre service de point de terminaison

Activez les MTL dans AWS App Mesh à l'aide d'AWS Private CA sur Amazon EKS

Créée par Omar Kahil (AWS), Emmanuel Saliu (AWS), Muhammad Shahzad (AWS) et Andy Wong (AWS)

Récapitulatif

Ce modèle montre comment implémenter la sécurité mutuelle de la couche de transport (MTL) sur Amazon Web Services (AWS) à l'aide de certificats émis par l'autorité de certification privée AWS (AWS Private CA) dans AWS App Mesh. Il utilise l'API du service de découverte secrète (SDS) d'Envoy via le Secure Production Identity Framework for Everyone (SPIFFE). SPIFFE est un projet open source de la Cloud Native Computing Foundation (CNCF) bénéficiant d'un large soutien communautaire qui fournit une gestion fine et dynamique de l'identité des charges de travail. Pour implémenter les normes SPIFFE, utilisez l'environnement d'exécution SPIRE SPIFFE.

L'utilisation de MTL dans App Mesh permet une authentification bidirectionnelle entre pairs, car elle ajoute une couche de sécurité par rapport au protocole TLS et permet aux services du maillage de vérifier le client qui établit la connexion. Dans la relation client-serveur, le client fournit également un certificat X.509 pendant le processus de négociation de session. Le serveur utilise ce certificat pour identifier et authentifier le client. Cela permet de vérifier si le certificat est émis par une autorité de certification (CA) fiable et s'il est valide.

Conditions préalables et limitations

Prérequis

- Un cluster Amazon Elastic Kubernetes Service (Amazon EKS) avec des groupes de nœuds autogérés ou gérés
- Contrôleur App Mesh déployé sur le cluster avec le SDS activé
- Un certificat privé d'AWS Certificate Manager (ACM) émis par AWS Private CA

Limites

- SPIRE ne peut pas être installé sur AWS Fargate car l'agent SPIRE doit être exécuté en tant que Kubernetes. DaemonSet

Versions du produit

- Graphique AWS App Mesh Controller 1.3.0 ou version ultérieure

Architecture

Le schéma suivant montre le cluster EKS avec App Mesh dans le VPC. Le serveur SPIRE d'un nœud de travail communique avec les agents SPIRE des autres nœuds de travail, ainsi qu'avec AWS Private CA. Envoy est utilisé pour les communications MTL entre les nœuds de travail de l'agent SPIRE.

Le diagramme suivant illustre les étapes suivantes :

1. Le certificat est délivré.
2. Demandez la signature et le certificat du certificat.

Outils

Services AWS

- Autorité de certification privée AWS — L'autorité de certification privée AWS (AWS Private CA) permet de créer des hiérarchies d'autorités de certification (CA) privées, y compris racine et subordonnée CAs, sans les coûts d'investissement et de maintenance liés à l'exploitation d'une autorité de certification sur site.
- AWS App Mesh — AWS App Mesh est un maillage de services qui facilite la surveillance et le contrôle des services. App Mesh normalise la façon dont vos services communiquent, vous offrant ainsi une visibilité cohérente et un contrôle du trafic réseau pour chaque service d'une application.
- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré que vous pouvez utiliser pour exécuter Kubernetes sur AWS sans avoir à installer, exploiter et gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.

Autres outils

- Helm — Helm est un gestionnaire de packages pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes. Ce modèle utilise Helm pour déployer AWS App Mesh Controller.
- Graphique AWS App Mesh Controller : ce modèle utilise le graphique AWS App Mesh Controller pour activer AWS App Mesh sur Amazon EKS.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Configurez App Mesh avec Amazon EKS.	Suivez les étapes de déploiement de base fournies dans le référentiel.	DevOps ingénieur
Installez SPIRE.	Installez SPIRE sur le cluster EKS à l'aide de spire_setup.yaml.	DevOps ingénieur
Installez le certificat AWS Private CA.	Créez et installez un certificat pour votre autorité de certification racine privée en suivant les instructions de la documentation AWS.	DevOps ingénieur
Accordez des autorisations au rôle d'instance du nœud de cluster.	Pour associer des politiques au rôle d'instance du nœud de cluster, utilisez le code figurant dans la section Informations supplémentaires.	DevOps ingénieur
Ajoutez le plugin SPIRE pour AWS Private CA.	Pour ajouter le plugin à la configuration du serveur SPIRE, utilisez le code figurant dans la section Informations supplémentaires. Remplacez le nom de ressource `certificate_authority_arn` Amazon (ARN) par votre ARN CA privé. L'algorithme de signature utilisé doit être le même que celui de l'autorit	DevOps ingénieur

Tâche	Description	Compétences requises
	é de certification privée. Remplacez `your_region` par votre région AWS. Pour plus d'informations sur le plugin, voir Plug-in serveur : UpstreamAuthority « aws_pca ».	
Mettez à jour bundle.cert.	Après avoir créé le serveur SPIRE, un `spire-bundle.yaml` fichier sera créé. Modifiez la `bundle.crt` valeur du `spire-bundle.yaml` fichier de l'autorité de certification privée au certificat public.	DevOps ingénieur

Déployez et enregistrez les charges de travail

Tâche	Description	Compétences requises
Enregistrez les entrées de nœuds et de charges de travail avec SPIRE.	Pour enregistrer le nœud et la charge de travail (services) auprès de SPIRE Server, utilisez le code du référentiel.	DevOps ingénieur
Créez un maillage dans App Mesh avec les mTLS activés.	Créez un nouveau maillage dans App Mesh avec tous les composants de votre application de microservices (par exemple, service virtuel, routeur virtuel et nœuds virtuels).	DevOps ingénieur

Tâche	Description	Compétences requises
Inspectez les entrées enregistrées.	Vous pouvez inspecter les entrées enregistrées pour vos nœuds et charges de travail en exécutant la commande suivante. `kubectl exec -n spire spire-server-0 -- /opt/spire/bin/spire-server entry show` Cela affichera les entrées pour les agents SPIRE.	DevOps ingénieur

Vérifier le trafic MTL

Tâche	Description	Compétences requises
Vérifiez le trafic MTL.	1. À partir du service frontal, envoyez un en-tête HTTP au service principal et vérifiez la réussite de la réponse auprès des services enregistrés dans SPIRE. 2. Pour l'authentification TLS mutuelle, vous pouvez inspecter les `ssl.handshake` statistiques en exécutant la commande suivante. `kubectl exec -it $POD -n $NAMESPACE -c envoy -- curl http://`	DevOps ingénieur

Tâche	Description	Compétences requises
	`localhost:9901/stats	grep ssl.handshake`  Après avoir exécuté la commande précédente, vous devriez voir le `ssl.handshake` nombre d'écouteurs, qui ressemblera à l'exemple suivant :  `listener.0.0.0.0_15000.ssl.handshake: 2`	

Tâche	Description	Compétences requises
Vérifiez que les certificats sont émis par AWS Private CA.	Vous pouvez vérifier que les plugins ont été correctem ent configurés et que les certificats sont émis par votre autorité de certification privée en amont en consultan t les journaux de votre serveur SPIRE. Exécutez la commande suivante. `kubectl logs spire-ser ver-0 -n spire` Consultez ensuite les journaux produits. Ce code suppose que votre serveur est nommé `spire-server-0` et qu'il est hébergé dans votre espace de noms Spire. Vous devriez voir un chargemen t réussi des plugins et une connexion établie avec votre autorité de certification privée en amont.	DevOps ingénieur

Ressources connexes

- Utilisation de MTL avec SPIFFE/SPIRE dans AWS App Mesh sur Amazon EKS
- Activation des MTL dans AWS App Mesh à l'aide de SPIFFE/SPIRE dans un environnement Amazon EKS multi-comptes
- Procédure pas à pas utilisée dans ce modèle
- Plug-in de serveur : UpstreamAuthority « aws_pca »
- Démarrage rapide pour Kubernetes

Informations supplémentaires

Attacher des autorisations au rôle d'instance du nœud de cluster

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ACMPCASigning",
            "Effect": "Allow",
            "Action": [
                "acm-pca:DescribeCertificateAuthority",
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm:ExportCertificate"
            ],
            "Resource": "*"
        }
    ]
}
AWS Managed Policy: "AWSAppMeshEnvoyAccess"
```

Ajoutez le plugin SPIRE pour ACM

```
Add the SPIRE plugin for ACM
Change certificate_authority_arn to your PCA ARN. The signing algorithm used must be
 the same as the signing algorithm on the PCA. Change your_region to the appropriate
 AWS Region.
UpstreamAuthority "aws_pca" {
    plugin_data {
        region = "your_region"
        certificate_authority_arn = "arn:aws:acm-pca:...."
        signing_algorithm = "your_signing_algorithm"
    }
}
```

Automatisez les sauvegardes pour les instances de base de données Amazon RDS for PostgreSQL à l'aide d'AWS Batch

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

La sauvegarde de vos bases de données PostgreSQL est une tâche importante qui peut généralement être effectuée à l'aide de l'utilitaire pg_dump, qui utilise la commande COPY par défaut pour créer un schéma et un vidage des données d'une base de données PostgreSQL. Toutefois, ce processus peut devenir répétitif si vous avez besoin de sauvegardes régulières pour plusieurs bases de données PostgreSQL. Si vos bases de données PostgreSQL sont hébergées dans le cloud, vous pouvez également tirer parti de la fonctionnalité de sauvegarde automatique fournie par Amazon Relational Database Service (Amazon RDS) pour PostgreSQL. Ce modèle décrit comment automatiser les sauvegardes régulières pour les instances de base de données Amazon RDS for PostgreSQL à l'aide de l'utilitaire pg_dump.

Remarque : Les instructions supposent que vous utilisez Amazon RDS. Toutefois, vous pouvez également utiliser cette approche pour les bases de données PostgreSQL hébergées en dehors d'Amazon RDS. Pour effectuer des sauvegardes, la fonction AWS Lambda doit pouvoir accéder à vos bases de données.

Un événement Amazon CloudWatch Events basé sur le temps lance une fonction Lambda qui recherche des balises de sauvegarde spécifiques appliquées aux métadonnées des instances de base de données PostgreSQL sur Amazon RDS. Si les instances de base de données PostgreSQL possèdent la balise DBDump bkp:Automated = Active et d'autres balises de sauvegarde requises, la fonction Lambda soumet des tâches individuelles pour chaque sauvegarde de base de données à AWS Batch.

AWS Batch traite ces tâches et télécharge les données de sauvegarde dans un compartiment Amazon Simple Storage Service (Amazon S3). Ce modèle utilise un fichier Dockerfile et un fichier entrypoint.sh pour créer une image de conteneur Docker qui est utilisée pour effectuer des sauvegardes dans le cadre de la tâche AWS Batch. Une fois le processus de sauvegarde terminé, AWS Batch enregistre les détails de la sauvegarde dans une table d'inventaire sur Amazon DynamoDB. Comme mesure de protection supplémentaire, un événement CloudWatch Events déclenche une notification Amazon Simple Notification Service (Amazon SNS) en cas d'échec d'une tâche dans AWS Batch.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un environnement informatique géré ou non géré existant. Pour plus d'informations, consultez la section Environnements de calcul gérés et non gérés dans la documentation AWS Batch.
- Image Docker de l'interface de ligne de commande (CLI) AWS version 2, installée et configurée.
- Instances de base de données Amazon RDS for PostgreSQL existantes.
- Un compartiment S3 existant.
- Docker, installé et configuré sous Linux, macOS ou Windows.
- Connaissance du codage dans Lambda.

Architecture

Pile technologique

- CloudWatch Événements Amazon
- Amazon DynamoDB
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon RDS
- Amazon SNS
- Amazon S3
- AWS Batch
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- Docker

Outils

- Amazon CloudWatch Events — CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux ressources AWS.

- Amazon DynamoDB — DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité sans faille.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs AWS géré qui est sécurisé, évolutif et fiable.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud AWS.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages aux abonnés par les éditeurs.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.
- AWS Batch — AWS Batch vous aide à exécuter des charges de travail de calcul par lots sur le cloud AWS.
- AWS KMS — AWS Key Management Service (AWS KMS) est un service géré qui vous permet de créer et de contrôler facilement les clés de chiffrement utilisées pour chiffrer vos données.
- AWS Lambda — Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs.
- AWS Secrets Manager — Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Docker — Docker aide les développeurs à emballer, expédier et exécuter facilement n'importe quelle application sous la forme d'un conteneur léger, portable et autonome.

Vos instances de base de données PostgreSQL sur Amazon RDS doivent avoir des balises appliquées à leurs métadonnées. La fonction Lambda recherche des balises pour identifier les instances de base de données qui doivent être sauvegardées. Les balises suivantes sont généralement utilisées.

Balise	Description
BKP:Automatisé = Actif DBDump	Identifie une instance de base de données Amazon RDS comme candidate aux sauvegardes.

point de vente : = AutomatedBackupSecret <secret_name >	Identifie le secret Secrets Manager qui contient les identifiants de connexion Amazon RDS.
BKP : S3Bucket automatisé = DBDump <s3_bucket_name>	Identifie le compartiment S3 auquel envoyer les sauvegardes.
BKP DBDump : Fréquence automatisée BKP DBDump : heure automatisée	Identifiez la fréquence et les heures auxquelle s les bases de données doivent être sauvegard ées.
bkp : pgdumpcommand = <pgdump_c ommand>	Identifie les bases de données pour lesquelles les sauvegardes doivent être effectuées.

Épopées

Création d'une table d'inventaire dans DynamoDB

Tâche	Description	Compétences requises
Créez une table dans DynamoDB.	Connectez-vous à la console de gestion AWS, ouvrez la console Amazon DynamoDB et créez une table. Pour obtenir de l'aide sur ce sujet et sur d'autres articles, consultez la section Ressources connexes.	Administrateur cloud, administrateur de base de données
Vérifiez que la table a été créée.	Exécutez la commande `aws dynamodb describe-table --table-name <table-name> | grep TableStatus` . Si la table existe, la commande renvoie le `"TableStatus": "ACTIVE",` résultat.	Administrateur cloud, administrateur de base de données

Création d'une rubrique SNS pour les échecs de tâches dans AWS Batch

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Ouvrez la console Amazon SNS, choisissez Rubriques et créez une rubrique SNS portant ce nom. `JobFailedAlert` Inscrivez une adresse e-mail active au sujet et consultez votre boîte de réception pour confirmer l'e-mail d'abonnement au réseau social envoyé par AWS Notifications.	Administrateur du cloud
Créez une règle d'échec de tâche pour AWS Batch.	Ouvrez la CloudWatch console Amazon, choisisse z Events, puis Create rule. Choisissez Afficher les options avancées, puis Modifier. Pour créer un modèle qui sélection ne les événements à traiter par vos cibles, remplacez le texte existant par le code « Échec de la tâche » figurant dans la section Informati ons supplémentaires. Ce code définit une règle d' CloudWatch événements qui démarre lorsqu'AWS Batch a un `Failed` événement.	Administrateur du cloud
Ajoutez une cible de règle d'événement.	Dans Cibles, choisissez Ajouter des cibles, puis sélectionnez la rubrique `JobFailedAlert` SNS.	Administrateur du cloud

Tâche	Description	Compétences requises
	Configurez les autres détails et créez la règle Cloudwatch Events.	

Créez une image Docker et envoyez-la vers un référentiel Amazon ECR

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR.	Ouvrez la console Amazon ECR et choisissez la région AWS dans laquelle vous souhaitez créer votre référenti el. Choisissez Référentiels, puis sélectionnez Créer un référentiel. Configurez le référentiel en fonction de vos besoins.	Administrateur du cloud
Écrivez un fichier Dockerfile.	Connectez-vous à Docker et utilisez les « Exemple de fichier Dockerfile » et « Exemple de fichier entrypoin t.sh » de la section Informati ons supplémentaires pour créer un Dockerfile.	DevOps ingénieur
Créez une image Docker et envoyez-la vers le référentiel Amazon ECR.	Créez le Dockerfile en une image Docker et transfére z-le vers le référentiel Amazon ECR. Pour obtenir de l'aide concernant cette histoire, consultez la section Ressources connexes.	DevOps ingénieur

Création des composants AWS Batch

Tâche	Description	Compétences requises
Créez une définition de tâche AWS Batch.	Ouvrez la console AWS Batch et créez une définition de tâche qui inclut l'identifiant de ressource uniforme (URI) du référentiel Amazon ECR comme propriété`Image`.	Administrateur du cloud
Configurez la file d'attente des tâches AWS Batch.	Sur la console AWS Batch, choisissez Job queues, puis Create queue. Créez une file d'attente qui stockera les tâches jusqu'à ce qu'AWS Batch les exécute sur les ressources de votre environnement informatique. Important : assurez-vous d'écrire une logique pour qu'AWS Batch enregistre les détails de la sauvegarde dans la table d'inventaire DynamoDB.	Administrateur du cloud

Création et planification d'une fonction Lambda

Tâche	Description	Compétences requises
Créez une fonction Lambda pour rechercher des balises.	Créez une fonction Lambda qui recherche des balises sur vos instances de base de données PostgreSQL et identifie les candidats de sauvegarde. Assurez-vous que votre fonction Lambda	DevOps ingénieur

Tâche	Description	Compétences requises
	peut identifier la `bkp:AutomatedDBDump = Active` balise et toutes les autres balises requises. Important : La fonction Lambda doit également être capable d'ajouter des tâches à la file d'attente des tâches AWS Batch.	
Créez un CloudWatch événement basé sur le temps.	Ouvrez la CloudWatch console Amazon et créez un événement CloudWatch Events qui utilise une expression cron pour exécuter votre fonction Lambda selon un calendrier régulier. Important : Tous les événements planifiés utilisent le fuseau horaire UTC.	Administrateur du cloud

Testez l'automatisation des sauvegardes

Tâche	Description	Compétences requises
Créez une clé Amazon KMS.	Ouvrez la console Amazon KMS et créez une clé KMS qui peut être utilisée pour chiffrer les informations d'identification Amazon RDS stockées dans AWS Secrets Manager.	Administrateur du cloud
Créez un secret AWS Secrets Manager.	Ouvrez la console AWS Secrets Manager et stockez vos informations d'identif	Administrateur du cloud

Tâche	Description	Compétences requises
	ication de base de données Amazon RDS for PostgreSQL en tant que secret.	
Ajoutez les balises requises aux instances de base de données PostgreSQL.	**Important** Ouvrez la console Amazon RDS et ajoutez des balises aux instances de base de données PostgreSQL que vous souhaitez sauvegarder automatiquement. Vous pouvez utiliser les balises figurant dans le tableau de la section Outils. Si vous avez besoin de sauvegardes à partir de plusieurs bases de données PostgreSQL au sein de la même instance Amazon RDS, `-d test:-d test1` utilisez-la comme valeur pour la balise. `bkp:pgdumpcommand testet test1` sont des noms de base de données. Assurez-vous qu'il n'y a pas d'espace après les deux points (:).	Administrateur du cloud

Tâche	Description	Compétences requises
Vérifiez l'automatisation des sauvegardes.	Pour vérifier l'automatisation des sauvegardes, vous pouvez soit appeler la fonction Lambda, soit attendre que le planning de sauvegard e commence. Une fois le processus de sauvegard e terminé, vérifiez que la table d'inventaire DynamoDB contient une entrée de sauvegarde valide pour vos instances de base de données PostgreSQL. S'ils correspon dent, le processus d'automat isation des sauvegardes est réussi.	Administrateur du cloud

Ressources connexes

Création d'une table d'inventaire dans DynamoDB

- Création d'une table Amazon DynamoDB

Création d'une rubrique SNS pour les échecs de tâches dans AWS Batch

- Création d'une rubrique Amazon SNS
- Envoyer des alertes SNS en cas d'échec d'une tâche dans AWS Batch

Créez une image Docker et envoyez-la vers un référentiel Amazon ECR

- Création d'un référentiel Amazon ECR

- Écrivez un Dockerfile, créez une image Docker et envoyez-la vers Amazon ECR

Création des composants AWS Batch

- Création d'une définition de tâche AWS Batch
- Configuration de votre environnement informatique et de la file d'attente des tâches AWS Batch
- Création d'une file d'attente de tâches dans AWS Batch

Création d'une fonction Lambda

- Création d'une fonction Lambda et écriture de code
- Utiliser Lambda avec DynamoDB

Création d'un CloudWatch événement

- Création d'un CloudWatch événement basé sur le temps
- Utiliser des expressions cron dans Cloudwatch Events

Testez l'automatisation des sauvegardes

- Création d'une clé Amazon KMS
- Création d'un secret dans le Gestionnaire de Secrets
- Ajouter des balises à une instance Amazon RDS

Informations supplémentaires

Événement d'échec de la tâche :

```
{
  "detail-type": [
```

```
    "Batch Job State Change"
  ],
  "source": [
    "aws.batch"
  ],
  "detail": {
    "status": [
      "FAILED"
    ]
  }
}
```

Exemple de fichier Docker :

```
FROM alpine:latest
RUN apk --update add py-pip postgresql-client jq bash && \
pip install awscli && \
rm -rf /var/cache/apk/*
ADD entrypoint.sh /usr/bin/
RUN chmod +x /usr/bin/entrypoint.sh
ENTRYPOINT ["entrypoint.sh"]
```

Exemple de fichier entrypoint.sh :

```
 #!/bin/bash
set -e
DATETIME=`date +"%Y-%m-%d_%H_%M"`
FILENAME=RDS_PostGres_dump_${RDS_INSTANCE_NAME}
FILE=${FILENAME}_${DATETIME}

aws configure --profile new-profile set role_arn arn:aws:iam::${TargetAccountId}:role/
${TargetAccountRoleName}
aws configure --profile new-profile set credential_source EcsContainer

echo "Central Account access provider IAM role is: "
aws sts get-caller-identity

echo "Target Customer Account access provider IAM role is: "
aws sts get-caller-identity --profile new-profile

securestring=$(aws secretsmanager get-secret-value --secret-id $SECRETID --output json
 --query 'SecretString' --region=$REGION --profile new-profile)
```

```
if [[ ${securestring} ]]; then
    echo "successfully accessed secrets manager and got the credentials"
    export PGPASSWORD=$(echo $securestring | jq --raw-output | jq -r '.DB_PASSWORD')
    PGSQL_USER=$(echo $securestring | jq --raw-output | jq -r '.DB_USERNAME')
    echo "Executing pg_dump for the PostGres endpoint ${PGSQL_HOST}"
    # pg_dump -h $PGSQL_HOST -U $PGSQL_USER -n dms_sample | gzip -9 -c  | aws s3 cp -
 --region=$REGION  --profile new-profile s3://$BUCKET/$FILE
    # in="-n public:-n private"
    IFS=':' list=($EXECUTE_COMMAND);
    for command in "${list[@]}";
      do
        echo $command;
        pg_dump -h $PGSQL_HOST -U $PGSQL_USER ${command} | gzip -9 -c  | aws s3 cp - --
region=$REGION --profile new-profile s3://${BUCKET}/${FILE}-${command}".sql.gz"
        echo $?;
        if  [[ $? -ne 0 ]]; then
            echo "Error occurred in database backup process. Exiting now....."
            exit 1
        else
            echo "Postgresql dump was successfully taken for the RDS endpoint
 ${PGSQL_HOST} and is uploaded to the following S3 location s3://${BUCKET}/${FILE}-
${command}.sql.gz"
            #write the details into the inventory table in central account
            echo "Writing to DynamoDB inventory table"
            aws dynamodb put-item --table-name ${RDS_POSTGRES_DUMP_INVENTORY_TABLE} --
region=$REGION --item '{ "accountId": { "S": "'"${TargetAccountId}"'" }, "dumpFileUrl":
 {"S": "'"s3://${BUCKET}/${FILE}-${command}.sql.gz"'" }, "DumpAvailableTime": {"S":
 "'"`date +"%Y-%m-%d::%H::%M::%S"` UTC"'"}}'
            echo $?
            if  [[ $? -ne 0 ]]; then
                echo "Error occurred while putting item to DynamoDb Inventory Table.
 Exiting now....."
                exit 1
            else
                echo "Successfully written to DynamoDb Inventory Table
 ${RDS_POSTGRES_DUMP_INVENTORY_TABLE}"
            fi
        fi
      done;
else
    echo "Something went wrong {$?}"
    exit 1
fi
```

```
exec "$@"
```

Automatisez le déploiement du gestionnaire de terminaison de nœuds dans Amazon EKS à l'aide d'un pipeline CI/CD

Créée par Sandip Gangapadhyay (AWS), John Vargas (AWS), Pragtideep Singh (AWS), Sandeep Gawande (AWS) et Viyoma Sachdeva (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Sur le cloud Amazon Web Services (AWS), vous pouvez utiliser AWS Node Termination Handler, un projet open source, pour gérer avec élégance la fermeture d'une instance Amazon Elastic Compute Cloud EC2 (Amazon) dans Kubernetes. AWS Node Termination Handler permet de garantir que le plan de contrôle Kubernetes répond de manière appropriée aux événements susceptibles de rendre votre EC2 instance indisponible. Ces événements incluent les suivants :

- EC2 maintenance planifiée de l'instance
- Interruptions des instances Amazon EC2 Spot
- Redimensionner le groupe Auto Scaling en
- Rééquilibrage du groupe Auto Scaling entre les zones de disponibilité
- EC2 résiliation de l'instance via l'API ou l'AWS Management Console

Si un événement n'est pas géré, le code de votre application risque de ne pas s'arrêter correctement. Le rétablissement de la disponibilité totale peut également prendre plus de temps ou planifier accidentellement le travail sur les nœuds en panne. Le `aws-node-termination-handler` (NTH) peut fonctionner selon deux modes différents : service de métadonnées d'instance (IMDS) ou processeur de file d'attente. Pour plus d'informations sur les deux modes, consultez le fichier Readme.

Ce modèle utilise AWS CodeCommit et automatise le déploiement de NTH en utilisant le processeur de file d'attente via un pipeline d'intégration continue et de livraison continue (CI/CD).

> **Note**
>
> Si vous utilisez des groupes de nœuds gérés par EKS, vous n'avez pas besoin du`aws-node-termination-handler`.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un navigateur Web compatible avec l'AWS Management Console. Consultez la liste des navigateurs pris en charge.
- AWS Cloud Development Kit (AWS CDK) installé.
- `kubectl`, l'outil de ligne de commande Kubernetes, installé.
- `eksctl`, l'interface de ligne de commande AWS (AWS CLI) pour Amazon Elastic Kubernetes Service (Amazon EKS), installée.
- Un cluster EKS en cours d'exécution avec la version 1.20 ou ultérieure.
- Un groupe de nœuds autogéré rattaché au cluster EKS. Pour créer un cluster Amazon EKS avec un groupe de nœuds autogéré, exécutez la commande suivante.

```
eksctl create cluster --managed=false --region <region> --name <cluster_name>
```

  Pour plus d'informations`eksctl`, consultez la documentation eksctl.
- Fournisseur AWS Identity and Access Management (IAM) OpenID Connect (OIDC) pour votre cluster. Pour plus d'informations, consultez la section Création d'un fournisseur IAM OIDC pour votre cluster.

Limites

- Vous devez utiliser une région AWS qui prend en charge le service Amazon EKS.

Versions du produit

- Kubernetes version 1.20 ou ultérieure
- `eksctl`version 0.107.0 ou ultérieure
- AWS CDK version 2.27.0 ou ultérieure

Architecture

Pile technologique cible

- Un cloud privé virtuel (VPC)
- Un cluster EKS
- Amazon Simple Queue Service (Amazon SQS)
- IAM
- Kubernetes

Architecture cible

Le schéma suivant montre une vue d'ensemble des end-to-end étapes à suivre lors du démarrage de la terminaison du nœud.

Le flux de travail illustré dans le diagramme comprend les étapes de haut niveau suivantes :

1. L'événement de fin d' EC2 instance de dimensionnement automatique est envoyé à la file d'attente SQS.
2. Le NTH Pod surveille la présence de nouveaux messages dans la file d'attente SQS.
3. Le NTH Pod reçoit le nouveau message et effectue les opérations suivantes :
   - Cordonne le nœud afin que le nouveau pod ne s'exécute pas sur le nœud.
   - Draine le nœud, de sorte que le module existant soit évacué
   - Envoie un signal d'accrochage du cycle de vie au groupe Auto Scaling afin que le nœud puisse être arrêté.

Automatisation et mise à l'échelle

- Le code est géré et déployé par AWS CDK, soutenu par AWS CloudFormation Nested Stacks.
- Le plan de contrôle Amazon EKS couvre plusieurs zones de disponibilité pour garantir une haute disponibilité.
- Pour le dimensionnement automatique, Amazon EKS prend en charge le Kubernetes Cluster Autoscaler et Karpenter.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Amazon EC2 Auto Scaling vous aide à maintenir la disponibilité des applications et vous permet d'ajouter ou de supprimer automatiquement EC2 des instances Amazon selon les conditions que vous définissez.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

Autres outils

- kubectl est un outil de ligne de commande Kubernetes permettant d'exécuter des commandes sur des clusters Kubernetes. Vous pouvez utiliser kubectl pour déployer des applications, inspecter et gérer les ressources du cluster et consulter les journaux.

Code

Le code de ce modèle est disponible dans le deploy-nth-to-eksdépôt sur GitHub .com. Le dépôt de code contient les fichiers et dossiers suivants.

- `nth folder`— Le graphique Helm, les fichiers de valeurs et les scripts permettant de scanner et de déployer le CloudFormation modèle AWS pour Node Termination Handler.
- `config/config.json`— Le fichier de paramètres de configuration de l'application. Ce fichier contient tous les paramètres nécessaires au déploiement du CDK.
- `cdk`— Code source du kit AWS CDK.

- `setup.sh`— Le script utilisé pour déployer l'application AWS CDK afin de créer le pipeline CI/CD requis et les autres ressources requises.
- `uninstall.sh`— Le script utilisé pour nettoyer les ressources.

Pour utiliser l'exemple de code, suivez les instructions de la section Epics.

Bonnes pratiques

Pour connaître les meilleures pratiques en matière d'automatisation du gestionnaire de terminaison de nœuds AWS, consultez les pages suivantes :

- Guides des meilleures pratiques EKS
- Gestionnaire de terminaison de nœuds - Configuration

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises

Clonez le dépôt.	Pour cloner le dépôt à l'aide de SSH (Secure Shell), exécutez la commande suivante.
	`git clone git@github.com:aws-samples/deploy-nth-to-eks.git`
	Pour cloner le dépôt à l'aide du protocole HTTPS, exécutez la commande suivante.
	`git clone https://github.com/aws-samples/deploy-nth-to-eks.git`
		Développeur d'applications, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	Le clonage du dépôt crée un dossier nommé. `deploy-nth-to-eks` Accédez à ce répertoire. `cd deploy-nth-to-eks`	
Définissez le fichier kubeconfig.	Définissez vos informations d'identification AWS dans votre terminal et confirmez que vous êtes autorisé à assumer le rôle de cluster. Vous pouvez utiliser l'exemple de code suivant. `aws eks update-kubeconfig --name <Cluster_Name> --region <region>--role-arn <Role_ARN>`	AWS DevOps, DevOps ingénieur, développeur d'applications

Déployer le pipeline CI/CD

Tâche	Description	Compétences requises
Configurez les paramètres.	Dans le `config/config.json` fichier, configurez les paramètres obligatoires suivants. • `pipelineName` : nom du pipeline CI/CD à créer par AWS CDK (par exemple,) `deploy-nth-to-` .	Développeur d'applications, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	`eks-pipeline` AWS CodePipeline créera un pipeline portant ce nom. • `repositoryName` : Le CodeCommit dépôt AWS à créer (par exemple,`deploy-nth-to-eks-repo`). AWS CDK créera ce dépôt et le définira comme source pour le pipeline CI/CD. **Note** Cette solution créera ce CodeCommit dépôt et la branche (fournis dans le paramètre de branche suivant). • `branch`: le nom de la branche dans le dépôt (par exemple,`main`). Un commit dans cette branche lancera le pipeline CI/CD. • `cfn_scan_script` : chemin du script qui sera utilisé pour scanner le CloudFormation modèle AWS pour NTH (`scan.sh`). Ce script existe dans `nth` le dossier qui fera partie du CodeCommit dépôt AWS.	

Tâche	Description	Compétences requises
	• `cfn_deploy_scrip t` : chemin du script qui sera utilisé pour déployer le CloudFormation modèle AWS pour NTH (`installApp.sh`). • `stackName` : nom de la CloudFormation pile à déployer. • `eksClusterName` : nom du cluster EKS existant. • `eksClusterRole` : rôle IAM qui sera utilisé pour accéder au cluster EKS pour tous les appels d'API Kubernetes (par exemple,) . `clusteradmin` Ce rôle est généralement ajouté `aws-authConfigMap` . • `create_cluster_rol e` : Pour créer le rôle `eksClusterRole` IAM, entrez yes. Si vous souhaitez fournir un rôle de cluster existant dans le `eksClusterRole` paramètre, entrez no. • `create_iam_oidc_pr ovider` : Pour créer le fournisseur IAM OIDC pour votre cluster, entrez yes. Si un fournisseur IAM OIDC existe déjà, entrez le numéro. Pour plus d'informa	

Tâche	Description	Compétences requises
	tions, consultez la section Création d'un fournisseur IAM OIDC pour votre cluster. • `AsgGroupName` : liste séparée par des virgules des noms de groupes Auto Scaling qui font partie du cluster EKS (par exemple,`ASG_Group_1,ASG_Group_2`). • `region`: nom de la région AWS où se trouve le cluster (par exemple,`us-east-2`). • `install_cdk` : si AWS CDK n'est pas actuellement installé sur la machine, entrez yes. Exécutez la `cdk --version` commande pour vérifier si la version installée du CDK AWS est la version 2.27.0 ou ultérieure. Dans ce cas, entrez le numéro Si vous entrez « oui », le script setup.sh exécutera la `sudo npm install -g cdk@2.27.0` commande pour installer AWS CDK sur la machine. Le script nécessite des autorisations sudo. Entrez donc le mot de	

Tâche	Description	Compétences requises
	passe du compte lorsque vous y êtes invité.	
Créez le pipeline CI/CD pour déployer NTH.	Exécutez le script setup.sh. `./setup.sh` Le script déploiera l'application AWS CDK qui créera le CodeCommit dépôt avec un exemple de code, le pipeline et les CodeBuild projets basés sur les paramètres saisis par l'utilisateur dans `config/config.json` le fichier. Ce script demandera le mot de passe lors de l'installation des packages npm avec la commande sudo.	Développeur d'applications, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Passez en revue le pipeline CI/CD.	Ouvrez la console de gestion AWS et passez en revue les ressources suivantes créées dans la pile. • CodeCommit dépôt avec le contenu du dossier `nth` • CodeBuild projet AWS`cfn-scan`, qui analysera le CloudFormation modèle à la recherche de vulnérabilités. • CodeBuild projet`Nth-Deploy` , qui déploiera le CloudFormation modèle AWS et les cartes NTH Helm correspondantes via le CodePipeline pipeline AWS. • Un CodePipeline pipeline pour déployer NTH. Une fois le pipeline exécuté avec succès, la version Helm `aws-node-termination-handler` est installée dans le cluster EKS. En outre, un Pod nommé `aws-node-termination-handler` est en cours d'exécution dans l'`kube-system` espace de noms du cluster.	Développeur d'applications, AWS DevOps, DevOps ingénieur

Tester le déploiement de NTH

Tâche	Description	Compétences requises
Simulez un événement de mise à l'échelle d'un groupe Auto Scaling.	Pour simuler un événement de mise à l'échelle automatique, procédez comme suit : 1. Sur la console AWS, ouvrez la EC2 console et choisissez Auto Scaling Groups. 2. Sélectionnez le groupe Auto Scaling portant le même nom que celui indiqué dans`config/config.json`, puis choisissez Edit. 3. Diminuez la capacité souhaitée et minimale de 1. 4. Choisissez Mettre à jour.	
Passez en revue les journaux.	Pendant l'événement de scale-in, le NTH Pod bouclera et drainera le nœud de travail correspondant (l' EC2 instance qui sera résiliée dans le cadre de l'événement de scale-in). Pour consulter les journaux, utilisez le code de la section Informations supplémentaires.	Développeur d'applications, AWS DevOps, DevOps ingénieur

Nettoyage

Tâche	Description	Compétences requises
Nettoyez toutes les ressources AWS.	Pour nettoyer les ressources créées par ce modèle, exécutez la commande suivante. `./uninstall.sh` Cela nettoiera toutes les ressources créées dans ce modèle en supprimant la CloudFormation pile.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Le registre npm n'est pas configuré correctement.	Lors de l'installation de cette solution, le script installe npm install pour télécharger tous les packages requis. Si, pendant l'installation, vous voyez un message indiquant « Impossible de trouver le module », le registre npm n'est peut-être pas configuré correctement. Pour voir le paramètre de registre actuel, exécutez la commande suivante. `npm config get registry` Pour définir le registre avec`https://registry.npmjs.org/`, exécutez la commande suivante.

Problème	Solution
	`npm config set registry https://registry.npmjs.org`
Retardez la livraison des messages SQS.	Dans le cadre de votre dépannage, si vous souhaitez retarder la remise des messages SQS à NTH Pod, vous pouvez ajuster le paramètre de délai de livraison SQS. Pour plus d'informations, consultez les files d'attente Amazon SQS Delay.

Ressources connexes

- Code source du gestionnaire de terminaison des nœuds AWS
- EC2 atelier
- AWS CodePipeline
- Amazon Elastic Kubernetes Service (Amazon EKS)
- Kit de développement AWS Cloud
- AWS CloudFormation

Informations supplémentaires

1. Trouvez le nom du NTH Pod.

```
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
kubectl get pods -n kube-system |grep aws-node-termination-handler
aws-node-termination-handler-65445555-kbqc7   1/1     Running   0          26m
```

2. Consultez les journaux. Un exemple de journal ressemble à ce qui suit. Cela indique que le nœud a été bouclé et vidé avant d'envoyer le signal de fin du cycle de vie du groupe Auto Scaling.

```
kubectl -n kube-system logs aws-node-termination-handler-65445555-kbqc7
022/07/17 20:20:43 INF Adding new event to the event store
 event={"AutoScalingGroupName":"eksctl-my-cluster-target-nodegroup-
```

```
ng-10d99c89-NodeGroup-ZME36IGAP7O1","Description":"ASG Lifecycle Termination
 event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n","EndTime":"0001-01-01T00:00:00Z","EventID":"asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564","InProgress":fal
east-2.compute.internal","NodeProcessed":false,"Pods":null,"ProviderID":"aws:///us-
east-2c/i-0409f2a9d3085b80e","StartTime":"2022-07-17T20:20:42.702Z","State":""}
2022/07/17 20:20:44 INF Requesting instance drain event-id=asg-lifecycle-
term-33383831316538382d353564362d343332362d613931352d383430666165636334333564
 instance-id=i-0409f2a9d3085b80e kind=SQS_TERMINATE node-name=ip-192-168-75-60.us-
east-2.compute.internal provider-id=aws:///us-east-2c/i-0409f2a9d3085b80e
2022/07/17 20:20:44 INF Pods on node node_name=ip-192-168-75-60.us-
east-2.compute.internal pod_names=["aws-node-qchsw","aws-node-termination-
handler-65445555-kbqc7","kube-proxy-mz5x5"]
2022/07/17 20:20:44 INF Draining the node
2022/07/17 20:20:44 ??? WARNING: ignoring DaemonSet-managed Pods: kube-system/aws-node-
qchsw, kube-system/kube-proxy-mz5x5
2022/07/17 20:20:44 INF Node successfully cordoned and drained
 node_name=ip-192-168-75-60.us-east-2.compute.internal reason="ASG Lifecycle
 Termination event received. Instance will be interrupted at 2022-07-17 20:20:42.702
 +0000 UTC \n"
2022/07/17 20:20:44 INF Completed ASG Lifecycle Hook (NTH-K8S-TERM-HOOK) for instance
 i-0409f2a9d3085b80e
```

Automatically build and deploy a Java application to Amazon EKS using a CI/CD pipeline

Créée par MAHESH RAGHUNANDANAN (AWS), James Radtke (AWS) et Jomcy Pappachen (AWS)

Récapitulatif

Ce modèle décrit comment créer un pipeline d'intégration et de livraison continues (CI/CD) qui crée et déploie automatiquement une application Java selon les DevSecOps pratiques recommandées sur un cluster Amazon Elastic Kubernetes Service (Amazon EKS) sur le. AWS Cloud Ce modèle utilise une application d'accueil développée avec un framework Java Spring Boot et qui utilise Apache Maven.

Vous pouvez utiliser l'approche de ce modèle pour créer le code d'une application Java, empaqueter les artefacts de l'application sous forme d'image Docker, scanner l'image de sécurité et télécharger l'image en tant que conteneur de charge de travail sur Amazon EKS. L'approche de ce modèle est utile si vous souhaitez migrer d'une architecture monolithique étroitement couplée vers une architecture de microservices. Cette approche vous permet également de surveiller et de gérer l'ensemble du cycle de vie d'une application Java, ce qui garantit un niveau d'automatisation supérieur et permet d'éviter les erreurs ou les bogues.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Command Line Interface (AWS CLI) version 2, installée et configurée. Pour plus d'informations à ce sujet, consultez la section Installation ou mise à jour vers la dernière version AWS CLI de la AWS CLI documentation.

  AWS CLI la version 2 doit être configurée avec le même rôle AWS Identity and Access Management (IAM) qui crée le cluster Amazon EKS, car seul ce rôle est autorisé à ajouter d'autres rôles IAM au. `aws-auth ConfigMap` Pour plus d'informations et pour connaître les étapes de configuration AWS CLI, consultez la section Configuration des paramètres dans la AWS CLI documentation.
- Rôles et autorisations IAM avec accès complet à AWS CloudFormation. Pour plus d'informations à ce sujet, consultez la section Contrôle de l'accès avec IAM dans la AWS CloudFormation documentation.

- Un cluster Amazon EKS existant, avec les détails du nom du rôle IAM et le nom de ressource Amazon (ARN) du rôle IAM pour les nœuds de travail du cluster EKS.
- Kubernetes Cluster Autoscaler, installé et configuré dans votre cluster Amazon EKS. Pour plus d'informations, consultez la section Scale cluster computing with Karpenter et Cluster Autoscaler dans la documentation Amazon EKS.
- Accès au code du GitHub référentiel.

> **Important**
>
> AWS Security Hub est activé dans le cadre des AWS CloudFormation modèles inclus dans le code de ce modèle. Par défaut, une fois Security Hub activé, un essai gratuit de 30 jours est proposé. Après la période d'essai, cela entraîne un coût Service AWS. Pour de plus amples informations sur la tarification, veuillez consulter AWS Security Hub Tarification.

Versions du produit

- Helm version 3.4.2 ou ultérieure
- Apache Maven version 3.6.3 ou ultérieure
- BridgeCrew Checkov version 2.2 ou ultérieure
- Aqua Security Trivy version 0.37 ou ultérieure

Architecture

Pile technologique

- AWS CodeBuild
- AWS CodeCommit

  Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus. Cependant, cette solution fonctionnera avec n'importe quel fournisseur Git de système de contrôle de version (VCS) tel que GitHub ou GitLab avec des modifications minimales.
- Amazon CodeGuru
- AWS CodePipeline

- Amazon Elastic Container Registry (Amazon ECR)
- Amazon EKS
- Amazon EventBridge
- AWS Security Hub
- Amazon Simple Notification Service (Amazon SNS)

Architecture cible

Le schéma suivant illustre le flux de travail suivant :

1. Le développeur met à jour le code de l'application Java dans la branche de base du CodeCommit référentiel, ce qui crée une pull request (PR).
2. Dès que le PR est soumis, Amazon CodeGuru Reviewer passe automatiquement en revue le code, l'analyse en fonction des meilleures pratiques pour Java et donne des recommandations au développeur.
3. Une fois le PR fusionné avec la branche de base, un EventBridge événement Amazon est créé.
4. L' EventBridge événement initie le CodePipeline pipeline, qui démarre.
5. CodePipeline exécute la phase de CodeSecurity scan (sécurité continue).
6. AWS CodeBuild lance le processus d'analyse de sécurité dans lequel les fichiers Helm du déploiement Dockerfile et Kubernetes sont analysés à l'aide de Checkov, et le code source de l'application est analysé en fonction des modifications de code incrémentielles. L'analyse du code source de l'application est effectuée par le wrapper de l'interface de ligne de commande (CLI) CodeGuru Reviewer.
7. Si la phase d'analyse de sécurité est réussie, la phase de construction (intégration continue) est lancée.
8. Au cours de la phase de construction CodeBuild , génère l'artefact, l'empaquette dans une image Docker, scanne l'image pour détecter les failles de sécurité à l'aide d'Aqua Security Trivy et stocke l'image dans Amazon ECR.
9. Les vulnérabilités détectées à l'étape 8 sont téléchargées vers Security Hub pour une analyse plus approfondie par les développeurs ou les ingénieurs. Security Hub fournit une vue d'ensemble et des recommandations pour remédier aux vulnérabilités.
10. Les notifications par e-mail concernant les phases séquentielles du CodePipeline pipeline sont envoyées via Amazon SNS.

11. Une fois les phases d'intégration continue terminées, CodePipeline passe à la phase de déploiement (livraison continue).
12. L'image Docker est déployée sur Amazon EKS en tant que charge de travail de conteneur (pod) à l'aide de graphiques Helm.
13. Le pod d'application est configuré avec l'agent Amazon CodeGuru Profiler, qui envoie les données de profilage de l'application (processeur, utilisation du tas et latence) à CodeGuru Profiler, ce qui aide les développeurs à comprendre le comportement de l'application.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.

  Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus
- Amazon CodeGuru Profiler collecte les données de performances d'exécution de vos applications en ligne et fournit des recommandations qui peuvent vous aider à affiner les performances de vos applications.
- Amazon CodeGuru Reviewer utilise l'analyse des programmes et l'apprentissage automatique pour détecter les défauts potentiels difficiles à détecter pour les développeurs et propose des suggestions pour améliorer votre code Java et Python.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.

- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources, notamment des AWS Lambda fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Security Hubfournit une vue complète de votre état de sécurité sur AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres services

- Helm est un gestionnaire de paquets open source pour Kubernetes.
- Apache Maven est un outil de gestion et de compréhension de projets logiciels.
- BridgeCrew Checkov est un outil d'analyse de code statique permettant de scanner les fichiers d'infrastructure en tant que code (IaC) pour détecter les erreurs de configuration susceptibles d'entraîner des problèmes de sécurité ou de conformité.
- Aqua Security Trivy est un scanner complet pour détecter les vulnérabilités dans les images de conteneurs, les systèmes de fichiers et les référentiels Git, en plus des problèmes de configuration.

Code

Le code de ce modèle est disponible dans le GitHub aws-codepipeline-devsecops-amazoneksréférentiel.

Bonnes pratiques

- Ce modèle suit les meilleures pratiques de sécurité IAM afin d'appliquer le principe du moindre privilège pour les entités IAM à toutes les phases de la solution. Si vous souhaitez étendre la solution avec des outils supplémentaires Services AWS ou tiers, nous vous recommandons de consulter la section sur l'application des autorisations de moindre privilège dans la documentation IAM.

- Si vous avez plusieurs applications Java, nous vous recommandons de créer des pipelines CI/CD distincts pour chaque application.
- Si vous avez une application monolithe, nous vous recommandons de la diviser en microservices dans la mesure du possible. Les microservices sont plus flexibles, ils facilitent le déploiement des applications sous forme de conteneurs et ils offrent une meilleure visibilité sur la création et le déploiement globaux de l'application.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Pour cloner le dépôt, exécutez la commande suivante. `git clone https://github.com/aws-samples/aws-codepipeline-devsecops-amazoneks`	Développeur d'applications, DevOps ingénieur
Créez un compartiment S3 et téléchargez le code.	1. Connectez-vous à la console Amazon S3 AWS Management Console, ouvrez-la, puis créez un compartiment S3 dans l' Région AWS endroit où vous prévoyez de déployer cette solution. Pour plus d'informations, consultez la section Création d'un compartiment dans la documentation Amazon S3. 2. Dans le compartiment S3, créez un dossier nommé`code`.	AWS DevOps, administrateur du cloud, DevOps ingénieur

Tâche	Description	Compétences requises

	3. Accédez à l'endroit où vous avez cloné le dépôt. Pour créer une version compressée de l'intégralité du code avec l'extension .zip (`cicdstack.zip`) et valider le fichier .zip, exécutez les commandes suivantes dans l'ordre.
	`cd aws-codepipeline-devsecops-amazoneks`
	`python -m zipfile -c cicdstack.zip *`
	`python -m zipfile -t cicdstack.zip`
	Note
	Si la `python` commande échoue et indique que Python n'a pas été trouvé, utilisez-le à la `python3` place.
	4. Téléchargez le `cicdstack.zip` fichier dans le dossier de code que vous avez créé précédemment dans le compartiment S3.	

Tâche	Description	Compétences requises
Créez une AWS CloudFormation pile.	1. Ouvrez la console AWS CloudFormation et choisissez Créer une pile. 2. Dans Spécifier le modèle, choisissez Télécharger un fichier modèle, chargez le `cf_templates/codecommit_ecr.yaml` fichier, puis cliquez sur Suivant. 3. Dans Spécifier les détails de la pile, entrez le nom de la pile, puis fournissez les valeurs de paramètres d'entrée suivantes : • `CodeCommitRepositoryBranchName` : nom de la branche où résidera votre code (le nom par défaut est`main`) • `CodeCommitRepositoryName` : le nom du CodeCommitrepository à créer • `CodeCommitRepositoryS3Bucket` : nom du compartiment S3 dans lequel vous avez créé le dossier de code • `CodeCommitRepositoryS3BucketObjKey` : `code/cicdstack.zip`	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	• `ECRRepositoryName` : nom du référentiel Amazon ECR à créer 4. Choisissez Next, utilisez les paramètres par défaut pour les options de configuration de la pile, puis choisissez Next. 5. Dans la section Révision, vérifiez le modèle et les détails de la pile, puis choisissez Create stack. La pile est ensuite créée, y compris les référentiels CodeCommit et Amazon ECR. 6. Notez les noms des référentiels CodeCommit et Amazon ECR, qui seront nécessaires pour configurer le pipeline Java CI/CD.	
Validez le déploiement de la CloudFormation pile.	1. Sous Stacks sur la CloudFormation console, vérifiez l'état de la CloudFormation pile que vous avez déployée. Le statut de la pile doit être CREATE COMPLETE. 2. Depuis la console, vérifiez que les référentiels CloudFormation et Amazon ECR ont été provisionnés et sont prêts.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Supprimez le compartiment S3.	Videz et supprimez le compartiment S3 que vous avez créé précédemment. Pour plus d'informations, consultez Supprimer un compartiment dans la documentation Amazon S3.	AWS DevOps, DevOps ingénieur

Configuration des diagrammes Helm

Tâche	Description	Compétences requises
Configurez les diagrammes Helm de votre application Java.	1. À l'emplacement où vous avez cloné le GitHub référentiel, accédez au dossier`helm_charts/aws-proserve-java-greeting`. Dans ce dossier, le `values.dev.yaml` fichier contient des informations sur la configuration des ressources Kubernetes que vous pouvez modifier pour vos déploiements de conteneurs sur Amazon EKS. Mettez à jour le paramètre du référentiel Docker en fournissant votre Compte AWS identifiant et Région AWS le nom du référentiel Amazon ECR. `image:`	DevOps ingénieur

Tâche	Description	Compétences requises

	<pre> repository:
	 <account-id>.dkr.ecr.<region>.amazonaws.com/<app-ecr-repo-name></pre>
	2. Le type de service du module Java est défini sur`LoadBalancer` .
	<pre>service:
	  type: LoadBalancer
	  port: 80
	  targetPort: 8080
	  path: /hello
	  initialDelaySeconds: 60
	  periodSeconds: 30</pre>
	Pour utiliser un autre service (par exemple,`NodePort`), vous pouvez modifier ce paramètre. Pour plus d'informations, consultez la documentation de Kubernetes.
	3. Vous pouvez activer le Kubernetes Horizontal Pod Autoscaler en modifiant le paramètre sur. `autoscaling enabled: true`
	<pre>autoscaling:
	  enabled: true
	  minReplicas: 1
	  maxReplicas: 100</pre>	

Tâche	Description	Compétences requises
	<pre> targetCPUUtilizati onPercentage: 80 # targetMem oryUtilizationPerc entage: 80</pre> 4. Vous pouvez activer différentes fonctionnalités pour les charges de travail Kubernetes en modifiant les valeurs du `values.<ENV>.yaml` fichier, en indiquant où se `<ENV>` trouve votre environnement de développement, de production, d'UAT ou d'assurance qualité.	

Tâche	Description	Compétences requises

Validez les graphiques de Helm pour détecter les erreurs de syntaxe.	1. Depuis le terminal, vérifiez que Helm v3 est installé sur votre poste de travail local en exécutant la commande suivante.
	`helm --version`
	Si Helm v3 n'est pas installé, installez-le.
	2. Dans le terminal, accédez au répertoire des diagrammes Helm (`helm_charts/aws-proserve-java-greeting`) et exécutez la commande suivante.
	`helm lint . -f values.dev.yaml`
	Cela permettra de vérifier la présence d'éventuelles erreurs de syntaxe dans les diagrammes de Helm.
		DevOps ingénieur

Configuration du pipeline Java CI/CD

Tâche	Description	Compétences requises
Créez le pipeline CI/CD.	1. Ouvrez la console AWS CloudFormation et choisissez Créer une pile.	AWS DevOps

Tâche	Description	Compétences requises
	2. Dans Spécifier le modèle, choisissez Télécharger un fichier modèle, chargez le `cf_templates/build_deployment.yaml` modèle, puis cliquez sur Suivant. 3. Dans Spécifier les détails de la pile, spécifiez le nom de la pile, puis fournissez les valeurs suivantes pour les paramètres d'entrée : • `CodeBranchName` : nom de branche du CodeCommit dépôt où réside votre code • `EKSClusterName` : nom de votre cluster EKS (pas l'`EKSCluster` ID) • `EKSCodeBuildAppName` : nom de l'application Helm chart (`aws-proserve-java-greeting`) • `EKSWorkerNodeRoleARN` : ARN du rôle IAM attribué aux nœuds de travail Amazon EKS • `EKSWorkerNodeRoleName` : nom du rôle IAM attribué aux nœuds de travail Amazon EKS	

Tâche	Description	Compétences requises
	• `EcrDockerRepository` : nom du référentiel Amazon ECR dans lequel les images Docker de votre code seront stockées • `EmailRecipient` : adresse e-mail à laquelle les notifications de build doivent être envoyées • `EnvType`: Environnement (par exemple, dev, test ou prod) • `SourceRepoName` : nom du CodeCommit dépôt dans lequel se trouve votre code 4. Choisissez Suivant. Utilisez les paramètres par défaut dans Configurer les options de pile, puis choisissez Next. 5. Dans la section Révision, vérifiez les détails du CloudFormation modèle et de la pile, puis choisissez Next. 6. Sélectionnez Créer la pile. 7. Pendant le déploiement de la CloudFormation pile, le propriétaire de l'adresse e-mail que vous avez fournie dans les paramètre	

Tâche	Description	Compétences requises
	s recevra un message l'invitant à s'abonner à une rubrique SNS. Pour s'abonner à Amazon SNS, le propriétaire doit choisir le lien contenu dans le message. 8. Une fois la pile créée, ouvrez l'onglet Sorties de la pile, puis enregistrez la valeur ARN de la clé `EksCodeBuildkubeRoleARN` de sortie. Cette valeur d'ARN IAM sera requise ultérieurement lorsque vous autoriserez le rôle CodeBuild IAM à déployer des charges de travail dans le cluster Amazon EKS.	

Activer l'intégration entre Security Hub et Aqua Security

Tâche	Description	Compétences requises
Activez l'intégration d'Aqua Security.	Cette étape est nécessaire pour télécharger les résultats de vulnérabilité des images Docker signalés par Trivy vers Security Hub. Comme il AWS CloudFormation ne prend pas en charge les intégrations de Security Hub, ce processus	Administrateur AWS, DevOps ingénieur

Tâche	Description	Compétences requises
	doit être effectué manuellement. 1. Ouvrez la AWS Security Hub console et accédez à Integrations. 2. Recherchez Aqua Security, puis sélectionnez Aqua Security : Aqua Security. 3. Choisissez Accepter les résultats.	

Configurer CodeBuild pour exécuter les commandes Helm ou kubectl

Tâche	Description	Compétences requises
Permet CodeBuild d'exécuter des commandes Helm ou kubectl dans le cluster Amazon EKS.	CodeBuild Pour être authentifié afin d'utiliser Helm ou des `kubectl` commandes avec le cluster Amazon EKS, vous devez ajouter les rôles IAM au. `aws-auth` `ConfigMap` Dans ce cas, ajoutez l'ARN du rôle IAM`EksCodeBuildkubeRoleARN` , qui est le rôle IAM créé pour que le CodeBuild service accède au cluster Amazon EKS et y déploie des charges de travail. Il s'agit d'une activité ponctuelle.	DevOps

Tâche	Description	Compétences requises
	Important La procédure suivante doit être terminée avant la phase d'approbation du déploiement dans CodePipeline. 1. Ouvrez le script `cf_templates/kube_aws_auth_configmap_patch.sh` shell dans votre environnement Amazon Linux ou macOS. 2. Authentifiez-vous auprès du cluster Amazon EKS en exécutant la commande suivante. `aws eks --region <aws-region> update-kubeconfig --name <eks-cluster-name>` 3. Exécutez le script shell à l'aide de la commande suivante, en le `<rolearn-eks-codebuild-kubectl>` remplaçant par la valeur ARN `EksCodeBuildkubeRoleARN` que vous avez enregistrée précédemment.	

Tâche	Description	Compétences requises
	`bash cf_templates/kube_aws_auth_configmap_patch.sh <rolearn-eks-codebuild-kubectl>` `aws_authConfigMap` Il est configuré et l'accès est accordé.	

Valider le pipeline CI/CD

Tâche	Description	Compétences requises
Vérifiez que le pipeline CI/CD démarre automatiquement.	1. La phase de CodeSecurity scan du pipeline échoue généralement si Checkov détecte des vulnérabilités dans les graphiques Dockerfile ou Helm. Cependant, le but de cet exemple est d'établir un processus permettant d'identifier les vulnérabilités de sécurité potentielles plutôt que de les corriger par le biais du pipeline CI/CD, généralement un DevSecOps processus. Dans le fichier`buildspec/buildspec_secscan.yaml` , la `checkov` commande utilise l'`--`	DevOps

Tâche	Description	Compétences requises

	`soft-fail` indicateur pour éviter une défaillance du pipeline.
	
	`- echo -e "\n Running Dockerfile Scan"`
	`- checkov -f code/app/Dockerfile --framework dockerfile --soft-fail --summary-position bottom`
	`- echo -e "\n Running Scan of Helm Chart files"`
	`- cp -pv helm_charts/$EKS_CODEBUILD_APP_NAME/values.dev.yaml helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml`
	`- checkov -d helm_charts/$EKS_CODEBUILD_APP_NAME --framework helm --soft-fail --summary-position bottom`
	`- rm -rfv helm_charts/$EKS_CODEBUILD_APP_NAME/values.yaml`
	
	Pour que le pipeline échoue lorsque des vulnérabilités sont signalées pour les graphiques Dockerfile et Helm, l'`--soft-fail` option doit être supprimée de la `checkov`	

Tâche	Description	Compétences requises
	commande. Les développeurs ou les ingénieurs peuvent ensuite corriger les vulnérabilités et valider les modifications dans le référentiel du code CodeCommit source. 2. À l'instar de CodeSecurity Scan, la phase de compilation utilise Aqua Security Trivy pour identifier `HIGH` les vulnérabilités liées aux images `CRITICAL` Docker avant de transférer l'application vers Amazon ECR. `- AWS_REGION=$AWS_DEFAULT_REGION AWS_ACCOUNT_ID=$AWS_ACCOUNT_ID trivy -d image --no-progress --ignore-unfixed --exit-code 0 --severity HIGH,CRITICAL --format template --template "@securityhub/asff.tpl" -o securityhub/report.asff $AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/$IMAGE_REPO_NAME:$CODEBUILD_RESOLVED_SOURCE_VERSION` Dans cet exemple, le pipeline n'échoue pas	

Tâche	Description	Compétences requises
	lorsque des vulnérabilités d'image Docker sont signalées, car la `trivy` commande du `buildspec/buildspec.yml` fichier inclut l'indicateur **`--exit-code`** avec une valeur de`0`. Pour que le pipeline échoue lorsque `HIGH` des `CRTICAL` vulnérabilités sont signalées, modifiez la valeur de `--exit-code 1`. Les développeurs ou les ingénieurs peuvent ensuite corriger les vulnérabilités et valider les modifications dans le référentiel du code CodeCommit source. 3. Les vulnérabilités des images Docker signalées par Aqua Security Trivy sont téléchargées sur Security Hub. Sur la console Security Hub, accédez à Findings. Filtrez les résultats avec Record State = Active et Product = Aqua Security. Ceci répertorie les vulnérabilités liées aux images Docker dans Security Hub. L'apparition de vulnérabilités dans Security Hub peut	

Tâche	Description	Compétences requises
	prendre entre 15 minutes et une heure. Pour plus d'informations sur le démarrage du pipeline en utilisant CodePipeline, voir Démarrer un pipeline dansCodePipeline, Démarrer un pipeline manuellement et Démarrer un pipeline selon un calendrier dans la CodePipeline documentation.	

Tâche	Description	Compétences requises
Approuvez le déploiement.	1. Une fois la phase de construction terminée, il existe une porte d'approbation du déploiement. Le réviseur ou un responsable de version doit inspecter la version et, si toutes les exigences sont remplies, l'approuver. Il s'agit de l'approche recommandée pour les équipes qui utilisent la livraison continue pour le déploiement d'applications. 2. Après approbation, le pipeline lance la phase de déploiement. 3. Une fois la phase de déploiement réussie, le CodeBuild journal de cette étape fournit l'URL de l'application. Utilisez l'URL pour vérifier que l'application est prête.	DevOps

Tâche	Description	Compétences requises
Validez le profilage des applications.	Une fois le déploieme nt terminé et le module d'application déployé dans Amazon EKS, l'agent Amazon CodeGuru Profiler configuré dans l'application essaie d'envoyer les données de profilage de l'application (processeur, résumé du segment de mémoire, latence et goulots d'étranglement) à Profiler. CodeGuru Lors du déploiement initial d'une application, CodeGuru Profiler met environ 15 minutes à visualiser les données de profilage.	AWS DevOps

Ressources connexes

- AWS CodePipeline documentation
- Numérisation d'images avec Trivy dans un AWS CodePipeline (article de AWS blog)
- Améliorer vos applications Java à l'aide d'Amazon CodeGuru Profiler (article de AWS blog)
- AWS Syntaxe du format ASFF (Security Finding Format)
- Modèles d' EventBridge événements Amazon
- Mise à niveau du casque

Informations supplémentaires

- AWS CodeCommit n'est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus. Cette solution

fonctionnera également avec n'importe quel fournisseur Git de système de contrôle de version (VCS) tel que GitHub ou GitLab avec des modifications minimales.

- CodeGuru Profiler ne doit pas être confondu avec le AWS X-Ray service en termes de fonctionnalités. Nous vous recommandons d'utiliser CodeGuru Profiler pour identifier les lignes de code les plus coûteuses susceptibles de provoquer des blocages ou des problèmes de sécurité, et de les corriger avant qu'elles ne deviennent un risque potentiel. Le service X-Ray est destiné à la surveillance des performances des applications.
- Dans ce modèle, les règles d'événements sont associées au bus d'événements par défaut. Si nécessaire, vous pouvez étendre le modèle pour utiliser un bus d'événements personnalisé.
- Ce modèle utilise CodeGuru Reviewer comme outil de test statique de sécurité des applications (SAST) pour le code des applications. Vous pouvez également utiliser ce pipeline pour d'autres outils, tels que SonarQube Checkmarx. Vous pouvez ajouter les instructions de configuration de numérisation pour chacun de ces outils `buildspec/buildspec_secscan.yaml` afin de remplacer les instructions de CodeGuru numérisation.

Créez une définition de tâche Amazon ECS et montez un système de fichiers sur des EC2 instances à l'aide d'Amazon EFS

Créée par Durga Prasad Cheepuri (AWS)

Récapitulatif

Ce modèle fournit des exemples de code et des étapes pour créer une définition de tâche Amazon Elastic Container Service (Amazon ECS) qui s'exécute sur des instances Amazon Elastic Compute Cloud (EC2Amazon) dans le cloud Amazon Web Services (AWS), tout en utilisant Amazon Elastic File System (Amazon EFS) pour monter un système de fichiers sur EC2 ces instances. Les tâches Amazon ECS qui utilisent Amazon EFS montent automatiquement les systèmes de fichiers que vous spécifiez dans la définition de la tâche et mettent ces systèmes de fichiers à la disposition des conteneurs de la tâche dans toutes les zones de disponibilité d'une région AWS.

Pour répondre à vos exigences en matière de stockage persistant et de stockage partagé, vous pouvez utiliser Amazon ECS et Amazon EFS ensemble. Par exemple, vous pouvez utiliser Amazon EFS pour stocker des données utilisateur persistantes et des données d'application pour vos applications avec des paires de conteneurs ECS actifs et de secours exécutées dans différentes zones de disponibilité pour une haute disponibilité. Vous pouvez également utiliser Amazon EFS pour stocker des données partagées auxquelles les conteneurs ECS et les charges de travail distribuées peuvent accéder en parallèle.

Pour utiliser Amazon EFS avec Amazon ECS, vous pouvez ajouter une ou plusieurs définitions de volume à une définition de tâche. Une définition de volume inclut un identifiant de système de fichiers Amazon EFS, un identifiant de point d'accès et une configuration pour l'autorisation AWS Identity and Access Management (IAM) ou le chiffrement TLS (Transport Layer Security) en transit. Vous pouvez utiliser les définitions de conteneur dans les définitions de tâches pour spécifier les volumes de définition de tâches qui sont montés lors de l'exécution du conteneur. Lorsqu'une tâche utilisant un système de fichiers Amazon EFS s'exécute, Amazon ECS s'assure que le système de fichiers est monté et disponible pour les conteneurs qui ont besoin d'y accéder.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cloud privé virtuel (VPC) avec un point de terminaison de réseau privé virtuel (VPN) ou un routeur

- (Recommandé) L'agent de conteneur Amazon ECS 1.38.0 ou version ultérieure pour la compatibilité avec les points d'accès Amazon EFS et les fonctionnalités d'autorisation IAM (pour plus d'informations, consultez le billet de blog AWS New for Amazon EFS — IAM Authorization and Access Points.)

Limites

- Les versions de l'agent de conteneur Amazon ECS antérieures à la version 1.35.0 ne prennent pas en charge les systèmes de fichiers Amazon EFS pour les tâches utilisant le type de EC2 lancement.

Architecture

Le schéma suivant montre un exemple d'application qui utilise Amazon ECS pour créer une définition de tâche et monter un système de fichiers Amazon EFS sur des EC2 instances dans des conteneurs ECS.

Le schéma suivant illustre le flux de travail suivant :

1. Créez un système de fichiers Amazon EFS.
2. Créez une définition de tâche avec un conteneur.
3. Configurez les instances de conteneur pour monter le système de fichiers Amazon EFS. La définition de tâche fait référence aux montages de volumes, afin que l'instance de conteneur puisse utiliser le système de fichiers Amazon EFS. Les tâches ECS ont accès au même système de fichiers Amazon EFS, quelle que soit l'instance de conteneur sur laquelle elles ont été créées.
4. Créez un service Amazon ECS avec trois instances de la définition de tâche.

Pile technologique

- Amazon EC2
- Amazon ECS
- Amazon EFS

Outils

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que vous le souhaitez, et vous pouvez les étendre ou les intégrer.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif permettant d'exécuter, d'arrêter et de gérer des conteneurs sur un cluster. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate. Pour mieux contrôler votre infrastructure, vous pouvez également exécuter vos tâches et services sur un cluster d' EC2 instances que vous gérez.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) fournit un système de fichiers NFS élastique simple, évolutif et entièrement géré à utiliser avec les services cloud AWS et les ressources sur site.
- AWS CLI — L'interface de ligne de commande AWS (AWS CLI) est un outil open source permettant d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande. Avec une configuration minimale, vous pouvez exécuter des commandes de l'interface de ligne de commande AWS qui mettent en œuvre des fonctionnalités équivalentes à celles fournies par la console de gestion AWS basée sur un navigateur à partir d'une invite de commande.

Épopées

Créer un système de fichiers Amazon EFS

Tâche	Description	Compétences requises
Créez un système de fichiers Amazon EFS à l'aide de l'AWS Management Console.	1. **Note** Créez un système de fichiers Amazon EFS et choisissez le VPC qui inclut vos conteneurs. : Si vous utilisez un autre VPC, configurez une	AWS DevOps

Tâche	Description	Compétences requises
	connexion d'appairage VPC. 2. Notez l'ID du système de fichiers.	

Créez une définition de tâche Amazon ECS à l'aide d'un système de fichiers Amazon EFS ou de l'AWS CLI

Tâche	Description	Compétences requises
Créez une définition de tâche à l'aide d'un système de fichiers Amazon EFS.	Créez une définition de tâche à l'aide de la nouvelle console Amazon ECS ou de la console Amazon ECS classique avec les configurations suivantes : • Si vous utilisez la nouvelle console, choisissez les EC2 instances Amazon pour l'environnement d'applications. Si vous utilisez la console classique, choisissez EC2le type de lancement. • Ajoutez un volume. Entrez le nom du volume, choisissez EFS pour le type de volume, puis choisissez l'ID du système de fichiers que vous avez noté précédemment. Pour le répertoire racine, choisissez le chemin du système de fichiers Amazon EFS que vous	AWS DevOps

Tâche	Description	Compétences requises
	souhaitez héberger sur l'hôte du conteneur Amazon ECS.	

Tâche	Description	Compétences requises

Créez une définition de tâche à l'aide de l'interface de ligne de commande AWS.	1. Pour créer un modèle JSON avec des espaces réservés aux paramètres d'entrée pour la définition de votre tâche, exécutez la commande suivante :
	`aws ecs register-task-definition --generate-cli-skeleton`
	2. Pour créer la définition de tâche à l'aide du modèle JSON, exécutez la commande suivante :
	`aws ecs register-task-definition --cli-input-json file://<path_to_your_json_file>`
	3. **Note**
	Entrez les paramètres d'entrée dans votre modèle JSON en fonction du `task_definition_parameters.json` fichier (joint). : Pour plus d'informations sur les paramètres d'entrée, consultez les paramètres
		AWS DevOps

Tâche	Description	Compétences requises
	de définition des tâches (documentation Amazon ECS) et register-task-definition(Référence des commandes de l'AWS CLI).	

Ressources connexes

- Définitions des tâches Amazon ECS
- Volumes Amazon EFS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Déployer des fonctions Lambda avec des images de conteneurs

Créée par Ram Kandaswamy (AWS)

Récapitulatif

AWS Lambda prend en charge les images de conteneurs en tant que modèle de déploiement. Ce modèle montre comment déployer des fonctions Lambda via des images de conteneur.

Lambda est un service de calcul sans serveur piloté par les événements que vous pouvez utiliser pour exécuter du code pour pratiquement n'importe quel type d'application ou de service principal sans provisionner ni gérer de serveurs. Grâce à la prise en charge des images de conteneur pour les fonctions Lambda, vous bénéficiez de 10 Go de stockage maximum pour votre artefact d'application et de la possibilité d'utiliser des outils de développement d'images de conteneur familiers.

L'exemple de ce modèle utilise Python comme langage de programmation sous-jacent, mais vous pouvez utiliser d'autres langages, tels que Java, Node.js ou Go. Pour la source, considérez un système basé sur Git tel que GitHub GitLab, ou Bitbucket, ou utilisez Amazon Simple Storage Service (Amazon S3).

Conditions préalables et limitations

Prérequis

- Amazon Elastic Container Registry (Amazon ECR) activé
- Code de l'application
- Images Docker avec le client d'interface d'exécution et la dernière version de Python
- Connaissance pratique de Git

Limites

- La taille d'image maximale prise en charge est de 10 Go.
- Le temps d'exécution maximal d'un déploiement de conteneur basé sur Lambda est de 15 minutes.

Architecture

Architecture cible

1. Vous créez un dépôt Git et vous y validez le code de l'application.
2. Le AWS CodeBuild projet est déclenché par les modifications apportées aux validations.
3. Le CodeBuild projet crée l'image Docker et publie l'image créée sur Amazon ECR.
4. Vous créez la fonction Lambda à l'aide de l'image dans Amazon ECR.

Automatisation et mise à l'échelle

Ce modèle peut être automatisé à l'aide de AWS CloudFormation AWS Cloud Development Kit (AWS CDK), ou d'opérations d'API à partir d'un SDK. Lambda peut automatiquement évoluer en fonction du nombre de demandes, et vous pouvez l'ajuster à l'aide des paramètres de simultanéité. Pour plus d'informations, consultez la documentation Lambda.

Outils

Services AWS

- AWS CloudFormationAWS CloudFormationhelps vous permet de configurer les AWS ressources, de les approvisionner rapidement et de manière cohérente, et de les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS. Ce modèle utilise AWS CloudFormation Application Composer, qui vous permet de visualiser et de modifier visuellement les AWS CloudFormation modèles.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- GitHub, GitLab, et Bitbucket font partie des systèmes de contrôle de source basés sur Git les plus couramment utilisés pour suivre les modifications du code source.

Bonnes pratiques

- Rendez votre fonction aussi efficace et aussi petite que possible pour éviter de charger des fichiers inutiles.
- Efforcez-vous de placer les couches statiques plus haut dans votre liste de fichiers Docker et de placer les couches qui changent plus souvent plus bas. Cela améliore la mise en cache, ce qui améliore les performances.
- Le propriétaire de l'image est responsable de la mise à jour et des correctifs de l'image. Ajoutez cette cadence de mise à jour à vos processus opérationnels. Pour plus d'informations, consultez la documentation AWS Lambda.

Épopées

Créez un projet dans CodeBuild

Tâche	Description	Compétences requises
Créez un dépôt Git.	Créez un dépôt Git qui contiendra le code source de l'application, le Dockerfile et le `buildspec.yaml` fichier.	Developer
Créez un CodeBuild projet.	Pour utiliser un CodeBuild projet afin de créer l'image Lambda personnalisée, procédez comme suit : 1. Connectez-vous à la CodeBuild console et AWS Management Console ouvrez-la à l'adresse https://console.aws.amazon.com/codesuite/ codebuild/. 2. Crée un projet. Pour source, choisissez le dépôt Git que vous avez créé. Pour plus d'informations	Developer

Tâche	Description	Compétences requises
	sur les différents types d'intégration du référentiel Git, consultez la documentation relative à l'utilisation des connexions. 3. Vérifiez que le mode privilégié est activé. Pour créer des images Docker, cela est nécessaire. Dans le cas contraire, l'image ne sera pas créée correctement. 4. Entrez des valeurs pour le nom et la description du projet.	
Modifiez le Dockerfile.	Le Dockerfile doit se trouver dans le répertoire de premier niveau dans lequel vous développez l'application. Le code Python doit se trouver dans le `src` dossier. Lorsque vous créez l'image, utilisez les images officielles prises en charge par Lambda. Sinon, une erreur de démarrage se produira, rendant le processus d'emballage plus difficile. Pour plus de détails, consultez la section Informations supplémentaires.	Developer

Tâche	Description	Compétences requises
Créez un référentiel dans Amazon ECR.	Créez un référentiel de conteneurs dans Amazon ECR. Dans l'exemple de commande suivant, le nom du référentiel créé est `cf-demo` : `aws ecr create-repository --cf-demo` Le référentiel sera référencé dans le `buildspec.yaml` fichier.	Administrateur AWS, développeur
Poussez l'image vers Amazon ECR.	Vous pouvez l'utiliser CodeBuild pour exécuter le processus de création d'image. CodeBuild a besoin d'une autorisation pour interagir avec Amazon ECR et pour travailler avec S3. Dans le cadre du processus , l'image Docker est créée et envoyée au registre Amazon ECR. Pour plus de détails sur le modèle et le code, consultez la section Informations supplémentaires.	Developer

Tâche	Description	Compétences requises
Vérifiez que l'image se trouve dans le référentiel.	Pour vérifier que l'image se trouve dans le référentiel, sur la console Amazon ECR, sélectionnez Repositories. L'image doit être répertoriée, avec des balises et les résultats d'un rapport d'analyse des vulnérabilités si cette fonctionnalité a été activée dans les paramètres Amazon ECR. Pour plus d'informations, consultez la documentation AWS.	Developer

Créez la fonction Lambda pour exécuter l'image

Tâche	Description	Compétences requises
Créez la fonction Lambda.	Sur la console Lambda, choisissez Create function, puis choisissez Container image. Entrez le nom de la fonction et l'URI de l'image qui se trouve dans le référentiel Amazon ECR, puis choisissez Create function. Pour plus d'informations, consultez la documentation AWS Lambda.	Développeur d’applications
Testez la fonction Lambda.	Pour appeler et tester la fonction, choisissez Test. Pour plus d'informations, consultez la documentation AWS Lambda.	Développeur d’applications

Résolution des problèmes

Problème	Solution
La construction ne réussit pas.	1. Vérifiez si le mode privilégié est activé pour le CodeBuild projet. 2. Assurez-vous que les commandes associées à Docker disposent des autorisations nécessaires. J'essaie `sudo` d'ajouter des commandes. 3. Vérifiez que le rôle IAM associé CodeBuild dispose d'une politique comportant des actions appropriées pour interagir avec Amazon ECR, Amazon S3 et CloudWatch les journaux.

Ressources connexes

- Images de base pour Lambda
- Exemple Docker pour CodeBuild
- Transmettez des informations d'identification temporaires

Informations supplémentaires

Modifier le Dockerfile

Le code suivant montre les commandes que vous modifiez dans le Dockerfile :

```
FROM public.ecr.aws/lambda/python:3.xx

# Copy function code
COPY app.py ${LAMBDA_TASK_ROOT}
COPY requirements.txt  ${LAMBDA_TASK_ROOT}

# install dependencies
RUN pip3 install --user -r requirements.txt
```

```
# Set the CMD to your handler (could also be done as a parameter override outside of
 the Dockerfile)
CMD [ "app.lambda_handler" ]
```

Dans la `FROM` commande, utilisez la valeur appropriée pour la version de Python prise en charge par Lambda (par exemple,`3.12`). Il s'agira de l'image de base disponible dans le référentiel d'images public Amazon ECR.

La `COPY app.py ${LAMBDA_TASK_ROOT}` commande copie le code dans le répertoire racine de la tâche, que la fonction Lambda utilisera. Cette commande utilise la variable d'environnement afin que nous n'ayons pas à nous soucier du chemin réel. La fonction à exécuter est transmise en tant qu'argument à la `CMD [ "app.lambda_handler" ]` commande.

La `COPY requirements.txt` commande capture les dépendances nécessaires au code.

La `RUN pip install --user -r requirements.txt` commande installe les dépendances dans le répertoire utilisateur local.

Pour créer votre image, exécutez la commande suivante.

```
docker build -t <image name> .
```

Ajoutez l'image dans Amazon ECR

Dans le code suivant, remplacez-le `aws_account_id` par le numéro de compte, et remplacez-le `us-east-1` si vous utilisez une autre région. Le `buildspec` fichier utilise le numéro de CodeBuild version pour identifier de manière unique les versions d'image sous forme de valeur de balise. Vous pouvez le modifier en fonction de vos besoins.

Le code personnalisé buildspec

```
phases:
  install:
    runtime-versions:
       python: 3.xx
  pre_build:
    commands:
      - python3 --version
      - pip3 install --upgrade pip
      - pip3 install --upgrade awscli
      - sudo docker info
```

```
  build:
    commands:
      - echo Build started on `date`
      - echo Building the Docker image...
      - ls
      - cd app
      - docker build -t cf-demo:$CODEBUILD_BUILD_NUMBER .
      - docker container ls
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker image...
      - aws ecr get-login-password --region us-east-1 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-east-1.amazonaws.com
      - docker tag cf-demo:$CODEBUILD_BUILD_NUMBER aws_account_id.dkr.ecr.us-
east-1.amazonaws.com/cf-demo:$CODEBUILD_BUILD_NUMBER
      - docker push aws_account_id.dkr.ecr.us-east-1.amazonaws.com/cf-demo:
$CODEBUILD_BUILD_NUMBER
```

Déployez des microservices Java sur Amazon ECS à l'aide d'AWS Fargate

Créée par Vijay Thompson (AWS) et Sandeep Bondugula (AWS)

Récapitulatif

Ce modèle fournit des conseils pour le déploiement de microservices Java conteneurisés sur Amazon Elastic Container Service (Amazon ECS) à l'aide d'AWS Fargate. Le modèle n'utilise pas Amazon Elastic Container Registry (Amazon ECR) pour la gestion des conteneurs ; les images Docker sont plutôt extraites d'un hub Docker.

Conditions préalables et limitations

Prérequis

- Une application de microservices Java existante sur un hub Docker
- Un dépôt Docker public
- Un compte AWS actif
- Connaissance des services AWS, notamment Amazon ECS et Fargate
- Framework Docker, Java et Spring Boot
- Amazon Relational Database Service (Amazon RDS) est opérationnel (facultatif)
- Un cloud privé virtuel (VPC) si l'application nécessite Amazon RDS (facultatif)

Architecture

Pile technologique source

- Microservices Java (par exemple, implémentés dans Spring Boot) et déployés sur Docker

Architecture de la source

Pile technologique cible

- Un cluster Amazon ECS qui héberge chaque microservice à l'aide de Fargate
- Un réseau VPC pour héberger le cluster Amazon ECS et les groupes de sécurité associés
- Une définition de cluster/tâche pour chaque microservice qui lance des conteneurs à l'aide de Fargate

Architecture cible

Outils

Outils

- Amazon ECS élimine le besoin d'installer et d'exploiter votre propre logiciel d'orchestration de conteneurs, de gérer et de dimensionner un cluster de machines virtuelles ou de planifier des conteneurs sur ces machines virtuelles.
- AWS Fargate vous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou d'instances Amazon Elastic Compute Cloud (Amazon EC2). Il est utilisé conjointement avec Amazon Elastic Container Service (Amazon ECS).
- Docker est une plate-forme logicielle qui vous permet de créer, de tester et de déployer des applications rapidement. Docker regroupe les logiciels dans des unités standardisées appelées conteneurs qui contiennent tout ce dont le logiciel a besoin pour fonctionner, notamment les bibliothèques, les outils système, le code et le runtime.

Code Docker

Le Dockerfile suivant indique la version du kit de développement Java (JDK) utilisée, l'emplacement du fichier d'archive Java (JAR), le numéro de port exposé et le point d'entrée de l'application.

```
FROM openjdk:11
ADD target/Spring-docker.jar Spring-docker.jar
EXPOSE 8080
ENTRYPOINT ["java","-jar","Spring-docker.jar"]
```

Épopées

Création de nouvelles définitions de tâches

Tâche	Description	Compétences requises
Créez une définition de tâche.	L'exécution d'un conteneur Docker dans Amazon ECS nécessite une définition de tâche. Ouvrez la console	Administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
	Amazon ECS à l'https://console.aws.amazon.com/ecs/adresse, choisissez Définitions de tâches, puis créez une nouvelle définition de tâche. Pour plus d'informations, consultez la documentation Amazon ECS.	
Choisissez le type de lancement.	Choisissez Fargate comme type de lancement.	Administrateur système AWS, développeur d'applications
Configurez la tâche.	Définissez un nom de tâche et configurez l'application avec la quantité appropriée de mémoire de tâche et de processeur.	Administrateur système AWS, développeur d'applications
Définissez le conteneur.	Spécifiez le nom du conteneur. Pour l'image, entrez le nom du site Docker, le nom du référentiel et le nom de balise de l'image Docker ()`docker.io/sample-repo/sample-application:sample-tag-name` . Définissez les limites de mémoire pour l'application et définissez les mappages de ports (`8080, 80`) pour les ports autorisés.	Administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
Créez la tâche.	Lorsque les configurations de tâche et de conteneur sont en place, créez la tâche. Pour obtenir des instructions détaillées, consultez les liens dans la section Ressources connexes.	Administrateur système AWS, développeur d'applications

Configuration du cluster

Tâche	Description	Compétences requises
Créez et configurez un cluster.	Choisissez Networking only comme type de cluster, configurez le nom, puis créez le cluster ou utilisez un cluster existant s'il est disponible. Pour plus d'informations, consultez la documentation Amazon ECS.	Administrateur système AWS, développeur d'applications

Configurer la tâche

Tâche	Description	Compétences requises
Créez une tâche.	Dans le cluster, choisissez Exécuter une nouvelle tâche.	Administrateur système AWS, développeur d'applications
Choisissez le type de lancement.	Choisissez Fargate comme type de lancement.	Administrateur système AWS, développeur d'applications
Choisissez la définition de la tâche, la révision et la version de la plateforme.	Choisissez la tâche que vous souhaitez exécuter, la révision	Administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
	de la définition de la tâche et la version de la plateforme.	
Sélectionnez le cluster .	Choisissez le cluster à partir duquel vous souhaitez exécuter la tâche.	Administrateur système AWS, développeur d'applications
Spécifiez le nombre de tâches.	Configurez le nombre de tâches à exécuter. Si vous lancez deux tâches ou plus, un équilibreur de charge est nécessaire pour répartir le trafic entre les tâches.	Administrateur système AWS, développeur d'applications
Spécifiez le groupe de tâches.	(Facultatif) Spécifiez un nom de groupe de tâches pour identifier un ensemble de tâches connexes en tant que groupe de tâches.	Administrateur système AWS, développeur d'applications
Configurez le VPC, les sous-réseaux et les groupes de sécurité du cluster.	Configurez le VPC du cluster et les sous-réseaux sur lesquels vous souhaitez déployer l'application. Créez ou mettez à jour des groupes de sécurité (HTTP, HTTPS et port 8080) pour fournir un accès aux connexions entrantes et sortantes.	Administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
Configurez les paramètres IP publics.	Activez ou désactivez l'adresse IP publique, selon que vous souhaitez ou non utiliser une adresse IP publique pour les tâches Fargate. L'option recommandée par défaut est Activé.	Administrateur système AWS, développeur d'applications
Vérifiez les paramètres et créez la tâche	Vérifiez vos paramètres, puis choisissez Exécuter la tâche.	Administrateur système AWS, développeur d'applications

Découper

Tâche	Description	Compétences requises
Copiez l'URL de l'application.	Lorsque le statut de la tâche est passé à En cours d'exécution, sélectionnez la tâche. Dans la section Mise en réseau, copiez l'adresse IP publique.	Administrateur système AWS, développeur d'applications
Testez votre application.	Dans votre navigateur, saisissez l'adresse IP publique pour tester l'application.	Administrateur système AWS, développeur d'applications

Ressources connexes

- Principes de base de Docker pour Amazon ECS (documentation Amazon ECS)
- Amazon ECS sur AWS Fargate (documentation Amazon ECS)
- Création d'une définition de tâche (documentation Amazon ECS)
- Création d'un cluster (documentation Amazon ECS)
- Configuration des paramètres de service de base (documentation Amazon ECS)

- Configuration d'un réseau (documentation Amazon ECS)
- Déploiement de microservices Java sur Amazon ECS (article de blog)

Déployez des ressources et des packages Kubernetes à l'aide d'Amazon EKS et d'un référentiel de diagrammes Helm dans Amazon S3

Créée par Sagar Panigrahi (AWS)

Récapitulatif

Ce modèle vous permet de gérer efficacement les applications Kubernetes, quelle que soit leur complexité. Le modèle intègre Helm à vos pipelines d'intégration continue et de livraison continue (CI/CD) existants pour déployer des applications dans un cluster Kubernetes. Helm est un gestionnaire de packages Kubernetes qui vous aide à gérer les applications Kubernetes. Les diagrammes Helm permettent de définir, d'installer et de mettre à niveau des applications Kubernetes complexes. Les graphiques peuvent être versionnés et stockés dans les référentiels Helm, ce qui améliore le temps moyen de restauration (MTTR) en cas de panne.

Ce modèle utilise Amazon Elastic Kubernetes Service (Amazon EKS) pour le cluster Kubernetes. Il utilise Amazon Simple Storage Service (Amazon S3) comme référentiel de diagrammes Helm, afin que les graphiques puissent être gérés de manière centralisée et accessibles aux développeurs de l'entreprise.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif avec un cloud privé virtuel (VPC)
- Un cluster Amazon EKS
- Nœuds de travail configurés au sein du cluster Amazon EKS et prêts à prendre en charge des charges de travail
- Kubectl pour configurer le fichier kubeconfig d'Amazon EKS pour le cluster cible sur la machine cliente
- Accès à AWS Identity and Access Management (IAM) pour créer le compartiment S3
- Accès IAM (par programmation ou par rôle) à Amazon S3 depuis la machine cliente
- Gestion du code source et pipeline CI/CD

Limites

- Il n'existe actuellement aucun support pour la mise à niveau, la suppression ou la gestion des définitions de ressources personnalisées (CRDs).
- Si vous utilisez une ressource qui fait référence à un CRD, le CRD doit être installé séparément (en dehors du graphique).

Versions du produit

- Casque v3.6.3

Architecture

Pile technologique cible

- Amazon EKS
- Amazon VPC
- Amazon S3
- Gestion du code source
- Helm
- Kubectl

Architecture cible

Automatisation et mise à l'échelle

- AWS CloudFormation peut être utilisé pour automatiser la création de l'infrastructure. Pour plus d'informations, consultez la section Création de ressources Amazon EKS avec AWS CloudFormation dans la documentation Amazon EKS.
- Helm doit être intégré à votre outil d'automatisation CI/CD existant pour automatiser le packaging et la gestion des versions des graphiques Helm (hors de portée de ce modèle).
- GitVersion ou les numéros de version de Jenkins peuvent être utilisés pour automatiser le versionnement des graphiques.

Outils

Outils

- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré permettant d'exécuter Kubernetes sur AWS sans avoir à configurer ou à gérer votre propre plan de contrôle Kubernetes. Kubernetes est un système open source destiné à l'automatisation du déploiement, la mise à l'échelle et la gestion d'applications conteneurisées.
- Helm — Helm est un gestionnaire de packages pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- Kubectl — Kubectl est un utilitaire de ligne de commande permettant d'exécuter des commandes sur des clusters Kubernetes.

Code

L'exemple de code est joint en pièce jointe.

Épopées

Configuration et initialisation de Helm

Tâche	Description	Compétences requises
Installez le client Helm.	Pour télécharger et installer le client Helm sur votre système local, utilisez la commande suivante. `sudo curl https://raw.githubusercontent.com/helm/helm/master/scripts/get-helm-3 | bash`	DevOps ingénieur

Tâche	Description	Compétences requises
Validez l'installation de Helm.	Pour vérifier que Helm est capable de communiqu er avec le serveur d'API Kubernetes au sein du cluster Amazon EKS, exécutez. `helm version`	DevOps ingénieur

Création et installation d'un graphique Helm dans le cluster Amazon EKS

Tâche	Description	Compétences requises
Créez un graphique Helm pour NGINX.	Pour créer un graphique de barre nommé `my-nginx` sur la machine cliente, exécutez`helm create my-nginx`.	DevOps ingénieur
Passez en revue la structure du graphique.	Pour revoir la structure du graphique, exécutez la commande d'arbores cence`tree my-nginx/` .	DevOps ingénieur
Désactivez la création de comptes de service dans le graphique.	Dans`values.yaml` , sous la `serviceAccount` section, réglez la `create` clé sur`false`. Cette option est désactivée car il n'est pas nécessaire de créer un compte de service pour ce modèle.	DevOps ingénieur
Validez (lint) le graphique modifié pour détecter les erreurs syntaxiques.	Pour valider le graphique afin de détecter toute erreur syntaxique avant de l'install er dans le cluster cible,	DevOps ingénieur

Tâche	Description	Compétences requises
	exécutez`helm lint my-nginx/` .	
Installez le graphique pour déployer les ressources Kubernetes.	Pour exécuter l'installation du graphique Helm, utilisez la commande suivante. `helm install --name my-nginx-release --debug my-nginx/ --namespace helm-space` L'`debug`indicateur facultatif affiche tous les messages de débogage pendant l'installation. L'`namespace` indicateur indique l'espace de noms dans lequel la partie ressources de ce graphique sera créée.	DevOps ingénieur
Passez en revue les ressources du cluster Amazon EKS.	Pour consulter les ressources créées dans le cadre du graphique Helm dans l'espace de `helm-space` noms, utilisez la commande suivante. `kubectl get all -n helm-space`	DevOps ingénieur

Revenir à une version précédente d'une application Kubernetes

Tâche	Description	Compétences requises
Modifiez et mettez à niveau la version.	Pour modifier le graphique, dans `values.yaml`, remplacez la `replicaCount` valeur par2. Mettez ensuite à niveau la version déjà installée en exécutant la commande suivante. `helm upgrade my-nginx-release my-nginx/ --namespace helm-space`	DevOps ingénieur
Consultez l'historique de la version de Helm.	Pour répertorier toutes les révisions d'une version spécifique qui ont été installées à l'aide de Helm, exécutez la commande suivante. `helm history my-nginx-release`	DevOps ingénieur
Passez en revue les détails d'une révision spécifique.	Avant de passer ou de revenir à une version fonctionnelle, et pour une couche de validation supplémentaire avant d'installer une révision, visualisez les valeurs transmises à chacune des révisions à l'aide de la commande suivante. `helm get --revision=2 my-nginx-release`	DevOps ingénieur

Tâche	Description	Compétences requises
Retournez à une version précédente.	Pour revenir à une révision précédente, utilisez la commande suivante. `helm rollback my-nginx-release 1` Cet exemple revient à la révision numéro 1.	DevOps ingénieur

Initialisation d'un compartiment S3 en tant que référentiel Helm

Tâche	Description	Compétences requises
Créez un compartiment S3 pour les diagrammes Helm.	Créez un compartiment S3 unique. Dans le compartiment, créez un dossier appelé`charts`. L'exemple de ce modèle utilise `s3://my-helm-charts/charts` comme référentiel graphique cible.	Administrateur du cloud
Installez le plugin Helm pour Amazon S3.	Pour installer le plugin helm-s3 sur votre machine cliente, utilisez la commande suivante. `helm plugin install https://github.com/hypnoglow/helm-s3.git --version 0.10.0` Remarque : le support de Helm V3 est disponible avec la	DevOps ingénieur

Tâche	Description	Compétences requises
	version 0.9.0 et supérieure du plugin.	
Initialisez le référentiel Amazon S3 Helm.	Pour initialiser le dossier cible en tant que référentiel Helm, utilisez la commande suivante. `helm S3 init s3://my-helm-charts/charts` La commande crée un `index.yaml` fichier dans la cible pour suivre toutes les informations du graphique stockées à cet emplacement.	DevOps ingénieur
Ajoutez le référentiel Amazon S3 à Helm.	Pour ajouter le référentiel sur l'ordinateur client, utilisez la commande suivante. `helm repo add my-helm-charts s3://my-helm-charts/charts` Cette commande ajoute un alias au référentiel cible sur la machine cliente Helm.	DevOps ingénieur
Consultez la liste des référentiels.	Pour afficher la liste des référentiels de la machine cliente Helm, exécutez`helm repo list`.	DevOps ingénieur

Package et stockage des graphiques dans le référentiel Amazon S3 Helm

Tâche	Description	Compétences requises
Empaquetez le graphique.	Pour `my-nginx` empaqueter le graphique que vous avez créé, exécutez`helm package ./my-nginx/` . La commande regroupe tout le contenu du dossier `my-nginx` graphique dans un fichier d'archive, nommé en utilisant le numéro de version mentionné dans le `Chart.yaml` fichier.	DevOps ingénieur
Stockez le package dans le référentiel Amazon S3 Helm.	Pour télécharger le package dans le référentiel Helm d'Amazon S3, exécutez la commande suivante en utilisant le nom correct du `.tgz` fichier. `helm s3 push ./my-nginx-0.1.0.tgz my-helm-charts`	DevOps ingénieur
Recherchez le graphique Helm.	Pour vérifier que le graphique apparaît à la fois localement et dans le référentiel Helm d'Amazon S3, exécutez la commande suivante. `helm search repo my-nginx`	DevOps ingénieur

Modifier, versionner et empaqueter un graphique

Tâche	Description	Compétences requises
Modifiez et empaquetez le graphique.	Dans`values.yaml` , définissez la `replicaCount` valeur sur`1`. Ensuite, empaquetez le graphique en l'exécutant`helm package ./my-nginx/` , en changeant cette fois la version `Chart.yaml` en`0.1.1`. Le versionnement est idéalement mis à jour grâce à l'automatisation à l'aide d'outils tels que GitVersion les numéros de build Jenkins dans un pipeline CI/CD. L'automatisation du numéro de version n'est pas couverte par ce modèle.	DevOps ingénieur
Transférez la nouvelle version vers le référentiel Helm d'Amazon S3.	Pour transférer le nouveau package avec la version 0.1.1 vers le référentiel `my-helm-charts` Helm d'Amazon S3, exécutez la commande suivante. `helm s3 push ./my-nginx-0.1.1.tgz my-helm-charts`	DevOps ingénieur

Recherchez et installez un graphique depuis le référentiel Amazon S3 Helm

Tâche	Description	Compétences requises
Recherchez toutes les versions du graphique my-nginx.	Pour afficher toutes les versions disponibles d'un graphique, exécutez la commande suivante avec l'`--versions` indicateur. `helm search repo my-nginx --versions` Sans le drapeau, Helm affiche par défaut la dernière version téléchargée d'un graphique.	DevOps ingénieur
Installez un graphique depuis le référentiel Amazon S3 Helm.	Les résultats de la recherche de la tâche précédente montrent les différentes versions du `my-nginx` graphique. Pour installer la nouvelle version (0.1.1) depuis le référentiel Amazon S3 Helm, utilisez la commande suivante. `helm upgrade my-nginx-release my-helm-charts/my-nginx --version 0.1.1 --namespace helm-space`	DevOps ingénieur

Ressources connexes

- Documentation HELM
- plugin helm-s3 (licence MIT)

- Binaire du client HELM
- Documentation Amazon EKS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Déployez un exemple de microservice Java sur Amazon EKS et exposez le microservice à l'aide d'un Application Load Balancer

Créée par Vijay Thompson (AWS) et Akkamahadevi Hiremath (AWS)

Récapitulatif

Ce modèle décrit comment déployer un exemple de microservice Java en tant qu'application conteneurisée sur Amazon Elastic Kubernetes Service (Amazon EKS) à l'`eksctl`aide de l'utilitaire de ligne de commande et d'Amazon Elastic Container Registry (Amazon ECR). Vous pouvez utiliser un Application Load Balancer pour équilibrer la charge du trafic des applications.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI) version 1.7 ou ultérieure, installée et configurée sur macOS, Linux ou Windows
- Un démon Docker en cours d'exécution
- L'utilitaire de ligne de `eksctl` commande, installé et configuré sous macOS, Linux ou Windows (pour plus d'informations, consultez Getting started with Amazon EKS — eksctl dans la documentation Amazon EKS.)
- L'utilitaire de ligne de `kubectl` commande, installé et configuré sous macOS, Linux ou Windows (pour plus d'informations, consultez Installation ou mise à jour de kubectl dans la documentation Amazon EKS.)

Limites

- Ce modèle ne couvre pas l'installation d'un certificat SSL pour l'Application Load Balancer.

Architecture

Pile technologique cible

- Amazon ECR
- Amazon EKS

- Elastic Load Balancing

Architecture cible

Le schéma suivant montre une architecture permettant de conteneuriser un microservice Java sur Amazon EKS.

Outils

- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles, telles que les instances, les conteneurs et les adresses IP Amazon Elastic Compute Cloud (Amazon EC2), dans une ou plusieurs zones de disponibilité.
- eksctl vous aide à créer des clusters sur Amazon EKS.
- kubectl permet d'exécuter des commandes sur des clusters Kubernetes.
- Docker vous permet de créer, de tester et de fournir des applications dans des packages appelés conteneurs.

Épopées

Créez un cluster Amazon EKS à l'aide de eksctl

Tâche	Description	Compétences requises
Créez un cluster Amazon EKS.	Pour créer un cluster Amazon EKS qui utilise deux EC2 instances Amazon t2.small comme nœuds, exécutez la commande suivante :	Développeur, administrateur système

Tâche	Description	Compétences requises
	`eksctl create cluster --name <your-cluster-name> --version <version-number> --nodes=1 --node-type=t2.small` **Note** Le processus peut prendre entre 15 et 20 minutes. Une fois le cluster créé, la configuration Kubernetes appropriée est ajoutée à votre fichier kubeconfig. Vous pouvez utiliser le `kubeconfig` fichier avec `kubectl` pour déployer l'application ultérieurement.	
Vérifiez le cluster Amazon EKS.	Pour vérifier que le cluster est créé et que vous pouvez vous y connecter, exécutez la `kubectl get nodes` commande.	Développeur, administrateur système

Créez un référentiel Amazon ECR et envoyez l'image Docker.

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR.	Suivez les instructions de la section Création d'un référenti	Développeur, administrateur système

Tâche	Description	Compétences requises
	el privé dans la documentation Amazon ECR.	
Créez un fichier XML POM.	Créez un `pom.xml` fichier basé sur l'exemple de code de fichier POM dans la section Informations supplémentaires de ce modèle.	Développeur, administrateur système

Tâche	Description	Compétences requises

Créez un fichier source.	Créez un fichier source appelé `HelloWorld.java` dans le `src/main/java/eksExample` chemin en vous basant sur l'exemple suivant :
	`package eksExample;`
	`import static spark.Spark.get;`
	
	`public class HelloWorld {`
	`  public static void main(String[] args) {`
	`  get("/", (req, res) -> {`
	`  return "Hello World!";`
	`  });`
	`  }`
	`}`
	
	Veillez à utiliser la structure de répertoire suivante :
	`### Dockerfile`
	`### deployment.yaml`
	`### ingress.yaml`
	`### pom.xml`
	`### service.yaml`
	`### src`
	`  ### main`
	`  ### java`
	`  ### eksExample`
	`  ### HelloWorld.java`	

Tâche	Description	Compétences requises
Créez un fichier Dockerfile.	Créez un code `Dockerfile` basé sur l'exemple de code Dockerfile dans la section Informations supplémentaires de ce modèle.	Développeur, administrateur système

Tâche	Description	Compétences requises

Créez et publiez l'image Docker.	Dans le répertoire dans lequel vous souhaitez `Dockerfile` créer, étiqueter et transférer l'image vers Amazon ECR, exécutez les commandes suivantes :
	`aws ecr get-login -password --region <region>| docker login --username <username> --password-stdin <account_number>.dkr.ecr.<region>.amazonaws.com`
	`docker buildx build --platform linux/amd64 -t hello-world-java:v1 .`
	`docker tag hello-world-java:v1 <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	`docker push <account_number>.dkr.ecr.<region>.amazonaws.com/<repository_name>:v1`
	Note
	Modifiez la région AWS, le numéro de compte et les détails du référentiel dans les commandes précédentes. N'oubliez pas de noter l'URL de l'image	

Tâche	Description	Compétences requises
	pour une utilisation ultérieure. **Important** Un système macOS doté d'une puce M1 ne parvient pas à créer une image compatibl e avec Amazon EKS exécuté sur une AMD64 plate-forme. Pour résoudre ce problème, utilisez docker buildx pour créer une image Docker qui fonctionne sur Amazon EKS.	

Déployez les microservices Java

Tâche	Description	Compétences requises
Créez un fichier de déploieme nt.	Créez un fichier YAML appelé en `deployment.yaml` fonction de l'exemple de code de fichier de déploieme nt dans la section Informati ons supplémentaires de ce modèle.	Développeur, administrateur système

Tâche	Description	Compétences requises
	Note Utilisez l'URL de l'image que vous avez copiée précédemm ent comme chemin du fichier image pour le référentiel Amazon ECR.	
Déployez les microservices Java sur le cluster Amazon EKS.	Pour créer un déploiement dans votre cluster Amazon EKS, exécutez la `kubectl apply -f deploymen t.yaml` commande.	Développeur, administrateur système
Vérifiez l'état des capsules.	1. Pour vérifier l'état des pods, exécutez la `kubectl get pods` commande. 2. Attendez que le statut passe à Prêt.	Développeur, administrateur système
Créer un service.	1. Créez un fichier appelé `service.yaml` en fonction de l'exemple de code de fichier de service figurant dans la section Informations supplémen taires de ce modèle. 2. Exécutez la commande `kubectl apply -f service.yaml .`	Développeur, administrateur système

Tâche	Description	Compétences requises
Installez le module complémentaire AWS Load Balancer Controller.	Suivez les instructions de la section Installation du module complémentaire AWS Load Balancer Controller dans la documentation Amazon EKS. **Note** Le module complémentaire doit être installé pour créer un Application Load Balancer ou un Network Load Balancer pour un service Kubernetes.	Développeur, administrateur système
Créez une ressource d'entrée.	Créez un fichier YAML appelé en `ingress.yaml` fonction de l'exemple de code de fichier de ressource d'entrée dans la section Informations supplémentaires de ce modèle.	Développeur, administrateur système
Créez un Application Load Balancer.	Pour déployer la ressource d'entrée et créer un Application Load Balancer, exécutez `kubectl apply -f ingress.yaml` la commande.	Développeur, administrateur système

Tester l'application

Tâche	Description	Compétences requises
Testez et vérifiez l'application.	1. Pour obtenir le nom DNS de l'équilibreur de charge à partir du champ ADDRESS, exécutez la `kubectl get ingress.networking.k8s.io/java-microservice-ingress` commande. 2. Sur une EC2 instance du même VPC que vos nœuds Amazon EKS, exécutez la `curl -v <DNS address from previous command>` commande.	Développeur, administrateur système

Ressources connexes

- Création d'un référentiel privé (documentation Amazon ECR)
- Transférer une image Docker (documentation Amazon ECR)
- Contrôleurs d'entrée (Amazon EKS Workshop)
- Docker buildx (Docker docs)

Informations supplémentaires

Exemple de fichier POM

```
<?xml version="1.0" encoding="UTF-8"?>
<project xmlns="http://maven.apache.org/POM/4.0.0" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
  xsi:schemaLocation="http://maven.apache.org/POM/4.0.0 http://maven.apache.org/xsd/
maven-4.0.0.xsd">
```

```
  <modelVersion>4.0.0</modelVersion>


  <groupId>helloWorld</groupId>
  <artifactId>helloWorld</artifactId>
  <version>1.0-SNAPSHOT</version>


  <dependencies>
    <dependency>
      <groupId>com.sparkjava</groupId><artifactId>spark-core</
artifactId><version>2.0.0</version>
    </dependency>
  </dependencies>
  <build>
    <plugins>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-jar-plugin</
artifactId><version>2.4</version>
        <configuration><finalName>eksExample</finalName><archive><manifest>
              <addClasspath>true</addClasspath><mainClass>eksExample.HelloWorld</
mainClass><classpathPrefix>dependency-jars/</classpathPrefix>
            </manifest></archive>
        </configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-compiler-plugin</
artifactId><version>3.1</version>
        <configuration><source>1.8</source><target>1.8</target></configuration>
      </plugin>
      <plugin>
        <groupId>org.apache.maven.plugins</groupId><artifactId>maven-assembly-plugin</
artifactId>
        <executions>
          <execution>
            <goals><goal>attached</goal></goals><phase>package</phase>
            <configuration>
              <finalName>eksExample</finalName>
              <descriptorRefs><descriptorRef>jar-with-dependencies</descriptorRef></
descriptorRefs>
              <archive><manifest><mainClass>eksExample.HelloWorld</mainClass></
manifest></archive>
            </configuration>
          </execution>
```

```
        </executions>
      </plugin>
    </plugins>
  </build>
</project>
```

Exemple de Dockerfile

```
FROM bellsoft/liberica-openjdk-alpine-musl:17

RUN apk add maven
WORKDIR /code

# Prepare by downloading dependencies
ADD pom.xml /code/pom.xml
RUN ["mvn", "dependency:resolve"]
RUN ["mvn", "verify"]

# Adding source, compile and package into a fat jar
ADD src /code/src
RUN ["mvn", "package"]

EXPOSE 4567
CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]
```

Exemple de fichier de déploiement

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 2
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      containers:
      - name: java-microservice-container
```

```
        image: .dkr.ecr.amazonaws.com/:
        ports:
        - containerPort: 4567
```

Exemple de fichier de service

```
apiVersion: v1
kind: Service
metadata:
  name: "service-java-microservice"
spec:
  ports:
    - port: 80
      targetPort: 4567
      protocol: TCP
  type: NodePort
  selector:
    app.kubernetes.io/name: java-microservice
```

Exemple de fichier de ressources d'entrée

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: "java-microservice-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/load-balancer-name: apg2
    alb.ingress.kubernetes.io/target-type: ip
  labels:
    app: java-microservice
spec:
  rules:
    - http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              service:
                name: "service-java-microservice"
                port:
                  number: 80
```

Déployez une application en cluster sur Amazon ECS à l'aide d'AWS Copilot

Créée par Jean-Baptiste Guillois (AWS), Mathew George (AWS) et Thomas Scott (AWS)

Récapitulatif

Ce modèle montre comment déployer des conteneurs dans un cluster Amazon Elastic Container Service (Amazon ECS) de deux manières : en utilisant la console de gestion Amazon Web Services (AWS) et en utilisant AWS CoPilot, afin de montrer comment AWS Copilot simplifie les tâches de déploiement.

Amazon ECS est un service de gestion de conteneurs rapide et hautement évolutif qui facilite l'exécution, l'arrêt et la gestion des conteneurs sur un cluster. Vos conteneurs sont définis dans une définition de tâche qui vous sert à exécuter des tâches individuelles ou des tâches dans un service. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate. Pour mieux contrôler votre infrastructure, vous pouvez également exécuter vos tâches et services sur un cluster d'instances Amazon Elastic Compute Cloud (Amazon EC2) que vous gérez.

Les commandes de l'interface de ligne de commande (CLI) AWS Copilot simplifient la création, le lancement et l'exploitation d'applications conteneurisées prêtes pour la production sur Amazon ECS à partir d'un environnement de développement local. La CLI AWS Copilot s'aligne sur les flux de travail des développeurs qui prennent en charge les meilleures pratiques en matière d'applications modernes : de l'utilisation de l'infrastructure sous forme de code à la création d'un pipeline d'intégration et de livraison continues (CI/CD) provisionné pour le compte d'un utilisateur. Vous pouvez utiliser l'interface de ligne de commande AWS Copilot dans le cadre de votre cycle quotidien de développement et de test comme alternative à l'AWS Management Console.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI) installée localement et configurée pour utiliser votre compte AWS (consultez les instructions d'installation et les instructions de configuration dans la documentation de l'AWS CLI)
- AWS Copilot installé localement (consultez les instructions d'installation dans la documentation Amazon ECS)

- Docker installé sur votre machine locale (voir la documentation Docker)

Limites

- Docker applique des limites d'extraction de 100 images de conteneur par 6 heures et par adresse IP dans le cadre du forfait gratuit.

Architecture

Pile technologique cible

- Environnement AWS configuré avec un cloud privé virtuel (VPC), des sous-réseaux publics et privés et des groupes de sécurité
- Cluster Amazon ECS
- Définition du service et des tâches Amazon ECS
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon DynamoDB
- Application Load Balancer
- AWS Fargate
- Amazon Identity and Access Management (IAM) (IAM)
- Amazon CloudWatch
- AWS CloudTrail

Architecture cible

Lorsque vous déployez l'exemple d'application pour ce modèle, plusieurs tâches sont créées et déployées dans des zones de disponibilité distinctes. Chaque tâche stocke les données dans Amazon DynamoDB. Lorsque vous accédez à la page Web d'une tâche, vous pouvez consulter les données de toutes les autres tâches.

Outils

Services AWS

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs géré par AWS qui est sécurisé, évolutif et fiable. Amazon ECR prend en charge les référentiels privés avec des autorisations basées sur les ressources à l'aide d' IAM.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif permettant d'exécuter, d'arrêter et de gérer des conteneurs sur un cluster. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate. Pour mieux contrôler votre infrastructure, vous pouvez également exécuter vos tâches et services sur un cluster d'instances Amazon Elastic Compute Cloud (Amazon EC2) que vous gérez.
- AWS Copilot — AWS Copilot fournit une interface de ligne de commande qui vous aide à lancer et à gérer des applications conteneurisées sur AWS, notamment en les transférant vers un registre, en créant une définition de tâche et en créant un cluster.
- AWS Fargate — AWS Fargate est un moteur de calcul pay-as-you-go sans serveur qui vous permet de vous concentrer sur le développement d'applications sans gérer de serveurs. AWS Fargate est compatible avec Amazon ECS et Amazon Elastic Kubernetes Service (Amazon EKS). Lorsque vous exécutez vos tâches et services Amazon ECS avec le type de lancement Fargate ou un fournisseur de capacité Fargate, vous créez le package de votre application dans des conteneurs, spécifiez les besoins en CPU et mémoire, définissez les stratégies réseaux et IAM, et vous lancez l'application. Chaque tâche Fargate possède sa propre limite d'isolation et ne partage pas le noyau sous-jacent, les ressources du processeur, les ressources de mémoire ou l'interface elastic network avec une autre tâche.
- Amazon DynamoDB — Amazon DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité sans faille.
- Elastic Load Balancing (ELB) — Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles, telles que les EC2 instances, les conteneurs et les adresses IP, dans une ou plusieurs zones de disponibilité. Il contrôle l'état des cibles enregistrées et achemine le trafic uniquement vers les cibles saines. Elastic Load Balancing met à l'échelle votre équilibreur de charge à mesure que votre trafic entrant change au fil du temps. Il est capable de s'adapter automatiquement à la plupart des applications.

Outils

- Interface de ligne de commande Docker
- Interface de ligne de commande AWS (AWS CLI)

- Interface de ligne de commande AWS Copilot

Code

Le code de l'exemple d'application utilisé dans ce modèle est disponible sur GitHub, dans le référentiel Cluster Sample Application. Suivez les instructions de la section suivante pour utiliser les fichiers d'exemple.

Épopées

Déployer la pile d'applications : option 1 (AWS Management Console)

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Clonez le référentiel d'exemples de code à l'aide de la commande : `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	Développeur d'applications, AWS DevOps
Créez votre référentiel Amazon ECR.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon ECR dans les https://console.aws.amazon.com/ecr/référentiels. 2. Choisissez Créer un référentiel. 3. Pour le nom du référentiel, entrez cluster-sample-app. 4. Pour tous les autres paramètres, conservez les valeurs par défaut.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	5. Choisissez Créer un référentiel. Pour plus d'informations, consultez la section Création d'un référentiel privé dans la documentation Amazon ECR.	

Tâche	Description	Compétences requises

Créez, balisez et transférez votre image Docker dans votre référentiel Amazon ECR.	1. Sélectionnez le référentiel que vous venez de créer et choisissez Afficher les commandes push.
	2. Copiez les commandes affichées et exécutez-les localement pour créer, étiqueter et envoyer votre image docker. Ces commandes seront similaires aux suivantes.
	
	Pour authentifier votre client Docker auprès du registre :
	
	`aws ecr get-login -password --region <YOUR_AWS_REGION> | docker login --username AWS --password-stdin <YOUR_AWS_ACCOUNT>.dkr.ecr.<YOUR_AWS_REGION>.amazonaws.com`
	
	Pour créer votre image Docker :
	
	`docker build -t cluster-sample-app .`
	
	Pour baliser votre image Docker :
	
	`docker tag cluster-sample-app:latest`
		Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	<YOUR_AWS_ACCOUNT> .dkr.ecr.<YOUR_AWS _REGION>.amazonaws .com/cluster-sample- app:latest Pour transférer l'image Docker vers votre dépôt : docker push <YOUR_AWS _ACCOUNT>.dkr.ecr. <YOUR_AWS_REGION>. amazonaws.com/clus ter-sample-app:latest	

Tâche	Description	Compétences requises
Déployez la pile d'applications.	1. Ouvrez la CloudFormation console AWS à l'adresse https://console.aws.amazon.com/cloudformation/. 2. Sélectionnez Créer la pile. 3. Dans la section Préparer le modèle, sélectionnez Le modèle est prêt. 4. Dans la section Spécifier un modèle, sélectionnez Charger un modèle de fichier. 5. Choisissez le fichier local `cluster-sample-app-stack.yml` que vous avez cloné depuis le GitHub référentiel comme CloudFormation modèle, puis choisissez Next. 6. Entrez un nom pour votre pile, puis choisissez Next. 7. Conservez toutes les options par défaut, puis choisissez Next. 8. Passez en revue toutes les options, confirmez la création des ressources IAM, puis choisissez Create stack. 9. Lorsque votre pile d'applications a été déployée, choisissez l'onglet Sortie, copiez l'URL et ouvrez-la	AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises
	dans votre navigateur pour accéder à l'application. Pour plus d'informations sur le déploiement CloudFormation de modèles, consultez la section Création d'une pile dans la CloudFormation documentation AWS.	

Déployer la pile d'applications — option 2 (CLI AWS Copilot)

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Clonez le référentiel d'exemples de code à l'aide de la commande : `git clone https://github.com/aws-samples/cluster-sample-app cluster-sample-app && cd cluster-sample-app`	Développeur d'applications, AWS DevOps
Déployez votre image de conteneur sur AWS à l'aide de l'interface de ligne de commande AWS Copilot.	Déployez l'application en une seule étape à l'aide de la commande suivante dans le répertoire racine de votre projet : `copilot init --app cluster-sample-app --name demo --type "Load Balanced Web Service" --dockerfile ./Dockerf`	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	`ile --port 8080 --deploy` Vous devriez ensuite pouvoir accéder à l'application en utilisant le nom DNS fourni en sortie.	

Supprimer les ressources créées

Tâche	Description	Compétences requises
Supprimez les ressources créées via l'AWS Management Console.	Si vous avez utilisé l'option 1 (AWS Management Console) pour déployer la pile d'applications, suivez ces étapes lorsque vous êtes prêt à supprimer les ressources que vous avez créées : 1. Ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation/. 2. Sélectionnez la pile que vous avez créée, puis choisissez Supprimer. 3. Ouvrez la console Amazon ECR dans les https://console.aws.amazon.com/ecr/référentiels. 4. Sélectionnez le référentiel que vous avez créé, puis choisissez Supprimer.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
Supprimez les ressources créées par AWS Copilot.	Si vous avez utilisé l'option 2 (la CLI AWS Copilot) pour déployer la pile d'applications, exécutez la commande suivante depuis le répertoire racine de votre projet lorsque vous êtes prêt à supprimer les ressources que vous avez créées : `copilot app delete`	Développeur d'applications, AWS DevOps

Ressources connexes

- Installation ou mise à jour de la dernière version de l'AWS CLI (documentation de l'AWS CLI)
- Utilisation de l'interface de ligne de commande AWS Copilot (documentation Amazon ECS)
- Amazon ECS sur AWS Fargate (documentation Amazon ECR)
- Documentation Amazon ECS
- Documentation Amazon ECR
- CloudFormation Documentation Amazon
- Docker Desktop (documentation Docker)

Déployez une application basée sur GRPC sur un cluster Amazon EKS et accédez-y à l'aide d'un Application Load Balancer

Créée par Kirankumar Chandrashekar (AWS) et Huy Nguyen (AWS)

Récapitulatif

Ce modèle décrit comment héberger une application basée sur GRPC sur un cluster Amazon Elastic Kubernetes Service (Amazon EKS) et comment y accéder en toute sécurité via un Application Load Balancer.

gRPC est un framework open source d'appel de procédure à distance (RPC) qui peut s'exécuter dans n'importe quel environnement. Vous pouvez l'utiliser pour les intégrations de microservices et les communications client-serveur. Pour plus d'informations sur gRPC, consultez le billet de blog AWS Application Load Balancer support for end-to-end HTTP/2 and gRPC.

Ce modèle vous montre comment héberger une application basée sur GRPC qui s'exécute sur des pods Kubernetes sur Amazon EKS. Le client gRPC se connecte à un Application Load Balancer via le protocole HTTP/2 avec une connexion cryptée SSL/TLS. L'Application Load Balancer transmet le trafic vers l'application gRPC qui s'exécute sur les pods Amazon EKS. Le nombre de pods gRPC peut être automatiquement redimensionné en fonction du trafic à l'aide du Kubernetes Horizontal Pod Autoscaler. Le groupe cible de l'équilibreur de charge d'application effectue des contrôles de santé sur les nœuds Amazon EKS, évalue si la cible est saine et transmet le trafic uniquement aux nœuds sains.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Docker, installé et configuré sous Linux, macOS ou Windows.
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée sous Linux, macOS ou Windows.
- eksctl, installé et configuré sous Linux, macOS ou Windows.
- `kubectl`, installé et configuré pour accéder aux ressources de votre cluster Amazon EKS. Pour plus d'informations, consultez la section Installation ou mise à jour de kubectl dans la documentation Amazon EKS.
- g RPCurl, installé et configuré.

- Un cluster Amazon EKS nouveau ou existant. Pour plus d'informations, consultez Getting started with Amazon EKS.
- Votre terminal informatique est configuré pour accéder au cluster Amazon EKS. Pour plus d'informations, consultez Configurer votre ordinateur pour communiquer avec votre cluster dans la documentation Amazon EKS.
- AWS Load Balancer Controller, provisionné dans le cluster Amazon EKS.
- Nom d'hôte DNS existant avec un certificat SSL ou SSL/TLS valide. Vous pouvez obtenir un certificat pour votre domaine en utilisant AWS Certificate Manager (ACM) ou en téléchargeant un certificat existant sur ACM. Pour plus d'informations sur ces deux options, consultez les sections Demande d'un certificat public et Importation de certificats dans AWS Certificate Manager dans la documentation ACM.

Architecture

Le schéma suivant montre l'architecture mise en œuvre par ce modèle.

Le schéma suivant montre un flux de travail dans lequel le trafic SSL/TLS est reçu d'un client gRPC qui le décharge vers un Application Load Balancer. Le trafic est transféré en texte clair vers le serveur gRPC car il provient d'un cloud privé virtuel (VPC).

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Elastic Load Balancing répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.

Outils

- eksctl est un outil CLI simple permettant de créer des clusters sur Amazon EKS.
- kubectl est un utilitaire de ligne de commande permettant d'exécuter des commandes sur des clusters Kubernetes.
- AWS Load Balancer Controller vous aide à gérer les AWS Elastic Load Balancers pour un cluster Kubernetes.
- g RPCurl est un outil en ligne de commande qui vous permet d'interagir avec les services gRPC.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub grpc-traffic-on-alb-to-eks.

Épopées

Créez et envoyez l'image Docker du serveur gRPC vers Amazon ECR

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon ECR, puis créez un référentiel Amazon ECR. Pour plus d'informations, consultez la section Création d'un référentiel dans la documentation Amazon ECR. Assurez-vous d'enregistrer l'URL du référentiel Amazon ECR. Vous pouvez également créer un référentiel Amazon ECR avec l'AWS CLI en exécutant la commande suivante :	Administrateur du cloud

Tâche	Description	Compétences requises
	`aws ecr create-repository --repository-name helloworld-grpc`	

Développez l'image Docker.	1. Clonez le référentiel GitHub grpc-traffic-on-alb-to-eks.
	`git clone https://github.com/aws-samples/grpc-traffic-on-alb-to-eks.git`
	2. Dans le répertoire racine du référentiel, assurez-vous que le Dockerfile existe, puis exécutez la commande suivante pour créer l'image Docker :
	`docker build -t <amazon_ecr_repository_url>:<Tag> .`
	Important
	Assurez-vous de `<amazon_ecr_repository_url>` remplacer par l'URL du référentiel Amazon ECR que vous avez créé précédemment.
		DevOps ingénieur

Tâche	Description	Compétences requises

Transférez l'image Docker vers Amazon ECR.	1. Exécutez la commande suivante pour vous connecter au référentiel Amazon ECR :
	`aws ecr get-login -password --region us-east-1 --no-cli-auto-prompt | docker login --username AWS --password-stdin <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com`
	2. Transférez l'image Docker vers le référentiel Amazon ECR en exécutant la commande suivante :
	`docker push <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-grpc:1.0`
	⚠ Important
	Assurez-vous de le remplacer `<your_aws_account_id>` par votre identifiant de compte AWS.
		DevOps ingénieur

Déployez les manifestes Kubernetes sur le cluster Amazon EKS

Tâche	Description	Compétences requises
Modifiez les valeurs du fichier manifeste Kubernetes.	1. Modifiez le fichier manifeste `grpc-sample.yaml` Kubernetes dans le dossier Kubernetes du référentiel en fonction de vos besoins. Vous devez modifier les annotations et le nom d'hôte dans la ressource d'entrée. Pour un exemple de ressource d'entrée, consultez la section Informations supplémentaires. Pour plus d'informations sur les annotations d'entrée, consultez la section Annotations d'entrée dans la documentation de Kubernetes. 2. Dans la ressource de déploiement Kubernetes, remplacez la ressource de déploiement par l'identifiant `image` de ressource uniforme (URI) du référentiel Amazon ECR vers lequel vous avez transféré l'image Docker. Pour un exemple de ressource de déploiement, consultez la section Informations supplémentaires.	DevOps ingénieur

Tâche	Description	Compétences requises
Déployez le fichier manifeste Kubernetes.	Déployez le `grpc-sample.yaml` fichier sur le cluster Amazon EKS en exécutant la `kubectl` commande suivante : `kubectl apply -f ./kubernetes/grpc-sample.yaml`	DevOps ingénieur

Créez l'enregistrement DNS pour le FQDN de l'équilibreur de charge d'application

Tâche	Description	Compétences requises
Enregistrez le nom de domaine complet de l'Application Load Balancer.	1. Exécutez la `kubectl` commande suivante pour décrire la ressource d'entrée Kubernetes qui gère l'Application Load Balancer : `kubectl get ingress -n grpcserver` Un exemple de sortie est fourni dans la section Informations supplémentaires. Dans le résultat, le `HOSTS` champ affiche le nom d'hôte DNS pour lequel les certificats SSL ont été créés. 2. Enregistrez le nom de domaine complet (FQDN)	DevOps ingénieur

Tâche	Description	Compétences requises
	de l'équilibreur de charge d'application `Address` dans le champ de sortie. 3. Créez un enregistrement DNS qui pointe vers le FQDN de l'équilibreur de charge d'application. Si votre fournisseur DNS est Amazon Route 53, vous pouvez créer un enregistrement d'alias qui pointe vers le nom de domaine complet de l'équilibreur de charge d'application. Pour plus d'informations sur cette option, consultez Choisir entre des enregistrements alias et des enregistrements non alias dans la documentation de Route 53.	

Tester la solution

Tâche	Description	Compétences requises
Testez le serveur gRPC.	Utilisez g RPCurl pour tester le point de terminaison en exécutant la commande suivante : `grpcurl grpc.example.com:443 list`	DevOps ingénieur

Tâche	Description	Compétences requises
	`grpc.reflection.v1alpha.ServerReflection helloworld.helloworld` **Note** `grpc.example.com` Remplacez-le par votre nom DNS.	

Tâche	Description	Compétences requises

Testez le serveur gRPC à l'aide d'un client gRPC.	Dans l'`helloworld_client_ssl.py` exemple de client gRPC, remplacez le nom d'hôte de par le nom `grpc.example.com` d'hôte utilisé pour le serveur gRPC.
	
	L'exemple de code suivant montre la réponse du serveur gRPC à la demande du client :
	
	`python ./app/helloworld_client_ssl.py`
	`message: "Hello to gRPC server from Client"`
	
	`message: "Thanks for talking to gRPC server!! Welcome to hello world. Received message is \"Hello to gRPC server from Client\""`
	`received: true`
	
	Cela montre que le client peut communiquer avec le serveur et que la connexion est réussie.
		DevOps ingénieur

Nettoyage

Tâche	Description	Compétences requises
Supprimez l'enregistrement DNS.	Supprimez l'enregistrement DNS qui pointe vers le FQDN de l'équilibreur de charge d'application que vous avez créé précédemment.	Administrateur du cloud
Retirez l'équilibreur de charge.	Sur la EC2 console Amazon, choisissez Load Balancers , puis supprimez l'équilib reur de charge créé par le contrôleur Kubernetes pour votre ressource d'entrée.	Administrateur du cloud
Supprimez le cluster Amazon EKS.	Supprimez le cluster Amazon EKS en utilisant `eksctl` : `eksctl delete cluster -f ./eks.yaml`	AWS DevOps

Ressources connexes

- Répartition de charge réseau sur Amazon EKS
- Groupes cibles pour vos équilibreurs de charge d'applications

Informations supplémentaires

Exemple de ressource d'entrée :

```
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  annotations:
```

```
    alb.ingress.kubernetes.io/healthcheck-protocol: HTTP
    alb.ingress.kubernetes.io/ssl-redirect: "443"
    alb.ingress.kubernetes.io/backend-protocol-version: "GRPC"
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80}, {"HTTPS":443}]'
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/target-type: ip
    alb.ingress.kubernetes.io/certificate-arn: arn:aws:acm:<AWS-
Region>:<AccountId>:certificate/<certificate_ID>
  labels:
    app: grpcserver
    environment: dev
  name: grpcserver
  namespace: grpcserver
spec:
  ingressClassName: alb
  rules:
  - host: grpc.example.com # <----- replace this as per your host name for which the
 SSL certtficate is available in ACM
    http:
      paths:
      - backend:
          service:
            name: grpcserver
            port:
              number: 9000
        path: /
        pathType: Prefix
```

Exemple de ressource de déploiement :

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: grpcserver
  namespace: grpcserver
spec:
  selector:
    matchLabels:
      app: grpcserver
  replicas: 1
  template:
    metadata:
      labels:
```

```
        app: grpcserver
    spec:
      containers:
      - name: grpc-demo
        image: <your_aws_account_id>.dkr.ecr.us-east-1.amazonaws.com/helloworld-
grpc:1.0   #<------- Change to the URI that the Docker image is pushed to
        imagePullPolicy: Always
        ports:
        - name: grpc-api
          containerPort: 9000
        env:
        - name: POD_IP
          valueFrom:
            fieldRef:
              fieldPath: status.podIP
      restartPolicy: Always
```

Exemple de sortie :

```
NAME             CLASS           HOSTS                          Address
 PORTS          AGE
 grpcserver      <none>      <DNS-HostName>                 <ELB-address>
 80            27d
```

Déploiement et débogage de clusters Amazon EKS

Créée par Svenja Raether (AWS) et Mathew George (AWS)

Récapitulatif

Les conteneurs sont en train de devenir un élément essentiel du développement d'applications cloud natives. Kubernetes fournit un moyen efficace de gérer et d'orchestrer les conteneurs. Amazon Elastic Kubernetes Service (Amazon EKS) est un service entièrement géré et certifié conforme à Kubernetes destiné à la création, à la sécurisation, à l'exploitation et à la maintenance de clusters Kubernetes sur Amazon Web Services (AWS). Il prend en charge l'exécution de modules sur AWS Fargate afin de fournir une capacité de calcul adaptée à la demande.

Il est important que les développeurs et les administrateurs connaissent les options de débogage lorsqu'ils exécutent des charges de travail conteneurisées. Ce modèle vous guide dans le déploiement et le débogage de conteneurs sur Amazon EKS avec AWS Fargate. Cela inclut la création, le déploiement, l'accès, le débogage et le nettoyage des charges de travail Amazon EKS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Rôle AWS Identity and Access Management (IAM) configuré avec des autorisations suffisantes pour créer et interagir avec Amazon EKS, les rôles IAM et les rôles liés à un service
- Interface de ligne de commande AWS (AWS CLI) (AWS CLI) installée sur la machine locale
- eksctl
- kubectl
- Casque

Limites

- Ce modèle fournit aux développeurs des pratiques de débogage utiles pour les environnements de développement. Il n'indique pas les meilleures pratiques pour les environnements de production.
- Si vous utilisez Windows, utilisez les commandes spécifiques à votre système d'exploitation pour définir les variables d'environnement.

Versions du produit utilisées

- Version 2 de l'interface de ligne de commande AWS
- version kubectl avec une différence de version mineure par rapport au plan de contrôle Amazon EKS que vous utilisez
- dernière version de eksctl
- Casque v3

Architecture

Pile technologique

- Application Load Balancer
- Amazon EKS
- AWS Fargate

Architecture cible

Toutes les ressources présentées dans le diagramme sont approvisionnées à l'aide `eksctl` de `kubectl` commandes émises par une machine locale. Les clusters privés doivent être exécutés à partir d'une instance située dans le VPC privé.

L'architecture cible consiste en un cluster EKS utilisant le type de lancement Fargate. Cela fournit une capacité de calcul adaptée à la demande sans qu'il soit nécessaire de spécifier les types de serveurs. Le cluster EKS possède un plan de contrôle, qui est utilisé pour gérer les nœuds du cluster et les charges de travail. Les pods sont approvisionnés dans des sous-réseaux VPC privés couvrant plusieurs zones de disponibilité. La galerie publique Amazon ECR est référencée pour récupérer et déployer une image de serveur Web NGINX sur les pods du cluster.

Le schéma montre comment accéder au plan de contrôle Amazon EKS à l'aide de `kubectl` commandes et comment accéder à l'application à l'aide de l'Application Load Balancer.

.

1. Une machine locale en dehors du cloud AWS envoie des commandes au plan de contrôle Kubernetes à l'intérieur d'un VPC géré par Amazon EKS.

2. Amazon EKS planifie les pods en fonction des sélecteurs du profil Fargate.
3. La machine locale ouvre l'URL de l'Application Load Balancer dans le navigateur.
4. L'Application Load Balancer divise le trafic entre les pods Kubernetes des nœuds du cluster Fargate déployés dans des sous-réseaux privés couvrant plusieurs zones de disponibilité.

Outils

Services AWS

- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes. Ce modèle utilise également l'outil de ligne de commande eksctl pour travailler avec les clusters Kubernetes sur Amazon EKS.
- AWS Fargate vous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou d'instances Amazon Elastic Compute Cloud (Amazon EC2). Il est utilisé conjointement avec Amazon Elastic Container Service (Amazon ECS).
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité. Ce modèle utilise le composant de contrôle AWS Load Balancer Controller pour créer l'Application Load Balancer lorsqu'une entrée Kubernetes est provisionnée. L'Application Load Balancer répartit le trafic entrant entre plusieurs cibles.

Autres outils

- Helm est un gestionnaire de paquets open source pour Kubernetes. Dans ce modèle, Helm est utilisé pour installer le contrôleur AWS Load Balancer.
- Kubernetes est un système open source permettant d'automatiser le déploiement, le dimensionnement et la gestion des applications conteneurisées.
- NGINX est un serveur Web et un serveur proxy inverse à hautes performances.

Épopées

Création d'un cluster EKS

Tâche	Description	Compétences requises
Créez les fichiers.	À l'aide du code de la section Informations supplémentaires, créez les fichiers suivants : • `clusterconfig-fargate.yaml` • `nginx-deployment.yaml` • `nginx-service.yaml` • `nginx-ingress.yaml` • `index.html`	Développeur d'applications, administrateur AWS, AWS DevOps
Définissez les variables d'environnement.	**Note** Si une commande échoue en raison de tâches inachevées précédentes, attendez quelques secondes, puis réexécutez la commande. Ce modèle utilise la région AWS et le nom du cluster définis dans le fichier `clusterconfig-fargate.yaml` . Définissez les mêmes valeurs que les variables d'environnement	Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	pour les référencer dans d'autres commandes.
	
	`export AWS_REGION="us-east-1"`
	`export CLUSTER_NAME="my-fargate"`	

Créez un cluster EKS.	Pour créer un cluster EKS qui utilise les spécifications du `clusterconfig-fargate.yaml` fichier, exécutez la commande suivante. `eksctl create cluster -f clusterconfig-fargate.yaml` Le fichier contient le`ClusterConfig` , qui fournit un nouveau cluster EKS nommé `my-fargate-cluster` dans la `us-east-1` région et un profil Fargate par défaut (). `fp-default` Le profil Fargate par défaut est configuré avec deux sélecteurs `default` (et). `kube-system`	Développeur d'applications, AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises

Vérifiez le cluster créé.	Pour vérifier le cluster créé, exécutez la commande suivante.
	`eksctl get cluster --output yaml`
	Le résultat doit être le suivant.
	`- Name: my-fargate`
	`  Owned: "True"`
	`  Region: us-east-1`
	Vérifiez le profil Fargate créé à l'aide du. `CLUSTER_NAME`
	`eksctl get fargatepr ofile --cluster $CLUSTER_NAME --output yaml`
	Cette commande affiche des informations sur les ressource s. Vous pouvez utiliser ces informations pour vérifier le cluster créé. Le résultat doit être le suivant.
	`- name: fp-default`
	`  podExecutionRoleAR N: arn:aws:iam::<YOUR -ACCOUNT-ID>:role/ eksctl-my-fargate- cluster-FargatePod ExecutionRole-xxx`
	`  selectors:`
	`  - namespace: default`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	<pre>- namespace: kube-system
	status: ACTIVE
	subnets:
	- subnet-aaa
	- subnet-bbb
	- subnet-ccc</pre>	

Déployer un conteneur

Tâche	Description	Compétences requises
Déployez le serveur Web NGINX.	Pour appliquer le déploiement du serveur Web NGINX sur le cluster, exécutez la commande suivante. <pre>kubectl apply -f ./nginx-deployment.yaml</pre> Le résultat doit être le suivant. <pre>deployment.apps/nginx-deployment created</pre> Le déploiement inclut trois répliques de l'image NGINX extraite de la galerie publique Amazon ECR. L'image est déployée dans l'espace de noms par défaut et exposée sur le port 80 des pods en cours d'exécution.	Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

Vérifiez le déploiement et les modules.	(Facultatif) Vérifiez le déploiement. Vous pouvez vérifier l'état de votre déploiement à l'aide de la commande suivante.
	`kubectl get deployment`
	Le résultat doit être le suivant.
	`NAME READY UP-TO-DATE AVAILABLE AGE nginx-deployment 3/3 3 3 7m14s`
	Un pod est un objet déployable dans Kubernetes contenant un ou plusieurs conteneurs. Pour répertorier tous les pods, exécutez la commande suivante.
	`kubectl get pods`
	Le résultat doit être le suivant.
	`NAME READY STATUS RESTARTS AGE nginx-deployment-xxxx-aaa 1/1 Running 0 94s`
		Développeur d'applications, AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises
	`nginx-deployment-xxxx-bbb 1/1 Running 0 94s` `nginx-deployment-xxxx-ccc 1/1 Running 0 94s`	

Élargissez le déploiement.	Pour faire passer le déploiement des trois répliques spécifiées dans `deployment.yaml` à quatre répliques, utilisez la commande suivante.
	`kubectl scale deployment nginx-deployment --replicas 4`
	Le résultat doit être le suivant.
	`deployment.apps/nginx-deployment scaled`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Déployer un contrôleur AWS Load Balancer

Tâche	Description	Compétences requises
Définissez les variables d'environnement.	Décrivez la CloudFormation pile du cluster pour récupérer des informations sur son VPC. `aws cloudformation describe-stacks --stack-name eksctl-$CLUSTER_NAME-cluster --query "Stacks[0].Outputs[?OutputK`	Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	`ey==\`VPC\`].Outpu tValue"`
	
	Le résultat doit être le suivant.
	
	`[ "vpc-<YOUR-VPC-ID> " ]`
	
	Copiez l'ID VPC et exportez-le en tant que variable d'environ nement.
	
	`export VPC_ID="vpc- <YOUR-VPC-ID>"`	

Configurez IAM pour le compte de service de cluster.	Utilisez les extraits `AWS_REGION` et `CLUSTER_N AME` extraits de l'épopée précédente pour créer un fournisseur IAM Open ID Connect pour le cluster. `eksctl utils associate- iam-oidc-provider \ --region $AWS_REGION \ --cluster $CLUSTER_ NAME \ --approve`	Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

Téléchargez et créez la politique IAM.	Téléchargez la politique IAM pour le contrôleur AWS Load Balancer qui lui permet de passer des appels à APIs AWS en votre nom.
	`curl -o iam-policy.json https://raw.githubusercontent.com/kubernetes-sigs/aws-load-balancer-controller/main/docs/install/iam_policy.json`
	Créez la politique dans votre compte AWS à l'aide de l'interface de ligne de commande AWS.
	`aws iam create-policy \ --policy-name AWSLoadBalancerControllerIAMPolicy \ --policy-document file://iam-policy.json`
	Le résultat suivant doit s'afficher.
	`{ "Policy": { "PolicyName": "AWSLoadBalancerControllerIAMPolicy", "PolicyId": "<YOUR_POLICY_ID>",`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	<pre>"Arn": "arn:aws:
	iam::<YOUR-ACCOUNT
	-ID>:policy/AWSLoa
	dBalancerControlle
	rIAMPolicy",
	"Path": "/",
	"DefaultV
	ersionId": "v1",
	"Attachme
	ntCount": 0,
	"Permissi
	onsBoundaryUsageCo
	unt": 0,
	"IsAttachable":
	true,
	"CreateDate":
	"<YOUR-DATE>",
	"UpdateDate":
	"<YOUR-DATE>"
	}
	}</pre> Enregistrez le nom de ressource Amazon (ARN) de la politique sous `$POLICY_ARN` . <pre>export POLICY_AR
	N=”arn:aws:iam::<Y
	OUR-ACCOUNT-ID>:po
	licy/AWSLoadBalanc
	erControllerIAMPol
	icy”</pre>	

Tâche	Description	Compétences requises

Créez un compte de service IAM.	Créez un compte de service IAM nommé `aws-load-balancer-controller` dans l'espace de `kube-system` noms. Utilisez le `CLUSTER_NAME` `AWS_REGION`, et `POLICY_ARN` que vous avez configuré précédemment.
	`eksctl create iamserviceaccount \ --cluster=$CLUSTER_NAME \ --region=$AWS_REGION \ --attach-policy-arn=$POLICY_ARN \ --namespace=kube-system \ --name=aws-load-balancer-controller \ --override-existing-serviceaccounts \ --approve`
	Vérifiez la création.
	`eksctl get iamserviceaccount \ --cluster $CLUSTER_NAME \ --name aws-load-balancer-controller \ --namespace kube-system \ --output yaml`
	Le résultat doit être le suivant.
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	- metadata:
	    name: aws-load-balancer-controller
	    namespace: kube-system
	  status:
	    roleARN: arn:aws:iam::<YOUR-ACCOUNT-ID>:role/eksctl-my-fargate-addon-iam serviceaccount-ku-Role1-<YOUR-ROLE-ID>
	  wellKnownPolicies:
	    autoScaler: false
	    awsLoadBalancerController: false
	    certManager: false
	    ebsCSIController: false
	    efsCSIController: false
	    externalDNS: false
	    imageBuilder: false	

Tâche	Description	Compétences requises

Installez le contrôleur AWS Load Balancer.	Mettez à jour le référentiel Helm.
	`helm repo update`
	Ajoutez le référentiel de graphiques Amazon EKS au référentiel Helm.
	`helm repo add eks https://aws.github.io/eks-charts`
	Appliquez les définitions de ressources personnalisées Kubernetes (CRDs) utilisées par le AWS Load Balancer Controller eks-chart en arrière-plan.
	`kubectl apply -k "github.com/aws/eks-charts/stable/aws-load-balancer-controller//crds?ref=master"`
	Le résultat doit être le suivant.
	`customresourcedefinition.apiextensions.k8s.io/ingressclassparams.elbv2.k8s.aws created customresourcedefinition.apiextensions.k8s.io/targetgro`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises
	upbindings.elbv2.k 8s.aws created Installez le graphique Helm en utilisant les variables d'environnement que vous avez définies précédemment. helm install aws-load- balancer-controlle r eks/aws-load-balan cer-controller \ --set clusterName= $CLUSTER_NAME \ --set serviceAc count.create=false \ --set region=$A WS_REGION \ --set vpcId=$VPC_ID \ --set serviceAc count.name=aws-load- balancer-controller \ -n kube-system Le résultat doit être le suivant. NAME: aws-load- balancer-controller LAST DEPLOYED: <YOUR-DAT E> NAMESPACE: kube-system STATUS: deployed REVISION: 1 TEST SUITE: None NOTES: AWS Load Balancer controller installed!	

Tâche	Description	Compétences requises

Créez un service NGINX.	Créez un service pour exposer les pods NGINX à l'aide du `nginx-service.yaml` fichier.
	`kubectl apply -f nginx-service.yaml`
	Le résultat doit être le suivant.
	`service/nginx-service created`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Créez la ressource d'entrée Kubernetes.	Créez un service pour exposer l'entrée NGINX de Kubernetes à l'aide du fichier. `nginx-ingress.yaml`
	`kubectl apply -f nginx-ingress.yaml`
	Le résultat doit être le suivant.
	`ingress.networking.k8s.io/nginx-ingress created`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

Obtenez l'URL de l'équilibreur de charge.	Pour récupérer les informations d'entrée, utilisez la commande suivante.
	`kubectl get ingress nginx-ingress`
	Le résultat doit être le suivant.
	`NAME CLASS HOSTS ADDRESS PORTS AGE nginx-ingress <none> * k8s-default-nginxing-xxx.us-east-1.elb.amazonaws.com 80 80s`
	Copiez `ADDRESS` (par exemple `k8s-default-nginxing-xxx.us-east-1.elb.amazonaws.com`) le fichier de sortie et collez-le dans votre navigateur pour accéder au `index.html` fichier.
		Développeur d'applications, AWS DevOps, administrateur système AWS

Déboguer les conteneurs en cours d'exécution

Tâche	Description	Compétences requises
Sélectionnez un module.	Répertoriez tous les modules et copiez le nom du module souhaité.	Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	`kubectl get pods`
	
	Le résultat doit être le suivant.
	
	`NAME READY STATUS RESTARTS AGE nginx-deployment-xxxx-aaa 1/1 Running 0 55m nginx-deployment-xxxx-bbb 1/1 Running 0 55m nginx-deployment-xxxx-ccc 1/1 Running 0 55m nginx-deployment-xxxx-ddd 1/1 Running 0 42m`
	
	Cette commande répertorie les modules existants et des informations supplémentaires.
	
	Si vous êtes intéressé par un module spécifique, saisissez le nom du module qui vous intéresse pour la `POD_NAME` variable ou définissez-le comme variable d'environ nement. Sinon, omettez ce paramètre pour rechercher toutes les ressources.	

Tâche	Description	Compétences requises
	`export POD_NAME="nginx-deployment-<YOUR-POD-NAME>"`	
Accédez aux journaux.	Récupérez les journaux du module que vous souhaitez déboguer. `kubectl logs $POD_NAME`	Développeur d'applications, administrateur système AWS, AWS DevOps

Tâche	Description	Compétences requises

Transférez le port NGINX.	Utilisez le transfert de port pour mapper le port du pod permettant d'accéder au serveur Web NGINX à un port de votre machine locale.
	`kubectl port-forward deployment/nginx-deployment 8080:80`
	Dans votre navigateur, ouvrez l'URL suivante.
	`http://localhost:8080`
	La `port-forward` commande permet d'accéder au `index.html` fichier sans le rendre accessible au public via un équilibreur de charge. Ceci est utile pour accéder à l'application en cours d'exécution lors de son débogage. Vous pouvez arrêter le transfert de port en appuyant sur la commande clavier Ctrl+C.
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises
Exécutez des commandes dans le module.	Pour consulter le `index.html` fichier en cours, utilisez la commande suivante. `kubectl exec $POD_NAME -- cat /usr/share/nginx/html/index.html` Vous pouvez utiliser la `exec` commande pour émettre n'importe quelle commande directement dans le module. Cela est utile pour le débogage des applications en cours d'exécution.	Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

Copiez des fichiers dans un module.	Supprimez le `index.html` fichier par défaut de ce module.
	`kubectl exec $POD_NAME -- rm /usr/share/nginx/html/index.html`
	Téléchargez le fichier `index.html` local personnalisé dans le module.
	`kubectl cp index.html $POD_NAME:/usr/share/nginx/html/`
	Vous pouvez utiliser la `cp` commande pour modifier ou ajouter des fichiers directement dans n'importe quel module.
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

Utilisez le transfert de port pour afficher la modification.	Utilisez le transfert de port pour vérifier les modifications que vous avez apportées à ce module.
	`kubectl port-forward pod/$POD_NAME 8080:80`
	Ouvrez l'URL suivante dans votre navigateur.
	`http://localhost:8080`
	Les modifications apportées au `index.html` fichier doivent être visibles dans le navigateur.
		Développeur d'applications, AWS DevOps, administrateur système AWS

Supprimer des ressources

Tâche	Description	Compétences requises

Supprimez l'équilibreur de charge.	Supprimez l'entrée.
	`kubectl delete ingress/nginx-ingress`
	Le résultat doit être le suivant.
	`ingress.networking.k8s.io "nginx-ingress" deleted`
	Supprimez le service.
		Développeur d'applications, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises

	`kubectl delete service/nginx-service`
	
	Le résultat doit être le suivant.
	
	`service "nginx-service" deleted`
	
	Supprimez le contrôleur de l'équilibreur de charge.
	
	`helm delete aws-load-balancer-controller -n kube-system`
	
	Le résultat doit être le suivant.
	
	`release "aws-load-balancer-controller" uninstalled`
	
	Supprimez le compte de service.
	
	`eksctl delete iamserviceaccount --cluster $CLUSTER_NAME --namespace kube-system --name aws-load-balancer-controller`	

Tâche	Description	Compétences requises

Supprimez le déploiement.	Pour supprimer les ressources de déploiement, utilisez la commande suivante.
	`kubectl delete deploy/nginx-deployment`
	Le résultat doit être le suivant.
	`deployment.apps "nginx-deployment" deleted`
		Développeur d'applications, AWS DevOps, administrateur système AWS

Supprimez le cluster.	Supprimez le cluster EKS à l'aide de la commande suivante, où se `my-fargate` trouve le nom du cluster. `eksctl delete cluster --name $CLUSTER_NAME` Cette commande supprime l'ensemble du cluster, y compris toutes les ressources associées.	Développeur d'applications, AWS DevOps, administrateur système AWS
Supprimez la politique IAM.	Supprimez la politique créée précédemment à l'aide de l'interface de ligne de commande AWS. `aws iam delete-policy --policy-arn $POLICY_ARN`	Développeur d'applications, administrateur AWS, AWS DevOps

Résolution des problèmes

Problème	Solution
Vous recevez un message d'erreur lors de la création du cluster indiquant que la capacité de votre zone de disponibilité ciblée n'est pas suffisante pour prendre en charge le cluster. Un message similaire au suivant devrait s'afficher. `Cannot create cluster 'my-fargate' because us-east-1e, the targeted availability zone, does not currently have sufficient capacity to support the cluster. Retry and choose from these availability zones: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1f`	Créez à nouveau le cluster en utilisant les zones de disponibilité recommandées dans le message d'erreur. Spécifiez une liste de zones de disponibilité dans la dernière ligne de votre `clusterconfig-fargate.yaml` fichier (par exemple,`availabilityZones: ["us-east-1a", "us-east-1b", "us-east-1c"]`).

Ressources connexes

- Documentation Amazon EKS
- Répartition de la charge des applications sur Amazon EKS
- Guides des meilleures pratiques EKS
- Documentation du contrôleur AWS Load Balancer
- documentation eksctl
- Image NGINX de la galerie publique Amazon ECR
- Documentation du casque
- Déboguer les pods en cours d'exécution (documentation Kubernetes)
- Atelier Amazon EKS
- Erreurs de création de cluster EKS

Informations supplémentaires

clusterconfig-fargate.yaml

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: my-fargate
  region: us-east-1

fargateProfiles:
  - name: fp-default
    selectors:
      - namespace: default
      - namespace: kube-system
```

nginx-deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: "nginx-deployment"
  namespace: "default"
spec:
  replicas: 3
  selector:
    matchLabels:
      app: "nginx"
  template:
    metadata:
      labels:
        app: "nginx"
    spec:
      containers:
      - name: nginx
        image: public.ecr.aws/nginx/nginx:latest
        ports:
        - containerPort: 80
```

nginx-service.yaml

```
apiVersion: v1
kind: Service
metadata:
  annotations:
```

```
    alb.ingress.kubernetes.io/target-type: ip
  name: "nginx-service"
  namespace: "default"
spec:
  ports:
  - port: 80
    targetPort: 80
    protocol: TCP
  type: NodePort
  selector:
    app: "nginx"
```

nginx-ingress.yaml

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  namespace: "default"
  name:  "nginx-ingress"
  annotations:
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/scheme: internet-facing
spec:
  rules:
    - http:
        paths:
        - path: /
          pathType: Prefix
          backend:
            service:
              name: "nginx-service"
              port:
                number: 80
```

index.html

```
<!DOCTYPE html>
<html>

<body>
    <h1>Welcome to your customized nginx!</h1>
    <p>You modified the file on this running pod</p>
</body>
```

```
</html>
```

Déployez des conteneurs à l'aide d'Elastic Beanstalk

Créée par Thomas Scott (AWS) et Jean-Baptiste Guillois (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), AWS Elastic Beanstalk prend en charge Docker en tant que plate-forme disponible, afin que les conteneurs puissent fonctionner avec l'environnement créé. Ce modèle montre comment déployer des conteneurs à l'aide du service Elastic Beanstalk. Le déploiement de ce modèle utilisera l'environnement du serveur Web basé sur la plate-forme Docker.

Pour utiliser Elastic Beanstalk pour déployer et dimensionner des applications et des services Web, vous téléchargez votre code et le déploiement est automatiquement géré. Le provisionnement des capacités, l'équilibrage de charge, le dimensionnement automatique et la surveillance de l'état de santé des applications sont également inclus. Lorsque vous utilisez Elastic Beanstalk, vous pouvez contrôler totalement les ressources AWS qu'il crée en votre nom. Elastic Beanstalk n'entraîne aucun frais supplémentaire. Vous ne payez que pour les ressources AWS utilisées pour stocker et exécuter vos applications.

Ce modèle inclut des instructions de déploiement à l'aide de l'interface de ligne de commande AWS Elastic Beanstalk (EB CLI) et de l'AWS Management Console.

Cas d’utilisation

Les cas d'utilisation d'Elastic Beanstalk sont les suivants :

- Déployez un environnement prototype pour faire la démonstration d'une application frontale. (Ce modèle utilise un Dockerfile comme exemple.)
- Déployez une API pour gérer les demandes d'API pour un domaine donné.
- Déployez une solution d'orchestration à l'aide de Docker-Compose (`docker-compose.yml`ce modèle n'est pas utilisé comme exemple pratique).

Conditions préalables et limitations

Prérequis

- Un compte AWS
- AWS EB CLI installée localement
- Docker installé sur une machine locale

Limites

- Le forfait gratuit impose une limite d'extraction Docker de 100 extractions par 6 heures et par adresse IP.

Architecture

Pile technologique cible

- Instances Amazon Elastic Compute Cloud (Amazon EC2)
- Groupe de sécurité
- Application Load Balancer
- Groupe Auto Scaling

Architecture cible

Automatisation et mise à l'échelle

AWS Elastic Beanstalk peut automatiquement évoluer en fonction du nombre de demandes effectuées. Les ressources AWS créées pour un environnement incluent un Application Load Balancer, un groupe Auto Scaling et une ou plusieurs instances Amazon EC2 .

L'équilibreur de charge se trouve devant les EC2 instances Amazon, qui font partie du groupe Auto Scaling. Amazon EC2 Auto Scaling démarre automatiquement des EC2 instances Amazon supplémentaires pour s'adapter à la charge croissante de votre application. Si la charge de votre application diminue, Amazon EC2 Auto Scaling arrête les instances, mais maintient au moins une instance en cours d'exécution.

Déclencheurs de dimensionnement automatiques

Le groupe Auto Scaling de votre environnement Elastic Beanstalk utilise CloudWatch deux alarmes Amazon pour lancer les opérations de dimensionnement. Les déclencheurs par défaut évoluent quand le trafic réseau sortant moyen de chaque instance est supérieur à 6 Mo ou inférieur à 2 Mo sur une période de cinq minutes. Pour utiliser Amazon EC2 Auto Scaling de manière efficace, configurez des déclencheurs adaptés à votre application, à votre type d'instance et à vos exigences de service. Vous pouvez mettre à l'échelle en fonction de plusieurs statistiques, y compris la latence, les I/O disque, l'utilisation de l'UC et le nombre de demandes. Pour plus d'informations, consultez la section Déclencheurs Auto Scaling.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- L'interface de ligne de commande AWS EB (EB CLI) est un client de ligne de commande que vous pouvez utiliser pour créer, configurer et gérer des environnements Elastic Beanstalk.
- Elastic Load Balancing répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.

Autres services

- Docker regroupe les logiciels dans des unités standardisées appelées conteneurs qui incluent des bibliothèques, des outils système, du code et un environnement d'exécution.

Code

Le code de ce modèle est disponible dans le référentiel GitHub Cluster Sample Application.

Épopées

Construire avec un Dockerfile

Tâche	Description	Compétences requises
Clonez le référentiel distant.	• Pour cloner le dépôt, exécutez la commande`git clone https://github.com/aws-samples/cluster-sample-app.git . < /p >`	Développeur d'applications, administrateur AWS, AWS DevOps
Initialisez le projet Elastic Beanstalk Docker.	1. Créez un fichier appelé `aws.json` à la racine.	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	2. Dans le `aws.json` fichier, ajoutez le code suivant. `{ "AWSEBDockerrunVersion":"1", "Image":{ "Name":"cluster-sample-app" }, "Ports":[ { "ContainerPort":80 , "HostPort":8080 } ] }` 3. Exécutez la commande `eb init -p docker` à la racine du projet.	
Testez le projet localement.	1. Exécutez la commande `eb local run` à la racine du projet. 2. Testez l'application en accédant à. `http://localhost`	Développeur d'applications, administrateur AWS, AWS DevOps

Déploiement à l'aide d'EB CLI

Tâche	Description	Compétences requises
Exécuter la commande de déploiement	1. Exécutez la commande `eb create docker-sample-cluster-app` à la racine du projet.	Développeur d'applications, administrateur AWS, AWS DevOps
Accédez à la version déployée.	Une fois la commande de déploiement terminée, accédez au projet à l'aide de la `eb open` commande.	Développeur d'applications, administrateur AWS, AWS DevOps

Déploiement à l'aide de la console

Tâche	Description	Compétences requises
Déployez l'application à l'aide du navigateur.	1. Ouvrez la console. 2. Accédez à la console Elastic Beanstalk. 3. Choisissez Create Application. 4. Pour le nom de l'application, entrez Cluster-Sample-App. 5. Choisissez Docker comme plateforme. 6. Choisissez Importer votre code. 7. Choisissez votre fichier .zip local (à la racine du projet cloné) ou une URL publique Amazon Simple Storage Service (Amazon S3).	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
Accédez à la version déployée.	Après le déploiement, accédez à l'application déployée et choisissez l'URL fournie.	Développeur d'applications, administrateur AWS, AWS DevOps

Ressources connexes

- Environnements de serveurs Web
- Installation de l'interface de ligne de commande EB sur macOS
- Installation manuelle de l'interface de ligne de commande EB

Informations supplémentaires

Avantages de l'utilisation d'Elastic Beanstalk

- Provisionnement automatique de l'infrastructure
- Gestion automatique de la plateforme sous-jacente
- Correctifs et mises à jour automatiques pour prendre en charge l'application
- Dimensionnement automatique de l'application
- Possibilité de personnaliser le nombre de nœuds
- Possibilité d'accéder aux composants de l'infrastructure si nécessaire
- Facilité de déploiement par rapport aux autres solutions de déploiement de conteneurs

Générez une adresse IP sortante statique à l'aide d'une fonction Lambda, d'Amazon VPC et d'une architecture sans serveur

Créée par Thomas Scott (AWS)

Récapitulatif

Ce modèle décrit comment générer une adresse IP sortante statique dans le cloud Amazon Web Services (AWS) à l'aide d'une architecture sans serveur. Votre organisation peut bénéficier de cette approche si elle souhaite envoyer des fichiers à une entité commerciale distincte en utilisant le protocole SFTP (Secure File Transfer Protocol). Cela signifie que l'entité commerciale doit avoir accès à une adresse IP qui permet aux fichiers de passer par son pare-feu.

L'approche du modèle vous aide à créer une fonction AWS Lambda qui utilise une adresse IP élastique comme adresse IP sortante. En suivant les étapes de ce modèle, vous pouvez créer une fonction Lambda et un cloud privé virtuel (VPC) qui achemine le trafic sortant via une passerelle Internet dotée d'une adresse IP statique. Pour utiliser l'adresse IP statique, vous devez associer la fonction Lambda au VPC et à ses sous-réseaux.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Autorisations AWS Identity and Access Management (IAM) pour créer et déployer une fonction Lambda, ainsi que pour créer un VPC et ses sous-réseaux. Pour plus d'informations à ce sujet, consultez la section Rôle d'exécution et autorisations utilisateur dans la documentation AWS Lambda.
- Si vous envisagez d'utiliser l'infrastructure en tant que code (IaC) pour implémenter l'approche de ce modèle, vous avez besoin d'un environnement de développement intégré (IDE) tel qu'AWS Cloud9. Pour plus d'informations à ce sujet, consultez Qu'est-ce qu'AWS Cloud9 ? dans la documentation AWS Cloud9.

Architecture

Le schéma suivant montre l'architecture sans serveur pour ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Le trafic sortant part`NAT gateway 1`. `Public subnet 1`
2. Le trafic sortant part`NAT gateway 2`. `Public subnet 2`
3. La fonction Lambda peut être exécutée dans ou. `Private subnet 1` `Private subnet 2`
4. `Private subnet 1`et `Private subnet 2` acheminez le trafic vers les passerelles NAT dans les sous-réseaux publics.
5. Les passerelles NAT envoient le trafic sortant vers la passerelle Internet à partir des sous-réseaux publics.
6. Les données sortantes sont transférées de la passerelle Internet vers le serveur externe.

Pile technologique

- Lambda
- Amazon Virtual Private Cloud (Amazon VPC)

Automatisation et mise à l'échelle

Vous pouvez garantir la haute disponibilité (HA) en utilisant deux sous-réseaux publics et deux sous-réseaux privés dans différentes zones de disponibilité. Même si une zone de disponibilité devient indisponible, la solution du modèle continue de fonctionner.

Outils

- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) fournit une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d'AWS.

Épopées

Création d'un VPC

Tâche	Description	Compétences requises
Créez un nouveau VPC.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon VPC, puis créez un VPC nommé `Lambda VPC` dont la plage d'adresses CIDR est `10.0.0.0/25` la plage d'adresses CIDR. IPv4 Pour plus d'informations sur la création d'un VPC, consultez Getting started with Amazon VPC dans la documentation Amazon VPC.	Administrateur AWS

Création de deux sous-réseaux publics

Tâche	Description	Compétences requises
Créez le premier sous-réseau public.	1. Sur la console Amazon VPC, choisissez Subnets, puis Create Subnet. 2. Pour Balise de nom, saisissez `public-one` . 3. Pour VPC, choisissez `Lambda VPC`. 4. Choisissez une zone de disponibilité et enregistrez-la.	Administrateur AWS

Tâche	Description	Compétences requises
	5. Pour le bloc IPv4 CIDR, entrez `10.0.0.0/28` puis choisissez Create subnet.	
Créez le deuxième sous-rése au public.	1. Sur la console Amazon VPC, choisissez Subnets, puis Create Subnet. 2. Pour Balise de nom, saisissez `public-two` . 3. Pour VPC, choisissez `Lambda VPC`. 4. **Important** Choisissez une zone de disponibi lité et enregistr ez-la. : vous ne pouvez pas utiliser la zone de disponibi lité qui contient le `public-one` sous-réseau. 5. Pour le bloc IPv4 CIDR, entrez `10.0.0.16/28` puis choisissez Create subnet.	Administrateur AWS

Création de deux sous-réseaux privés

Tâche	Description	Compétences requises
Créez le premier sous-réseau privé.	1. Sur la console Amazon VPC, choisissez Subnets, puis Create Subnet. 2. Pour Balise de nom, saisissez `private-one` . 3. Pour VPC, choisissez `Lambda VPC`. 4. Choisissez la zone de disponibilité qui contient le `public-one` sous-réseau que vous avez créé précédemment. 5. Pour le bloc IPv4 CIDR, entrez `10.0.0.32/28` puis choisissez Create subnet.	Administrateur AWS
Créez le deuxième sous-réseau privé.	1. Sur la console Amazon VPC, choisissez Subnets, puis Create Subnet. 2. Pour Balise de nom, saisissez `private-two` . 3. Pour VPC, choisissez `Lambda VPC`. 4. Choisissez la même zone de disponibilité qui contient le `public-two` sous-réseau que vous avez créé précédemment. 5. Pour le bloc IPv4 CIDR, entrez `10.0.0.64/28`	Administrateur AWS

Tâche	Description	Compétences requises
	puis choisissez Create subnet.	

Créez deux adresses IP élastiques pour vos passerelles NAT

Tâche	Description	Compétences requises
Créez la première adresse IP élastique.	1. Sur la console Amazon VPC, choisissez Elastic, IPs puis choisissez Allocate new address. 2. Choisissez Allocation et enregistrez l'ID d'allocat ion pour votre adresse IP élastique nouvellement créée. **Note** Cette adresse IP élastique est utilisée pour votre première passerelle NAT.	Administrateur AWS
Créez la deuxième adresse IP élastique.	1. Sur la console Amazon VPC, choisissez Elastic, IPs puis choisissez Allocate new address. 2. Choisissez Allouer et enregistrez l'ID d'allocat ion pour cette deuxième adresse IP élastique.	Administrateur AWS

Tâche	Description	Compétences requises
	Note Cette adresse IP élastique est utilisée pour votre deuxième passerelle NAT.	

Création d'une passerelle Internet

Tâche	Description	Compétences requises
Créer une passerelle Internet	1. Sur la console Amazon VPC, choisissez Internet Gateways, puis Create Internet Gateway. 2. Entrez le `Lambda internet gateway` nom, puis choisissez Créer une passerelle Internet. Assurez-vous d'enregistrer l'identifiant de la passerelle Internet.	Administrateur AWS
Connectez la passerelle Internet au VPC.	Sélectionnez la passerelle Internet que vous venez de créer, puis choisissez Actions, Attach to VPC (Actions, Attacher au VPC).	Administrateur AWS

Création de deux passerelles NAT

Tâche	Description	Compétences requises
Créez la première passerelle NAT.	1. Sur la console Amazon VPC, choisissez NAT Gateways, puis Create NAT Gateway. 2. Entrez `nat-one` comme nom de passerelle NAT. 3. Choisissez `public-one` comme sous-réseau dans lequel créer la passerelle NAT. 4. Pour le type de connectiv ité, choisissez Public. 5. Pour l'ID d'allocation IP élastique, choisissez la première adresse IP élastique que vous avez créée précédemment et associez-la à la passerelle NAT. 6. Sélectionnez Créer une passerelle NAT.	Administrateur AWS
Créez la deuxième passerelle NAT.	1. Sur la console Amazon VPC, choisissez NAT Gateways, puis Create NAT Gateway. 2. Entrez `nat-two` comme nom de passerelle NAT. 3. Choisissez `public-two` comme sous-réseau dans	Administrateur AWS

Tâche	Description	Compétences requises
	lequel créer la passerelle NAT. 4. Pour le type de connectiv ité, choisissez Public. 5. Pour l'ID d'allocation IP élastique, choisissez la deuxième adresse IP élastique que vous avez créée précédemment et associez-la à la passerelle NAT. 6. Sélectionnez Créer une passerelle NAT.	

Créez des tables de routage pour vos sous-réseaux publics et privés

Tâche	Description	Compétences requises
Créez la table de routage pour le sous-réseau public.	1. Sur la console Amazon VPC, choisissez Route Tables, puis Create route table. 2. Entrez le `public-one-subnet` nom de la table de routage, puis choisissez Créer une table de routage. 3. Choisissez la table de `public-one-subnet` routage, choisissez Modifier les itinéraires, puis choisissez Ajouter un itinéraire.	Administrateur AWS

Tâche	Description	Compétences requises
	4. Spécifiez `0.0.0.0` dans le champ Destination, puis choisissez l'ID de passerelle Internet dans la liste des cibles. 5. Dans l'onglet Associations de sous-réseaux, choisissez Modifier les associations de sous-réseaux, choisissez le **`public-one`** sous-réseau avec la plage **`10.0.0.0/28`** CIDR, puis sélectionnez Enregistrer les associations. 6. Choisissez Save Changes (Enregistrer les modifications).	

Tâche	Description	Compétences requises
Créez la table de routage pour le sous-réseau public-two.	1. Sur la console Amazon VPC, choisissez Route Tables, puis Create route table. 2. Entrez le `public-two-subnet` nom de la table de routage, puis choisissez Créer une table de routage. 3. Choisissez la table de `public-two-subnet` routage, choisissez Modifier les itinéraires, puis choisissez Ajouter un itinéraire. 4. Spécifiez `0.0.0.0` dans le champ Destination, puis choisissez l'ID de passerelle Internet dans la liste des cibles. 5. Dans l'onglet Associations de sous-réseaux, choisissez Modifier les associations de sous-réseaux, choisissez le **`public-two`** sous-réseau avec la plage **`10.0.0.16/28`** CIDR, puis sélectionnez Enregistrer les associations. 6. Choisissez Save Changes (Enregistrer les modifications).	Administrateur AWS

Tâche	Description	Compétences requises
Créez la table de routage pour le sous-réseau private-one.	1. Sur la console Amazon VPC, choisissez Route Tables, puis Create route table. 2. Entrez le `private-one-subnet` nom de la table de routage, puis choisissez Créer une table de routage. 3. Choisissez la table de `private-one-subnet` routage, choisissez Modifier les itinéraires, puis choisissez Ajouter un itinéraire. 4. Spécifiez `0.0.0.0` dans le champ Destination, puis choisissez la passerelle NAT dans le `public-one` sous-réseau dans la liste des cibles. 5. Dans l'onglet Associations de sous-réseaux, choisissez Modifier les associations de sous-réseaux, choisissez le **`private-one`** sous-réseau avec la plage **`10.0.0.32/28`** CIDR, puis sélectionnez Enregistrer les associations. 6. Choisissez Save Changes (Enregistrer les modifications).	Administrateur AWS

Tâche	Description	Compétences requises
Créez la table de routage pour le sous-réseau private-two.	1. Sur la console Amazon VPC, choisissez Route Tables, puis Create route table. 2. Entrez le `private-two-subnet` nom de la table de routage, puis choisissez Créer une table de routage. 3. Choisissez la table de `private-two-subnet` routage, choisissez Modifier les itinéraires, puis choisissez Ajouter un itinéraire. 4. Spécifiez `0.0.0.0` dans le champ Destination, puis choisissez la passerelle NAT dans le `public-two` sous-réseau dans la liste des cibles. 5. Dans l'onglet Associations de sous-réseaux, choisissez Modifier les associations de sous-réseaux, choisissez le **`private-two`** sous-réseau avec la plage **`10.0.0.64/28`** CIDR, puis sélectionnez Enregistrer les associations. 6. Choisissez Save Changes (Enregistrer les modifications).	Administrateur AWS

Créez la fonction Lambda, ajoutez-la au VPC et testez la solution

Tâche	Description	Compétences requises
Créez une fonction Lambda.	1. Ouvrez la console AWS Lambda et choisissez Create function. 2. Sous Informations de base, entrez dans `Lambda test` Nom de la fonction, puis choisissez la langue de votre choix sous Runtime. 3. Choisissez Créer une fonction.	Administrateur AWS
Ajoutez la fonction Lambda à votre VPC.	1. Sur la console AWS Lambda, choisissez Functions, puis choisissez la fonction que vous avez créée précédemment. 2. Sélectionnez Configuration, puis VPC. 3. Choisissez Modifier, puis sélectionnez `Lambda VPC` les deux sous-réseaux privés. 4. Choisissez le groupe de sécurité par défaut à des fins de test, puis sélection nez Enregistrer.	Administrateur AWS
Écrivez du code pour appeler un service externe.	1. Dans le langage de programmation de votre choix, écrivez du code pour appeler un service externe	Administrateur AWS

Tâche	Description	Compétences requises
	qui renvoie votre adresse IP. 2. Vérifiez que l'adresse IP renvoyée correspond à l'une de vos adresses IP Elastic.	

Ressources connexes

- Configuration d'une fonction Lambda pour accéder aux ressources d'un VPC

Identifiez automatiquement les images de conteneur dupliquées lors de la migration vers un référentiel Amazon ECR

Créée par Rishabh Yadav (AWS) et Rishi Singla (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Le modèle fournit une solution automatisée pour déterminer si les images stockées dans différents référentiels de conteneurs sont des doublons. Cette vérification est utile lorsque vous envisagez de migrer des images d'autres référentiels de conteneurs vers Amazon Elastic Container Registry (Amazon ECR).

Pour les informations de base, le modèle décrit également les composants d'une image conteneur, tels que le résumé de l'image, le manifeste et les balises. Lorsque vous planifiez une migration vers Amazon ECR, vous pouvez décider de synchroniser les images de vos conteneurs entre les registres de conteneurs en comparant les résumés des images. Avant de migrer vos images de conteneur, vous devez vérifier si ces images existent déjà dans le référentiel Amazon ECR afin d'éviter toute duplication. Cependant, il peut être difficile de détecter les doublons en comparant les résumés d'images, ce qui peut entraîner des problèmes lors de la phase initiale de migration. Ce modèle compare les résumés de deux images similaires stockées dans des registres de conteneurs différents et explique pourquoi les résumés varient, afin de vous aider à comparer les images avec précision.

Conditions préalables et limitations

- Un actif Compte AWS
- Accès au registre public Amazon ECR
- Connaissance des éléments suivants : Services AWS
  - AWS CodeCommit
  - AWS CodePipeline
  - AWS CodeBuild
  - AWS Identity and Access Management (JE SUIS)
  - Amazon Simple Storage Service (Amazon S3)
- CodeCommit Informations d'identification configurées (voir les instructions)

Architecture

Composants de l'image du conteneur

Le schéma suivant illustre certains des composants d'une image de conteneur. Ces composants sont décrits après le schéma.

Termes et définitions

Les termes suivants sont définis dans la spécification d'image de l'Open Container Initiative (OCI).

- Registre : service de stockage et de gestion d'images.
- Client : outil qui communique avec les registres et fonctionne avec des images locales.
- Push : processus de téléchargement d'images dans un registre.
- Pull : processus de téléchargement d'images depuis un registre.
- Blob : forme binaire du contenu qui est stocké par un registre et qui peut être traité par un condensé.
- Index : construction qui identifie plusieurs manifestes d'images pour différentes plateformes informatiques (telles que x86-64 ou ARM 64 bits) ou types de supports. Pour plus d'informations, consultez la spécification de l'indice d'image OCI.
- Manifeste : document JSON qui définit une image ou un artefact téléchargé via le point de terminaison du manifeste. Un manifeste peut faire référence à d'autres blobs d'un dépôt à l'aide de descripteurs. Pour plus d'informations, consultez la spécification OCI Image Manifest.
- Couche du système de fichiers : bibliothèques système et autres dépendances d'une image.
- Configuration : blob contenant les métadonnées des artefacts et référencé dans le manifeste. Pour plus d'informations, consultez la spécification de configuration d'image OCI.
- Objet ou artefact : élément de contenu conceptuel stocké sous forme de blob et associé à un manifeste accompagné d'une configuration.
- Résumé : identifiant unique créé à partir d'un hachage cryptographique du contenu d'un manifeste. Le condensé d'image permet d'identifier de manière unique une image de conteneur immuable. Lorsque vous extrayez une image à l'aide de son condensé, vous téléchargez la même image à chaque fois, quel que soit le système d'exploitation ou l'architecture. Pour plus d'informations, consultez la spécification d'image OCI.

- Tag : Un identifiant de manifeste lisible par l'homme. Par rapport aux résumés d'images, qui sont immuables, les balises sont dynamiques. Une balise pointant vers une image peut changer et passer d'une image à l'autre, même si le résumé de l'image sous-jacent reste le même.

Architecture cible

Le schéma suivant montre l'architecture de haut niveau de la solution fournie par ce modèle pour identifier les images de conteneur dupliquées en comparant les images stockées dans Amazon ECR et dans des référentiels privés.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.

Code

Le code de ce modèle est disponible dans la solution automatisée du GitHub référentiel pour identifier les images de conteneur dupliquées entre les référentiels.

Bonnes pratiques

- AWS CloudFormation meilleures pratiques
- AWS CodePipeline meilleures pratiques

Épopées

Extraire des images de conteneurs depuis les référentiels publics et privés Amazon ECR

Tâche	Description	Compétences requises

Extrayez une image du référentiel public Amazon ECR.	Depuis le terminal, exécutez la commande suivante pour extraire l'image `amazonlinux` du référentiel public Amazon ECR.
	`$~ % docker pull public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	Lorsque l'image a été extraite sur votre machine locale, vous verrez le résumé d'extraction suivant, qui représente l'index de l'image.
	`2018.03: Pulling from amazonlinux/amazonlinux`
	`4ddc0f8d367f: Pull complete`
	`Digest: sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5`
	`Status: Downloaded newer image for public.ecr.aws/amazonlinux/amazonlinux:2018.03`
		Développeur d'applications, AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises
	`public.ecr.aws/amazonlinux/amazonlinux:2018.03`	

Tâche	Description	Compétences requises

Transférez l'image vers un référentiel privé Amazon ECR.	1. Créez un référentiel Amazon ECR privé nommé `test_ecr_repository` dans la région USA Est (Virginie du Nord) (`us-east-1`).
	`$~ % aws ecr get-login -password --region us-east-1 | docker login --username AWS --password-stdin <account-id>.dkr.ecr.us-east-1.amazonaws.com`
	`Login Succeeded`
	où `<account-id>` fait référence à votre Compte AWS.
	2. Marquez l'image locale que vous avez extraite précédemment. Utilisez la valeur `public.ecr.aws/amazonlinux/amazonlinux:2018.03` et transférez-la vers le référentiel privé Amazon ECR.
	`$~ % docker tag public.ecr.aws/amazonlinux/amazonlinux:2018.03 <account-id>.dkr.ecr.us-east-1.amazonaws.com/`
		Administrateur AWS, AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises

	`test_ecr_repositor y:latest`
	
	`$~ % docker push <account-id>.dkr.e cr.us-east-1.amazo naws.com/test_ecr_ repository:latest`
	
	Lorsque vous transférez l'image vers le référenti el Amazon ECR, Docker envoie l'image sous-jacente et non l'index de l'image.
	
	`The push refers to repository [<account -id>.dkr.ecr.us-ea st-1.amazonaws.com/ test_ecr_repository] d5655967c2c4: Pushed latest: digest: sha256:52db9000073 d93b9bdee6a7246a68 c35a741aaade05a8f4 febba0bf795cdac02 size: 529`	

Tâche	Description	Compétences requises

Extrayez la même image depuis le référentiel privé Amazon ECR.	1. Depuis le terminal, exécutez la commande suivante pour extraire l'image que vous avez précédemment envoyée vers le référentiel privé Amazon ECR.
	
	`$~ % docker pull <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`latest: Pulling from test_ecr_repository`
	`Digest: sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02`
	`Status: Image is up to date for <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	`<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	Le résumé de cette image correspond au résumé de l'image que vous avez envoyée au référentiel privé Amazon ECR et représente l'image sous-jacente. Cette valeur ne correspond pas
		Développeur d'applications, AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises

	à l'index d'image que vous avez extrait du référentiel public.
	2. Pour vérifier, récupérez l'index de l'image par condensé.
	
	`curl -k -H “Authorization: Bearer $TOKEN” https://public.ecr.aws/v2/amazonlinux/amazonlinux/manifests/sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b55`
	`{ “schemaVersion”: 2, “mediaType”: “application/vnd.docker.distribution.manifest.list.v2+json”, “manifests”: [ { “mediaType”: “application/vnd.docker.distribution.manifest.v2+json”, “size”: 529, “digest”: “sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02", “platform”: {`	

Tâche	Description	Compétences requises

	<pre>“architec
	ture”: “amd64”,
	“os”:
	“linux”
	}
	}
	]
	}</pre>	

Comparez les manifestes d'images

Tâche	Description	Compétences requises

Recherchez le manifeste de l'image stockée dans le référentiel public Amazon ECR.	Depuis le terminal, exécutez la commande suivante pour extraire le manifeste de l'image `public.ecr.aws/amazonlinux/amazonlinux:2018.03` depuis le référentiel public Amazon ECR.
	<pre>$~ % docker manifest
	inspect public.ec
	r.aws/amazonlinux/
	amazonlinux:2018.03
	{
	"schemaVersion": 2,
	"mediaType":
	"application/vnd.d
	ocker.distribution
	.manifest.list.v2+
	json",
	"manifests": [
	{
	"mediaType":
	"application/vnd.d</pre>
		Administrateur AWS, AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises

	ocker.distribution
	.manifest.v2+json",
	"size": 529,
	"digest":
	"sha256:52db900007
	3d93b9bdee6a7246a6
	8c35a741aaade05a8f
	4febba0bf795cdac02",
	"platform": {
	"architec
	ture": "amd64",
	"os":
	"linux"
	}
	}
	]
	}	

Tâche	Description	Compétences requises

Trouvez le manifeste de l'image stockée dans le référentiel privé Amazon ECR.	Depuis le terminal, exécutez la commande suivante pour extraire le manifeste de l'image `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` depuis le référentiel privé Amazon ECR.
	
	`$~ % docker manifest inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	
	`{ "schemaVersion": 2, "mediaType": "application/vnd.docker.distribution.manifest.v2+json", "config": { "mediaType": "application/vnd.docker.container.image.v1+json", "size": 1477, "digest": "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68" }, "layers": [ {`
		AWS DevOps, administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
	"mediaType": "application/vnd.docker.image.rootfs.diff.tar.gzip", "size": 62267075, "digest": "sha256:4ddc0f8d367f424871a060e2067749f32bd36a91085e7140dcb159952f2d71453" }] }	

Tâche	Description	Compétences requises
Comparez le résumé extrait par Docker avec le résumé du manifeste de l'image dans le référentiel privé Amazon ECR.	Une autre question est de savoir pourquoi le résumé fourni par la commande docker pull diffère du résumé du manifeste pour l'image. `<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest` Le condensé utilisé pour docker pull représente le condensé du manifeste d'image, qui est stocké dans un registre. Ce condensé est considéré comme la racine d'une chaîne de hachage, car le manifeste contient le hachage du contenu qui sera téléchargé et importé dans Docker. L'ID d'image utilisé dans Docker se trouve dans ce manifeste sous `config.digest` la forme. Cela représente la configuration d'image utilisée par Docker. On pourrait donc dire que le manifeste est l'enveloppe et que l'image est le contenu de l'enveloppe. Le résumé du manifeste est toujours différent de l'ID de l'image. Cependant, un manifeste spécifiqu	AWS DevOps, administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
	e doit toujours produire le même identifiant d'image. Le résumé du manifeste étant une chaîne de hachage, nous ne pouvons pas garantir qu'il sera toujours le même pour un identifiant d'image donné. Dans la plupart des cas, il produit le même résumé, bien que Docker ne puisse pas le garantir. La différenc e possible dans le résumé du manifeste provient du fait que Docker ne stocke pas les blobs compressés avec gzip localement. Par conséquent, l'exportation de couches peut produire un condensé différent , même si le contenu non compressé reste le même. L'identifiant de l'image vérifie que le contenu non compressé est identique ; c'est-à-dire que l'identifiant de l'image est désormais un identifia nt adressable au contenu (). `chainID`	
	Pour confirmer ces informati ons, vous pouvez comparer le résultat de la commande docker inspect sur les référenti els publics et privés Amazon ECR :	

Tâche	Description	Compétences requises

	1. Exécutez la commande suivante depuis votre terminal pour l'image stockée dans le référentiel public Amazon ECR.
	`$~ % docker inspect public.ecr.aws/amazonlinux/amazonlinux:2018.03`
	Pour le résultat de la commande, consultez la section Informations supplémentaires.
	2. Exécutez la commande suivante depuis votre terminal pour l'image stockée dans le référentiel privé Amazon ECR.
	`$~ % docker inspect <account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest`
	Pour le résultat de la commande, consultez la section Informations supplémentaires.
	Les résultats vérifient que les deux images ont le même	

Tâche	Description	Compétences requises
	condensé d'ID d'image et le même résumé de couche. Identifiant : `f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68` Couches : `d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2` En outre, les résumés sont basés sur les octets de l'objet géré localement (le fichier local est un tar de la couche d'image du conteneur) ou sur le blob transmis au serveur de registre. Toutefois, lorsque vous transférez le blob vers un registre, le tar est compressé et le condensé est calculé dans le fichier tar compressé . Par conséquent, la différence entre la valeur du docker pull digest provient de la compression appliquée au niveau du registre (Amazon ECR privé ou public). **Note** Cette explication est spécifique à l'utilisation d'un client Docker.	

Tâche	Description	Compétences requises
	Vous ne verrez pas ce comportement avec d'autres clients tels que nerdctl ou Finch, car ils ne compressent pas automatiquement l'image lors des opérations push et pull.	

Identifiez automatiquement les images dupliquées entre les référentiels publics et privés d'Amazon ECR

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le dépôt Github pour ce modèle dans un dossier local : `$git clone https://github.com/aws-samples/automated-solution-to-identify-duplicate-container-images-between-repositories`	Administrateur AWS, AWS DevOps
Configurez un pipeline CI/CD.	Le GitHub référentiel inclut un `.yaml` fichier qui crée une AWS CloudFormation pile dans laquelle configurer un pipeline AWS CodePipeline. 1. Connectez-vous à la AWS CloudFormation console	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	AWS Management Console et ouvrez-la. 2. Créez une pile à l'aide du `pipeline.yaml` fichier modèle, qui se trouve dans le `code` dossier du référentiel cloné. 3. Acceptez ou modifiez les valeurs par défaut des paramètres. Spécifiez les valeurs suivantes : • Nom de la pile • `ArtifactStoreBucketName` — Un compartiment S3 existant qui sera utilisé pour stocker AWS CodePipeline des artefacts • `OutputBucket` — Un compartiment S3 existant qui sera utilisé pour stocker les URIs images dupliquées • `SourceImageFile` — Un fichier texte existant nommé `input.txt` qui contient l'image URIs du référentiel public qui sera comparée au référentiel privé Amazon ECR pour détecter les doublons 4. Passez en revue et ajustez les options de pile, puis	

Tâche	Description	Compétences requises
	choisissez Soumettre pour exécuter le modèle. Le pipeline sera configuré en deux étapes (CodeCommit et CodeBuild, comme indiqué dans le schéma d'architecture) pour identifier les images du référentiel privé qui existent également dans le référenti el public. Le pipeline est configuré avec les ressources suivantes : • CodePipeline pour l'orchest ration du pipeline de déploiement. • Un CodeCommit référenti el pour stocker le script bash et le fichier d'entrée. Le script bash est utilisé pour comparer l'image du conteneur IDs dans les référentiels public et privé afin de trouver des doublons. Cette vérification est effectuée sur tous les référentiels du référentiel spécifié Compte AWS en un seul Région AWS. • Un CodeBuild projet visant à invoquer le script bash pour identifier les images déjà	

Tâche	Description	Compétences requises
	présentes dans le référentiel Amazon ECR. • Rôles IAM nécessaires pour autoriser l'accès. • Un compartiment S3 pour stocker le fichier de sortie contenant l'image URIs. • Un autre compartiment S3 pour stocker les CodePipel ine artefacts.	

Tâche	Description	Compétences requises
Renseignez le CodeCommit référentiel.	Pour remplir le CodeCommit référentiel, effectuez les opérations suivantes : 1. Ouvrez la CodeCommit console et naviguez jusqu'à l' Région AWS endroit où vous avez créé la CloudFormation pile. 2. Recherchez le référentiel que vous avez mis en service à l'aide du CloudFormation script dans la liste, choisissez Cloner l'URL, puis copiez le protocole URL HTTPS pour vous connecter au référentiel. 3. Ouvrez une invite de commande et exécutez la commande git clone avec l'URL HTTPS que vous avez copiée à l'étape précédente. 4. Accédez au répertoire racine. Créez un fichier nommé `input.txt` et remplissez-le avec le registre d'images public Amazon ECR URIs que vous souhaitez rechercher dans le référentiel privé Amazon ECR.	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

	5. Copiez les fichiers `script.sh buildspec .yml` , et `input.txt` depuis votre copie locale du GitHub référentiel Solution automatisée pour identifier les images de conteneur dupliquées entre les référentiels vers le référentiel cloné CodeCommit .
	6. Téléchargez les fichiers dans le répertoire CodeCommit à l'aide des commandes suivantes :
	`git add .`
	`git commit -m “added input files”`
	`git push`	

Nettoyer.	Pour éviter d'encourir de futurs frais, supprimez les ressources en procédant comme suit : 1. Accédez au compartiment S3 qui stocke les CodePipeline artefacts et videz-le. 2. Accédez au compartiment S3 qui stocke l'image URIs dupliquée et videz-le. 3. Accédez à la CloudFormation console et supprimez la pile que vous avez créée pour configurer le pipeline.	Administrateur AWS

Résolution des problèmes

Problème	Solution
Lorsque vous essayez de pousser, d'extraire ou d'interagir avec un CodeCommit référenti el depuis le terminal ou la ligne de commande, vous êtes invité à fournir un nom d'utilisateur et un mot de passe, et vous devez fournir les informations d'identification Git de votre utilisate ur IAM.	Les causes les plus fréquentes de cette erreur sont les suivantes : • Votre ordinateur local exécute un système d'exploitation qui ne prend pas en charge la gestion des informations d'identification, ou aucun utilitaire de gestion des informations d'identification n'est installé. • Les informations d'identification Git de votre utilisateur IAM n'ont pas été enregistrées dans l'un de ces systèmes de gestion des informations d'identification. En fonction de votre système d'exploitation et de votre environnement local, vous devrez peut-être installer un gestionnaire d'informa tions d'identification, configurer celui qui est inclus dans votre système d'exploitation ou personnaliser votre environnement local de manière à utiliser le stockage des informations d'identification. Par exemple, si votre ordinateu r exécute macOS, vous pouvez utiliser l'utilita ire Keychain Access pour stocker vos informati ons d'identification. Si votre ordinateur est sous Windows, vous pouvez utiliser le gestionnaire d'informations d'identification Git installé avec Git pour Windows. Pour plus d'informations, consultez Configuration pour les utilisateurs HTTPS à l'aide des informations d'identification Git dans la CodeCommit documentation et Stockage des informations d'identification dans la documentation Git.

Problème	Solution
Vous rencontrez des erreurs HTTP 403 ou « aucun identifiant d'authentification de base » lorsque vous transférez une image vers le référentiel Amazon ECR.	Ces messages d'erreur peuvent provenir de la commande docker push ou docker pull, même si vous vous êtes authentifié avec succès auprès de Docker à l'aide de la commande aws ecr. get-login-password Les causes connues sont les suivantes : • Vous vous êtes authentifié dans une autre région. Pour plus d'informations, consultez la section Authentification du registre privé dans la documentation Amazon ECR. • Vous vous êtes authentifié pour envoyer un envoi vers un référentiel pour lequel vous n'êtes pas autorisé. Pour plus d'informations, consultez la section Politiques relatives aux référentiels privés dans la documentation Amazon ECR. • Votre jeton a expiré. La période d'expiration par défaut pour les jetons obtenus à l'aide de cette `GetAuthorizationToken` opération est de 12 heures.

Ressources connexes

- Solution automatisée pour identifier les images de conteneur dupliquées entre les référentiels (GitHub référentiel)
- Galerie publique Amazon ECR
- Images privées dans Amazon ECR (documentation Amazon ECR)
- AWS::CodePipeline::Pipeline ressource (AWS CloudFormation documentation)
- Spécification du format d'image OCI

Informations supplémentaires

Résultat de l'inspection Docker pour l'image dans le référentiel public Amazon ECR


```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
```

```
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
 "sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
```

```
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Résultat de l'inspection Docker pour l'image dans le référentiel privé Amazon ECR

```
[
    {
        "Id":
 "sha256:f7cee5e1af28ad4e147589c474d399b12d9b551ef4c3e11e02d982fce5eebc68",
        "RepoTags": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/test_ecr_repository:latest",
            "public.ecr.aws/amazonlinux/amazonlinux:2018.03"
        ],
        "RepoDigests": [
            "<account-id>.dkr.ecr.us-east-1.amazonaws.com/
test_ecr_repository@sha256:52db9000073d93b9bdee6a7246a68c35a741aaade05a8f4febba0bf795cdac02",
            "public.ecr.aws/amazonlinux/
amazonlinux@sha256:f972d24199508c52de7ad37a298bda35d8a1bd7df158149b381c03f6c6e363b5"
        ],
        "Parent": "",
        "Comment": "",
        "Created": "2023-02-23T06:20:11.575053226Z",
        "Container":
 "ec7f2fc7d2b6a382384061247ef603e7d647d65f5cd4fa397a3ccbba9278367c",
        "ContainerConfig": {
            "Hostname": "ec7f2fc7d2b6",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
```

```
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/sh",
                "-c",
                "#(nop) ",
                "CMD [\"/bin/bash\"]"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
            "OnBuild": null,
            "Labels": {}
        },
        "DockerVersion": "20.10.17",
        "Author": "",
        "Config": {
            "Hostname": "",
            "Domainname": "",
            "User": "",
            "AttachStdin": false,
            "AttachStdout": false,
            "AttachStderr": false,
            "Tty": false,
            "OpenStdin": false,
            "StdinOnce": false,
            "Env": [
                "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
            ],
            "Cmd": [
                "/bin/bash"
            ],
            "Image":
"sha256:c1bced1b5a65681e1e0e52d0a6ad17aaf76606149492ca0bf519a466ecb21e51",
            "Volumes": null,
            "WorkingDir": "",
            "Entrypoint": null,
```

```
            "OnBuild": null,
            "Labels": null
        },
        "Architecture": "amd64",
        "Os": "linux",
        "Size": 167436755,
        "VirtualSize": 167436755,
        "GraphDriver": {
            "Data": {
                "MergedDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/merged",
                "UpperDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/diff",
                "WorkDir": "/var/lib/docker/overlay2/
c2c2351a82b26cbdf7782507500e5adb5c2b3a2875bdbba79788a4b27cd6a913/work"
            },
            "Name": "overlay2"
        },
        "RootFS": {
            "Type": "layers",
            "Layers": [

 "sha256:d5655967c2c4e8d68f8ec7cf753218938669e6c16ac1324303c073c736a2e2a2"
            ]
        },
        "Metadata": {
            "LastTagTime": "2023-03-02T10:28:47.142155987Z"
        }
    }
]
```

Installation de l'agent SSM sur les nœuds de travail Amazon EKS à l'aide de Kubernetes DaemonSet

Créée par Mahendra asiddappa (AWS)

Récapitulatif

Remarque, septembre 2021 : la dernière version optimisée d'Amazon EKS AMIs installe automatiquement l'agent SSM. Pour plus d'informations, consultez les notes de publication du mois de juin 2021 AMIs.

Dans Amazon Elastic Kubernetes Service (Amazon EKS), pour des raisons de sécurité, aucune paire de clés Secure Shell (SSH) n'est associée aux nœuds de travail. Ce modèle montre comment utiliser le type de DaemonSet ressource Kubernetes pour installer l'agent AWS Systems Manager (agent SSM) sur tous les nœuds de travail, au lieu de l'installer manuellement ou de remplacer l'Amazon Machine Image (AMI) pour les nœuds. DaemonSet utilise une tâche cron sur le nœud de travail pour planifier l'installation de l'agent SSM. Vous pouvez également utiliser ce modèle pour installer d'autres packages sur les nœuds de travail.

Lorsque vous résolvez des problèmes dans le cluster, l'installation de l'agent SSM à la demande vous permet d'établir une session SSH avec le nœud de travail, de collecter des journaux ou d'examiner la configuration de l'instance, sans paires de clés SSH.

Conditions préalables et limitations

Prérequis

- Un cluster Amazon EKS existant avec des nœuds de travail Amazon Elastic Compute Cloud (Amazon EC2).
- Les instances de conteneur doivent disposer des autorisations requises pour communiquer avec le service SSM. Le rôle géré AWS Identity and Access Management (IAM) Amazon SSMManaged InstanceCore fournit les autorisations requises pour que l'agent SSM s'exécute sur EC2 des instances. Pour plus d'informations, consultez la documentation d'AWS Systems Manager.

Limites

- Ce modèle ne s'applique pas à AWS Fargate, DaemonSets car il n'est pas pris en charge sur la plateforme Fargate.
- Ce modèle s'applique uniquement aux nœuds de travail basés sur Linux.

- Les DaemonSet pods fonctionnent en mode privilégié. Si le cluster Amazon EKS possède un webhook qui bloque les pods en mode privilégié, l'agent SSM ne sera pas installé.

Architecture

Le schéma suivant illustre l'architecture de ce modèle.

Outils

Outils

- kubectl est un utilitaire de ligne de commande utilisé pour interagir avec un cluster Amazon EKS. Ce modèle est utilisé `kubectl` pour déployer un agent DaemonSet sur le cluster Amazon EKS, qui installera l'agent SSM sur tous les nœuds de travail.
- Amazon EKS vous permet d'exécuter facilement Kubernetes sur AWS sans avoir à installer, exploiter et gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes. Kubernetes est un système open source destiné à l'automatisation du déploiement, la mise à l'échelle et la gestion d'applications conteneurisées.
- AWS Systems Manager Session Manager vous permet de gérer vos EC2 instances, vos instances sur site et vos machines virtuelles (VMs) via un shell interactif basé sur un navigateur en un clic ou via l'interface de ligne de commande AWS (AWS CLI).

Code

Utilisez le code suivant pour créer un fichier DaemonSet de configuration qui installera l'agent SSM sur le cluster Amazon EKS. Suivez les instructions de la section Epics.

```
cat << EOF > ssm_daemonset.yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  labels:
    k8s-app: ssm-installer
  name: ssm-installer
  namespace: kube-system
spec:
  selector:
    matchLabels:
```

```
      k8s-app: ssm-installer
  template:
    metadata:
      labels:
        k8s-app: ssm-installer
    spec:
      containers:
      - name: sleeper
        image: busybox
        command: ['sh', '-c', 'echo I keep things running! && sleep 3600']
      initContainers:
      - image: amazonlinux
        imagePullPolicy: Always
        name: ssm
        command: ["/bin/bash"]
        args: ["-c","echo '* * * * * root yum install -y https://s3.amazonaws.com/
ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm & rm -rf /etc/
cron.d/ssmstart' > /etc/cron.d/ssmstart"]
        securityContext:
          allowPrivilegeEscalation: true
        volumeMounts:
        - mountPath: /etc/cron.d
          name: cronfile
        terminationMessagePath: /dev/termination-log
        terminationMessagePolicy: File
      volumes:
      - name: cronfile
        hostPath:
          path: /etc/cron.d
          type: Directory
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      terminationGracePeriodSeconds: 30
EOF
```

Épopées

Configurer kubectl

Tâche	Description	Compétences requises
Installez et configurez kubectl pour accéder au cluster EKS.	S'il `kubectl` n'est pas déjà installé et configuré pour accéder au cluster Amazon EKS, consultez la section Installation de kubectl dans la documentation Amazon EKS.	DevOps

Déployez le DaemonSet

Tâche	Description	Compétences requises
Créez le fichier DaemonSet de configuration.	Utilisez le code de la section Code plus haut dans ce modèle pour créer un fichier de DaemonSet configuration appelé `ssm_daemonset.yaml`, qui sera déployé sur le cluster Amazon EKS. La nacelle lancée par DaemonSet possède un conteneur principal et un `init` conteneur. Le conteneur principal possède une `sleep` commande. Le `init` conteneur inclut une `command` section qui crée un fichier de travail cron pour installer l'agent SSM sur le chemin. `/etc/cron.d/` La tâche cron	DevOps

Tâche	Description	Compétences requises
	ne s'exécute qu'une seule fois et le fichier qu'elle crée est automatiquement supprimé une fois la tâche terminée. Lorsque le conteneur d'initialisation est terminé, le conteneur principal attend 60 minutes avant de sortir. Au bout de 60 minutes, un nouveau module est lancé. Ce module installe l'agent SSM, s'il est manquant, ou met à jour l'agent SSM vers la dernière version. Si nécessaire, vous pouvez modifier la `sleep` commande pour redémarrer le module une fois par jour ou pour l'exécuter plus souvent.	
Déployez le DaemonSet sur le cluster Amazon EKS.	Pour déployer le fichier DaemonSet de configuration que vous avez créé à l'étape précédente sur le cluster Amazon EKS, utilisez la commande suivante : `kubectl apply -f ssm_daemonset.yaml` Cette commande crée un DaemonSet pour exécuter les pods sur les nœuds de travail afin d'installer l'agent SSM.	DevOps

Ressources connexes

- Installation de kubectl (documentation Amazon EKS)
- Configuration du gestionnaire de sessions (documentation AWS Systems Manager)

Installez l'agent SSM et l' CloudWatch agent sur les nœuds de travail Amazon EKS à l'aide de preBootstrapCommands

Créée par Akkamahadevi Hiremath (AWS)

Récapitulatif

Ce modèle fournit des exemples de code et des étapes pour installer l'agent AWS Systems Manager (agent SSM) et l' CloudWatch agent Amazon sur les nœuds de travail Amazon Elastic Kubernetes Service (Amazon EKS) dans le cloud Amazon Web Services (AWS) lors de la création du cluster Amazon EKS. Vous pouvez installer l'agent SSM et l' CloudWatch agent en utilisant la `preBootstrapCommands` propriété du schéma du fichier de `eksctl` configuration (documentation Weaveworks). Vous pouvez ensuite utiliser l'agent SSM pour vous connecter à vos nœuds de travail sans utiliser de paire de clés Amazon Elastic Compute Cloud (Amazon EC2). En outre, vous pouvez utiliser l' CloudWatch agent pour surveiller l'utilisation de la mémoire et du disque sur vos nœuds de travail Amazon EKS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- L'utilitaire de ligne de commande eksctl, installé et configuré sur macOS, Linux ou Windows
- L'utilitaire de ligne de commande kubectl, installé et configuré sur macOS, Linux ou Windows

Limites

- Nous vous recommandons d'éviter d'ajouter des scripts de longue durée à la `preBootstrapCommands` propriété, car cela retarde l'adhésion du nœud au cluster Amazon EKS pendant les activités de dimensionnement. Nous vous recommandons plutôt de créer une Amazon Machine Image (AMI) personnalisée.
- Ce modèle s'applique uniquement aux instances Amazon EC2 Linux.

Architecture

Pile technologique

- Amazon CloudWatch
- Amazon Elastic Kubernetes Service (Amazon EKS)
- AWS Systems Manager Parameter Store

Architecture cible

Le schéma suivant montre un exemple d'utilisateur se connectant aux nœuds de travail Amazon EKS à l'aide de l'agent SSM installé à l'aide du`preBootstrapCommands`.

Le schéma suivant illustre le flux de travail suivant :

1. L'utilisateur crée un cluster Amazon EKS en utilisant le fichier `eksctl` de configuration avec la `preBootstrapCommands` propriété, qui installe l'agent SSM et CloudWatch l'agent.
2. Toute nouvelle instance qui rejoint le cluster ultérieurement en raison d'activités de dimensionnement est créée avec l'agent SSM et CloudWatch l'agent préinstallés.
3. L'utilisateur se connecte à Amazon à l'aide EC2 de l'agent SSM, puis surveille l'utilisation de la mémoire et du disque à l'aide de l' CloudWatch agent.

Outils

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.
- AWS Systems Manager Session Manager vous aide à gérer vos EC2 instances, vos instances sur site et vos machines virtuelles via un shell interactif basé sur un navigateur en un clic ou via l'interface de ligne de commande AWS (AWS CLI).
- eksctl est un utilitaire de ligne de commande permettant de créer et de gérer des clusters Kubernetes sur Amazon EKS.
- kubectl est un utilitaire de ligne de commande permettant de communiquer avec le serveur API du cluster.

Épopées

Création d'un cluster Amazon EKS

Tâche	Description	Compétences requises
Stockez le fichier de configuration de l' CloudWatch agent.	Stockez le fichier de configuration de l' CloudWatch agent dans le AWS Systems Manager Parameter Store de la région AWS dans laquelle vous souhaitez créer votre cluster Amazon EKS. Pour ce faire, créez un paramètre dans AWS Systems Manager Parameter Store et notez le nom du paramètre (par exemple,`AmazonCloudwatch-linux`). Pour plus d'informations, consultez l'exemple de code de fichier de configuration de l' CloudWatch agent dans la section Informations supplémentaires de ce modèle.	DevOps ingénieur
Créez le fichier de configuration et le cluster eksctl.	1. Créez un fichier `eksctl` de configuration qui inclut les étapes d'installation de l' CloudWatch agent et de l'agent SSM. Pour plus d'informations, consultez l'exemple de code de fichier de configuration eksctl dans la section Informati	AWS DevOps

Tâche	Description	Compétences requises
	ons supplémentaires de ce modèle. 2. Créez un cluster en exécutant la `eksctl create cluster -f cluster.yaml` commande.	

Vérifiez que l'agent SSM et l' CloudWatch agent fonctionnent

Tâche	Description	Compétences requises
Testez l'agent SSM.	Utilisez SSH pour vous connecter à vos nœuds de cluster Amazon EKS en utilisant l'une des méthodes décrites dans la section Démarrer une session dans la documentation AWS Systems Manager.	AWS DevOps
Testez l' CloudWatch agent.	Utilisez la CloudWatch console pour valider l' CloudWatch agent : 1. Connectez-vous à AWS Management Console et ouvrez la console CloudWatch . 2. Dans le volet de navigation, développez Metrics, puis choisissez All metrics. 3. Dans le champ de recherche de l'onglet	AWS DevOps

Tâche	Description	Compétences requises
	Parcourir, entrez puis choisissez CWAgent des métriques pour voir les métriques de mémoire et de disque.	

Ressources connexes

- Installation et exécution de l' CloudWatch agent sur vos serveurs (CloudWatch documentation Amazon)
- Création d'un paramètre Systems Manager (console) (documentation AWS Systems Manager)
- Création du fichier de configuration de l' CloudWatch agent (CloudWatch documentation Amazon)
- Démarrage d'une session (AWS CLI) (documentation AWS Systems Manager)
- Démarrage d'une session (EC2 console Amazon) (documentation AWS Systems Manager)

Informations supplémentaires

Exemple de fichier CloudWatch de configuration de l'agent

Dans l'exemple suivant, l' CloudWatch agent est configuré pour surveiller l'utilisation du disque et de la mémoire sur les instances Amazon Linux :

```
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "disk": {
```

```
                "measurement": [
                    "used_percent"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            },
            "mem": {
                "measurement": [
                    "mem_used_percent"
                ],
                "metrics_collection_interval": 60
            }
        }
    }
}
```

Exemple de fichier de configuration eksctl

```
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig
metadata:
  name: test
  region: us-east-2
  version: "1.24"
managedNodeGroups:
  - name: test
    minSize: 2
    maxSize: 4
    desiredCapacity: 2
    volumeSize: 20
    instanceType: t3.medium
    preBootstrapCommands:
    - sudo yum install amazon-ssm-agent -y
    - sudo systemctl enable amazon-ssm-agent
    - sudo systemctl start amazon-ssm-agent
    - sudo yum install amazon-cloudwatch-agent -y
    - sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-
config -m ec2 -s -c ssm:AmazonCloudwatch-linux
    iam:
      attachPolicyARNs:
        - arn:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy
```

```
        - arn:aws:iam::aws:policy/AmazonEKS_CNI_Policy
        - arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly
        - arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
        - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore
```

Informations supplémentaires sur le code

- Dans la dernière ligne de la `preBootstrapCommands` propriété `AmazonCloudwatch-linux` se trouve le nom du paramètre créé dans le magasin de paramètres AWS System Manager. Vous devez l'inclure `AmazonCloudwatch-linux` dans Parameter Store dans la même région AWS où vous avez créé le cluster Amazon EKS. Vous pouvez également spécifier un chemin de fichier, mais nous vous recommandons d'utiliser Systems Manager pour faciliter l'automatisation et la réutilisation.
- Si vous les utilisez `preBootstrapCommands` dans le fichier `eksctl` de configuration, deux modèles de lancement s'affichent dans l'AWS Management Console. Le premier modèle de lancement inclut les commandes spécifiées dans`preBootstrapCommands`. Le second modèle inclut les commandes spécifiées dans les données utilisateur Amazon EKS par défaut `preBootstrapCommands` et les contient. Ces données sont nécessaires pour que les nœuds rejoignent le cluster. Le groupe Auto Scaling du groupe de nœuds utilise ces données utilisateur pour créer de nouvelles instances.
- Si vous utilisez l'`iam`attribut dans le fichier de `eksctl` configuration, vous devez répertorier les politiques Amazon EKS par défaut ainsi que toutes les politiques supplémentaires requises dans les politiques AWS Identity and Access Management (IAM) jointes. Dans l'extrait de code issu de l'étape Créer le fichier de configuration et le cluster eksctl, `CloudWatchAgentServerPolicy` des politiques supplémentaires `AmazonSSMMangedInstanceCore` sont ajoutées pour garantir que l' CloudWatch agent et l'agent SSM fonctionnent comme prévu. Les `AmazonEC2ContainerRegistryReadOnly` politiques `AmazonEKSWorkerNodePolicyAmazonEKS_CNI_Policy`, sont des politiques obligatoires requises pour que le cluster Amazon EKS fonctionne correctement.

Migrer les contrôleurs d'entrée NGINX lors de l'activation du mode automatique Amazon EKS

Créée par Olawale Olaleye (AWS) et Shamanth Devagari (AWS)

Récapitulatif

Le mode automatique EKS pour Amazon Elastic Kubernetes Service (Amazon EKS) peut réduire la charge opérationnelle liée à l'exécution de vos charges de travail sur des clusters Kubernetes. Ce mode AWS permet également de configurer et de gérer l'infrastructure en votre nom. Lorsque vous activez le mode automatique EKS sur un cluster existant, vous devez planifier soigneusement la migration des configurations du contrôleur d'entrée NGINX. Cela est dû au fait que le transfert direct d'équilibreurs de charge réseau n'est pas possible.

Vous pouvez utiliser une stratégie de déploiement bleu/vert pour migrer une instance de NGINX Ingress Controller lorsque vous activez le mode automatique EKS dans un cluster Amazon EKS existant.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un cluster Amazon EKS exécutant Kubernetes version 1.29 ou ultérieure
- Extensions Amazon EKS exécutant des versions minimales
- Dernière version de kubectl
- Une instance de NGINX Ingress Controller existante
- (Facultatif) Une zone hébergée dans Amazon Route 53 pour le transfert de trafic basé sur le DNS

Architecture

Un déploiement bleu/vert est une stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Les déploiements bleu/vert offrent des fonctionnalités de lancement et de restauration quasi nulles. L'idée fondamentale est de transférer le trafic entre deux environnements identiques qui exécutent des versions différentes de votre application.

L'image suivante montre la migration des équilibreurs de charge réseau à partir de deux instances différentes de NGINX Ingress Controller lors de l'activation du mode automatique EKS. Vous utilisez un déploiement bleu/vert pour transférer le trafic entre les deux équilibreurs de charge réseau.

L'espace de noms d'origine est l'espace de noms bleu. C'est ici que s'exécutent le service et l'instance NGINX Ingress Controller d'origine, avant que vous n'activiez le mode automatique EKS. Le service et l'instance d'origine se connectent à un Network Load Balancer dont le nom DNS est configuré dans Route 53. Le AWS Load Balancer Controller a déployé ce Network Load Balancer dans le cloud privé virtuel (VPC) cible.

Le schéma montre le flux de travail suivant pour configurer un environnement pour un déploiement bleu/vert :

1. Installez et configurez une autre instance de NGINX Ingress Controller dans un espace de noms différent, un espace de noms vert.
2. Dans Route 53, configurez un nom DNS pour un nouveau Network Load Balancer.

Outils

Services AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Elastic Load Balancing répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Autres outils

- Helm est un gestionnaire de packages open source pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes.

- kubectl est une interface de ligne de commande qui vous permet d'exécuter des commandes sur des clusters Kubernetes.
- Le NGINX Ingress Controller connecte les applications et les services Kubernetes à la gestion des demandes, à l'authentification, aux ressources personnalisées en libre-service et au débogage.

Épopées

Passez en revue l'environnement existant

Tâche	Description	Compétences requises

Vérifiez que l'instance NGINX Ingress Controller d'origine est opérationnelle.	Entrez la commande suivante pour vérifier que les ressources de l'espace de `ingress-nginx` noms sont opérationnelles. Si vous avez déployé NGINX Ingress Controller dans un autre espace de noms, mettez à jour le nom de l'espace de noms dans cette commande.
	`kubectl get all -n ingress-nginx`
	Dans le résultat, vérifiez que les pods du NGINX Ingress Controller sont en cours d'exécution. Voici un exemple de résultat :
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-xqn9d`
		DevOps ingénieur

Tâche	Description	Compétences requises
	0/1 Completed 0 88m pod/ingress-nginx-admission-patch-lhk4j 0/1 Completed 1 88m pod/ingress-nginx-controller-68f68f859-xrz74 1/1 Running 2 (10m ago) 72m NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/ingress-nginx-controller LoadBalancer 10.100.67.255 k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80:30330/TCP,443:31462/TCP 88m service/ingress-nginx-controller-admission ClusterIP 10.100.201.176 <none> 443/TCP 88m NAME	

Tâche	Description	Compétences requises
	READY UP-TO-DATE AVAILABLE AGE deployment.apps/ingress-nginx-controller 1/1 1 1 88m NAME DESIRED CURRENT READY AGE replicaset.apps/ingress-nginx-controller-68f68f859 1 1 1 72m replicaset.apps/ingress-nginx-controller-d8c96cf68 0 0 0 88m NAME STATUS COMPLETIONS DURATION AGE job.batch/ingress-nginx-admission-create Complete 1/1 4s 88m job.batch/ingress-nginx-admission-patch Complete 1/1 5s 88m	

Déployez un exemple de HTTPd charge de travail pour utiliser le NGINX Ingress Controller

Tâche	Description	Compétences requises

Créez les ressources Kubernetes.	Entrez les commandes suivantes pour créer un exemple de déploiement, de service et d'entrée Kubernetes :
	`kubectl create deployment demo --image=httpd --port=80`
	`kubectl expose deployment demo`
	`kubectl create ingress demo --class=nginx \ --rule nginxautomode.local.dev/=demo:80`
		DevOps ingénieur

Passez en revue les ressources déployées.	Entrez la commande suivante pour afficher la liste des ressources déployées :
	`kubectl get all,ingress`
	Dans le résultat, vérifiez que le HTTPd module d'échantillonnage est en cours d'exécution. Voici un exemple de résultat :
	`NAME READY STATUS RESTARTS AGE`
		DevOps ingénieur

Tâche	Description	Compétences requises
	pod/demo-7d94f8cb4f-q68wc 1/1 Running 0 59m NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE service/demo ClusterIP 10.100.78.155 <none> 80/TCP 59m service/kubernetes ClusterIP 10.100.0.1 <none> 443/TCP 117m NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/demo 1/1 1 1 59m NAME DESIRED CURRENT READY AGE replicaset.apps/demo-7d94f8cb4f 1 1 1 59m NAME CLASS HOSTS ADDRESS PORTS AGE ingress.networking.k8s.io/demo	

Tâche	Description	Compétences requises
	`nginx nginxauto mode.local.dev k8s-ingress-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80 56m`	

Vérifiez que le service est joignable.	Entrez la commande suivante pour vérifier que le service est accessible via le nom DNS du Network Load Balancer :
	`curl -H "Host: nginxautomode.local.dev" http://k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com`
	Le résultat attendu est le suivant :
	`<html><body><h1>It works!</h1></body></html>`
		DevOps ingénieur

Tâche	Description	Compétences requises

(Facultatif) Créez un enregistrement DNS.	1. Suivez les instructions de la section Création d'enregistrements à l'aide de la console Amazon Route 53 (documentation Route 53) pour créer un enregistrement DNS pour le domaine configuré.
	2. Entrez la commande suivante pour confirmer que le service est accessible via le nom de domaine configuré :
	`curl "http://nginxautomode.local.dev/?[1-5]"`
	Le résultat attendu est le suivant :
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
	`<html><body><h1>It works!</h1></body></html>`
		DevOps ingénieur, AWS DevOps

Activer le mode automatique EKS sur le cluster existant

Tâche	Description	Compétences requises
Activez le mode automatique EKS.	Suivez les instructions de la section Activer le mode automatique EKS sur un cluster existant (documentation Amazon EKS).	AWS DevOps

Installer un nouveau contrôleur d'entrée NGINX

Tâche	Description	Compétences requises

Configurez une nouvelle instance de NGINX Ingress Controller.	1. Téléchargez le modèle deploy.yaml.
	2. Ouvrez le modèle deploy.yaml dans votre éditeur préféré.
	3. Dans la `kind: Namespace` section, entrez un nom unique pour l'espace de noms, tel que : `ingress-nginx-v2`
	`apiVersion: v1`
	`kind: Namespace`
	`metadata:`
	`  labels:`
	`  app.kubernetes.io/instance: ingress-nginx`
	`  app.kubernetes.io/name: ingress-nginx`
	`  name: ingress-nginx-v2`
		DevOps ingénieur

Tâche	Description	Compétences requises

	4. Pour chaque section, mettez à jour la `namespace` valeur avec le nouveau nom.
	5. Dans la section `kind: Deployment` , effectuez les opérations suivantes :
	a. Entrez une valeur unique pour`--controller-class` , telle que`k8s.io/ingress-nginx-v2` .
	b. Entrez une valeur unique pour`--ingress-class`, telle que`nginx-v2`.
	`apiVersion: apps/v1`
	`kind: Deployment`
	`name: ingress-nginx-controller`
	`namespace: ingress-nginx-v2`
	`...`
	`spec:`
	`containers:`
	`- args:`
	`- /nginx-ingress-controller`
	`- --publish-service=$(POD_NAMESPACE)/ingress-nginx-controller`
	`- --election-id=ingress-nginx-leader`	

Tâche	Description	Compétences requises

	<pre>- --control
	ler-class=k8s.io/i
	ngress-nginx-v2
	- --ingress-
	class=nginx-v2</pre>
	6. Dans la `kind: IngressClass` section, entrez les mêmes valeurs pour `--controller-class` et celles `--ingress-class` que vous avez utilisées dans la section précédente :
	<pre>apiVersion: networkin
	g.k8s.io/v1
	kind: IngressClass
	metadata:
	labels:
	app.kuber
	netes.io/component:
	controller
	app.kuber
	netes.io/instance:
	ingress-nginx
	app.kuber
	netes.io/name:
	ingress-nginx
	app.kuber
	netes.io/part-of:
	ingress-nginx
	app.kuber
	netes.io/version:
	1.12.0
	name: nginx-v2
	spec:
	controller: k8s.io/
	ingress-nginx-v2</pre>	

Tâche	Description	Compétences requises

	7. Dans la section suivante, ajoutez `loadBalancerClass: eks.amazonaws.com/nlb` pour provisionner un Network Load Balancer pour l'instance NGINX Ingress Controller :
	
	`apiVersion: v1`
	`kind: Service`
	`metadata:`
	`  name: ingress-nginx-controller`
	`  namespace: ingress-nginx-v2`
	`spec:`
	`...`
	`  selector:`
	`  app.kubernetes.io/component: controller`
	`  app.kubernetes.io/instance: ingress-nginx`
	`  app.kubernetes.io/name: ingress-nginx`
	`  type: LoadBalancer`
	`  loadBalancerClass: eks.amazonaws.com/nlb`
	
	8. Enregistrez et fermez le modèle deploy.yaml.	

Tâche	Description	Compétences requises
Déployez la nouvelle instance NGINX Instance Controller.	Entrez la commande suivante pour appliquer le fichier manifeste modifié : `kubectl apply -f deploy.yaml`	DevOps ingénieur

Tâche	Description	Compétences requises

Confirmez le déploiement réussi.	Entrez la commande suivante pour vérifier que les ressources de l'espace de `ingress-nginx-v2` noms sont opérationnelles :
	`kubectl get all -n ingress-nginx-v2`
	Dans le résultat, vérifiez que les pods du NGINX Ingress Controller sont en cours d'exécution. Voici un exemple de résultat :
	`NAME READY STATUS RESTARTS AGE pod/ingress-nginx-admission-create-7shrj 0/1 Completed 0 24s pod/ingress-nginx-admission-patch-vkxr5 0/1 Completed 1 24s pod/ingress-nginx-controller-757bfcbc6d-4fw52 1/1 Running 0 24s NAME TYPE CLUSTER-IP EXTERNAL-IP`
		DevOps ingénieur

Tâche	Description	Compétences requises
	PORT(S) AGE service/ingress- nginx-controller LoadBalancer 10.100.208.114 k8s-ingressn-ingre ssn-2e5e37fab6-848 337cd9c9d520f.elb.eu- west-1.amazonaws.com 80:31469/TCP,443:3 0658/TCP 24s service/ingress- nginx-controller- admission ClusterIP 10.100.150.114 <none> 443/TCP 24s NAME READY UP-TO-DATE AVAILABLE AGE deployment.apps/ ingress-nginx-co ntroller 1/1 1 1 24s NAME DESIRED CURRENT READY AGE replicaset.apps/ ingress-nginx-co ntroller-757bfcbc6d	

Tâche	Description	Compétences requises
	`1 1 1 24s NAME STATUS COMPLETIONS DURATION AGE job.batch/ingress-nginx-admission-create Complete 1/1 4s 24s job.batch/ingress-nginx-admission-patch Complete 1/1 5s 24s`	
Créez une nouvelle entrée pour l'exemple de HTTPd charge de travail.	Entrez la commande suivante pour créer une nouvelle entrée pour l'exemple de HTTPd charge de travail existant : `kubectl create ingress demo-new --class=nginx-v2 \ --rule nginxautomode.local.dev/=demo:80`	DevOps ingénieur

Tâche	Description	Compétences requises

Vérifiez que la nouvelle entrée fonctionne.	Entrez la commande suivante pour vérifier que la nouvelle entrée fonctionne :
	`curl -H "Host: nginxautomode.local.dev" k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com`
	Le résultat attendu est le suivant :
	`<html><body><h1>It works!</h1></body></html>`
		DevOps ingénieur

Découper

Tâche	Description	Compétences requises
Passez au nouvel espace de noms.	1. (Facultatif) Suivez les instructions de la section Modification des enregistrements (documentation Route 53) pour mettre à jour l'enregistrement DNS. 2. Lorsque vous avez confirmé que la nouvelle instance de NGINX Ingress Controller fonctionne comme prévu, supprimez l'original.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	3. Supprimez le Load AWS Balancer Controller autogéré. Pour obtenir des instructions, consultez Migrer des applications depuis le contrôleur d'entrée ALB obsolète (documentation Amazon EKS). 4. Videz les groupes de nœuds gérés. Pour obtenir des instructions, consultez Supprimer et vider des groupes de nœuds (documentation eksctl).	

Tâche	Description	Compétences requises

Passez en revue les deux entrées.	Entrez la commande suivante pour passer en revue les deux entrées créées pour l'exemple de HTTPd charge de travail :
	`kubectl get ingress`
	Voici un exemple de résultat :
	`NAME CLASS HOSTS ADDRESS PORTS AGE demo nginx nginxautomode.local.dev k8s-ingressn-ingressn-abcdefg-12345.elb.eu-west-1.amazonaws.com 80 95m demo-new nginx-v2 nginxautomode.local.dev k8s-ingressn-ingressn-2e5e37fab6-848337cd9c9d520f.elb.eu-west-1.amazonaws.com 80 33s`
		DevOps ingénieur

Ressources connexes

- Activer le mode automatique EKS sur un cluster existant (documentation Amazon EKS)

- Résoudre les problèmes liés aux équilibreurs de charge créés par le contrôleur de service Kubernetes dans Amazon EKS (Re:Post Knowledge Center)AWS
- Contrôleur d'entrée NGINX (documentation NGINX)

Migrez vos charges de travail de conteneurs d'Azure Red Hat OpenShift (ARO) vers Red Hat OpenShift Service on AWS (ROSA)

Créée par Naveen Ramasamy (AWS), Gireesh Sreekantan (AWS) et Srikanth Rangavajhala (AWS)

Récapitulatif

Ce modèle fournit des step-by-step instructions pour la migration des charges de travail de conteneur d'Azure Red Hat OpenShift (ARO) vers Red Hat OpenShift Service on AWS (ROSA). ROSA est un service Kubernetes géré fourni par Red Hat en collaboration avec. AWS Il vous aide à déployer, à gérer et à faire évoluer vos applications conteneurisées à l'aide de la plateforme Kubernetes et bénéficie de l'expertise de Red Hat en matière de Kubernetes et d'infrastructure. AWS Cloud

La migration des charges de travail de conteneurs d'ARO, d'autres clouds ou d'un environnement sur site vers ROSA implique le transfert d'applications, de configurations et de données d'une plateforme à une autre. Ce modèle permet d'assurer une transition en douceur tout en optimisant les AWS Cloud services, la sécurité et la rentabilité. Il couvre deux méthodes pour migrer vos charges de travail vers des clusters ROSA : CI/CD et Migration Toolkit for Containers (MTC).

Ce modèle couvre les deux méthodes. La méthode que vous choisissez dépend de la complexité et de la certitude de votre processus de migration. Si vous contrôlez totalement l'état de votre application et pouvez garantir une configuration cohérente via un pipeline, nous vous recommandons d'utiliser la méthode CI/CD. Toutefois, si l'état de votre application implique des incertitudes, des changements imprévus ou un écosystème complexe, nous vous recommandons d'utiliser le MTC comme chemin fiable et contrôlé pour migrer votre application et ses données vers un nouveau cluster. Pour une comparaison détaillée des deux méthodes, consultez la section Informations supplémentaires.

Avantages de la migration vers ROSA :

- ROSA s'intègre parfaitement AWS en tant que service natif. Il est facilement accessible par le biais du AWS Management Console et facturé par le biais d'un single Compte AWS. Il offre une compatibilité totale avec les autres Services AWS et fournit un support collaboratif à la fois de la part de Red Hat AWS et de Red Hat.
- ROSA prend en charge les déploiements hybrides et multicloud. Il permet aux applications de s'exécuter de manière cohérente dans les centres de données sur site et dans plusieurs environnements cloud.

- ROSA bénéficie de l'accent mis par Red Hat sur la sécurité et fournit des fonctionnalités telles que le contrôle d'accès basé sur les rôles (RBAC), la numérisation d'images et les évaluations des vulnérabilités pour garantir un environnement de conteneurs sécurisé.
- ROSA est conçu pour faire évoluer facilement les applications et propose des options de haute disponibilité. Il permet aux applications de se développer en fonction des besoins tout en préservant leur fiabilité.
- ROSA automatise et simplifie le déploiement d'un cluster Kubernetes par rapport aux méthodes de configuration et de gestion manuelles. Cela accélère le processus de développement et de déploiement.
- ROSA bénéficie de AWS Cloud services et assure une intégration parfaite avec des AWS offres telles que les services de base de données, les solutions de stockage et les services de sécurité.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Autorisations configurées à Services AWS cet effet sur lesquelles ROSA s'appuie pour fournir des fonctionnalités. Pour plus d'informations, consultez la section Conditions préalables dans la documentation ROSA.
- ROSA activé sur la console ROSA. Pour obtenir des instructions, consultez la documentation ROSA.
- Le cluster ROSA est installé et configuré. Pour plus d'informations, voir Commencer avec ROSA dans la documentation ROSA. Pour comprendre les différentes méthodes de configuration d'un cluster ROSA, consultez le guide AWS prescriptif sur les stratégies de mise en œuvre de ROSA.
- Connectivité réseau établie à partir du réseau local vers AWS le réseau AWS Direct Connect(préféré) ou AWS Virtual Private Network (AWS VPN).
- Une instance Amazon Elastic Compute Cloud (Amazon EC2) ou un autre serveur virtuel pour installer des outils tels que le `aws client` client OpenShift CLI (`oc`), le client ROSA et le binaire Git.

Conditions préalables supplémentaires pour la méthode CI/CD :

- Accès au serveur Jenkins sur site avec les autorisations nécessaires pour créer un nouveau pipeline, ajouter des stages, ajouter des OpenShift clusters et effectuer des builds.

- Accès au référentiel Git où le code source de l'application est conservé, avec les autorisations nécessaires pour créer une nouvelle branche Git et effectuer des validations sur la nouvelle branche.

Conditions préalables supplémentaires pour la méthode MTC :

- Un bucket Amazon Simple Storage Service (Amazon S3), qui sera utilisé comme référentiel de réplication.
- Accès administratif au cluster ARO source. Cela est nécessaire pour configurer la connexion MTC.

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

ROSA propose trois modèles de déploiement réseau : public, privé et AWS PrivateLink. PrivateLinkpermet aux équipes d'ingénierie de fiabilité des sites (SRE) de Red Hat de gérer le cluster en utilisant un sous-réseau privé connecté au PrivateLink point de terminaison du cluster dans un VPC existant.

Le choix de PrivateLink cette option permet d'obtenir la configuration la plus sécurisée. C'est pourquoi nous le recommandons pour les charges de travail sensibles ou pour les exigences de conformité strictes. Pour plus d'informations sur les options de déploiement sur les réseaux publics et privés, consultez la OpenShift documentation Red Hat.

> **Important**
>
> Vous ne pouvez créer un PrivateLink cluster qu'au moment de l'installation. Vous ne pouvez pas modifier un cluster à utiliser PrivateLink après l'installation.

Le schéma suivant illustre l' PrivateLink architecture d'un cluster ROSA utilisé pour se connecter AWS Direct Connect aux environnements sur site et ARO.

AWS autorisations pour ROSA

Pour obtenir AWS des autorisations sur ROSA, nous vous recommandons d'utiliser AWS Security Token Service (AWS STS) avec des jetons dynamiques de courte durée. Cette méthode utilise des rôles et des politiques prédéfinis de moindre privilège pour accorder à ROSA des autorisations minimales pour opérer dans le Compte AWS, et prend en charge l'installation, le plan de contrôle et les fonctionnalités de calcul de ROSA.

Redéploiement du pipeline CI/CD

CI/CD pipeline redeployment is the recommended method for users who have a mature CI/CDpipeline. Lorsque vous choisissez cette option, vous pouvez utiliser n'importe quelle stratégie de DevOps déploiement pour transférer progressivement la charge de votre application vers des déploiements sur ROSA.

> **Note**
>
> Ce modèle suppose un cas d'utilisation courant dans lequel vous disposez d'un pipeline Git, JFrog Artifactory et Jenkins sur site. Cette approche nécessite que vous établissiez une connectivité réseau entre votre réseau sur site et AWS via AWS Direct Connect, et que vous configuriez le cluster ROSA avant de suivre les instructions de la section Epics. Consultez la section Conditions préalables pour plus de détails.

Le schéma suivant montre le flux de travail de cette méthode.

Méthode MTC

Vous pouvez utiliser le kit de migration pour les conteneurs (MTC) pour migrer vos charges de travail conteneurisées entre différents environnements Kubernetes, tels que d'ARO à ROSA. MTC simplifie le processus de migration en automatisant plusieurs tâches clés et en fournissant un cadre complet pour gérer le cycle de vie de la migration.

Le schéma suivant montre le flux de travail de cette méthode.

Outils

Services AWS

- AWS DataSyncest un service de transfert et de découverte de données en ligne qui vous permet de déplacer des fichiers ou des données d'objets vers, depuis et entre les services AWS de stockage.
- AWS Direct Connectrelie votre réseau interne à un AWS Direct Connect emplacement via un câble à fibre optique Ethernet standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement destinées au public Services AWS tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- AWS PrivateLinkvous permet de créer des connexions privées unidirectionnelles entre vos clouds privés virtuels (VPCs) et des services extérieurs au VPC.
- Red Hat OpenShift Service on AWS (ROSA) est un service géré qui aide les OpenShift utilisateurs de Red Hat à créer, à faire évoluer et à gérer des applications conteneurisées sur. AWS
- AWS Security Token Service (AWS STS) vous permet de demander des informations d'identification temporaires à privilèges limités pour les utilisateurs.

Autres outils

- Le Migration Toolkit for Containers (MTC) fournit une console et une API pour la migration d'applications conteneurisées d'ARO vers ROSA.

Bonnes pratiques

- Pour des raisons de résilience et si vous avez des charges de travail de conformité en matière de sécurité, configurez un cluster ROSA multi-AZ qui utilise. PrivateLink Pour plus d'informations, consultez la documentation ROSA.

> **Note**
>
> PrivateLink ne peut pas être configuré après l'installation.

- Le compartiment S3 que vous utilisez pour le référentiel de réplication ne doit pas être public. Utilisez les politiques de compartiment S3 appropriées pour restreindre l'accès.
- Si vous choisissez la méthode MTC, utilisez l'option de migration par étapes pour réduire la période d'indisponibilité pendant le passage à un autre.
- Passez en revue vos quotas de service avant et après le provisionnement du cluster ROSA. Si nécessaire, demandez une augmentation de quota en fonction de vos besoins. Pour de plus amples informations, veuillez consulter la documentation sur les quotas de service.

- Consultez les directives de sécurité ROSA et mettez en œuvre les meilleures pratiques en matière de sécurité.
- Nous vous recommandons de supprimer l'administrateur de cluster par défaut après l'installation. Pour plus d'informations, consultez la OpenShift documentation Red Hat.
- Utilisez le dimensionnement automatique du pool de machines pour réduire les nœuds de travail inutilisés dans le cluster ROSA afin d'optimiser les coûts. Pour plus d'informations, consultez l'atelier ROSA.
- Utilisez le service Red Hat Cost Management pour OpenShift Container Platform afin de mieux comprendre et suivre les coûts des clouds et des conteneurs. Pour plus d'informations, consultez l'atelier ROSA.
- Surveillez et auditez les services et applications d'infrastructure du cluster ROSA en utilisant Services AWS. Pour plus d'informations, consultez l'atelier ROSA.

Épopées

Option 1 : Utiliser un pipeline CI/CD

Tâche	Description	Compétences requises
Ajoutez le nouveau cluster ROSA à Jenkins.	1. Sur la console Jenkins, choisissez Manage Jenkins, Configure System. 2. Sur la page Gérer Jenkins, dans la section OpenShift Plug-in, choisissez Ajouter un nouveau cluster. 3. Fournissez les informations requises telles que le nom du cluster, l'URL du serveur d'API et les informations du jeton pour vous authentifier auprès de ROSA.	Administrateur AWS, administrateur système AWS, AWS DevOps
Ajoutez le oc client à vos nœuds Jenkins.	1. Sur la console Jenkins, choisissez Manage Jenkins, Global Tool Configuration.	Administrateur AWS, administrateur système AWS, AWS DevOps

Tâche	Description	Compétences requises
	2. Dans la section Outils OpenShift client, installez la version du client OpenShift CLI (`oc`) identique à la version de votre cluster ROSA.	
Créez une nouvelle branche Git.	Créez une nouvelle branche dans votre dépôt Git pour`rosa-dev`. Cette branche sépare les modifications de code ou de paramètres de configuration pour ROSA de votre pipeline existant.	AWS DevOps
Images de tags pour ROSA.	Au cours de votre phase de création, utilisez une autre balise pour identifier les images créées à partir du pipeline ROSA.	Administrateur AWS, administrateur système AWS, AWS DevOps
Créez un pipeline.	Créez un nouveau pipeline Jenkins similaire à votre pipeline existant. Pour ce pipeline, utilisez la branche `rosa-dev` Git que vous avez créée précédemment et assurez-vous d'inclure les étapes de validation, de numérisation du code et de compilation Git identiques à celles de votre pipeline existant.	Administrateur AWS, administrateur système AWS, AWS DevOps

Tâche	Description	Compétences requises
Ajoutez une phase de déploiement ROSA.	Dans le nouveau pipeline, ajoutez une étape à déployer sur le cluster ROSA et référencez le cluster ROSA que vous avez ajouté à la configuration globale de Jenkins.	Administrateur AWS, AWS DevOps, administrateur système AWS
Commencez une nouvelle construction.	Dans Jenkins, sélectionnez votre pipeline et choisisse z Construire maintenant, ou lancez une nouvelle construct ion en validant une modificat ion de la `rosa-dev` branche dans Git.	Administrateur AWS, AWS DevOps, administrateur système AWS
Vérifier le déploiement.	Utilisez la commande oc ou la console ROSA pour vérifier que l'application a été déployée sur votre cluster ROSA cible.	Administrateur AWS, AWS DevOps, administrateur système AWS
Copiez les données dans le cluster cible.	Pour les charges de travail dynamiques, copiez les données du cluster source vers le cluster cible à l'aide AWS DataSync d'utilitaires open source tels que rsync, ou vous pouvez utiliser la méthode MTC. Pour plus d'informations, consultez la documentation AWS DataSync.	Administrateur AWS, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises
Testez votre application.	1. Récupérez l'URL de route de votre application à l'aide de la commande oc route ou de la console ROSA. 2. Testez votre application à l'aide de l'URL de la route.	Administrateur AWS, AWS DevOps, administrateur système AWS
Découpez.	Si vos tests sont réussis, utilisez la politique Amazon Route 53 appropriée pour déplacer le trafic de l'application hébergée par ARO vers l'application hébergée par Rosa. Lorsque vous aurez terminé cette étape, la charge de travail de votre application sera entièrement transférée vers le cluster ROSA.	Administrateur AWS, administrateur système AWS

Option 2 : utiliser le MTC

Tâche	Description	Compétences requises
Installez l'opérateur MTC.	Installez l'opérateur MTC sur les clusters ARO et ROSA : 1. Dans la console ARO ou ROSA, accédez à la OperatorHubpage Opérateurs. 2. Dans la zone Filtrer par mot clé, recherchez ou tapez MTC.	Administrateur AWS, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises
	3. Sélectionnez l'opérateur MTC pour afficher des informations supplémen taires. 4. Après avoir lu les informati ons relatives à l'opérateur, choisissez Installer.	
Configurez le trafic réseau vers le référentiel de réplicati on.	Si vous utilisez un serveur proxy, configurez-le pour autoriser le trafic réseau entre le référentiel de réplication et les clusters. Le référentiel de réplication est un objet de stockage intermédiaire que MTC utilise pour migrer les données. Les clusters source et cible doivent disposer d'un accès réseau au référenti el de réplication pendant la migration.	Administrateur AWS, AWS DevOps, administrateur système AWS
Ajoutez le cluster source au MTC.	Sur la console Web MTC, ajoutez le cluster source ARO.	Administrateur AWS, AWS DevOps, administrateur système AWS
Ajoutez Amazon S3 comme référentiel de réplication.	Sur la console Web MTC, ajoutez le compartiment Amazon S3 (voir Condition s préalables) en tant que référentiel de réplication.	Administrateur AWS, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises
Créez un plan de migration.	Sur la console Web MTC, créez un plan de migration et spécifiez le type de transfert de données comme Copy. Cela indiquera à MTC de copier les données du cluster source (ARO) vers le compartiment S3, et du compartiment vers le cluster cible (ROSA).	Administrateur AWS, AWS DevOps, administrateur système AWS

Tâche	Description	Compétences requises
Exécutez le plan de migration.	Exécutez le plan de migration à l'aide de l'option Stage ou Cutover : • Choisissez Stage pour copier les données vers le cluster cible sans arrêter votre application. Vous pouvez exécuter des migrations en plusieurs étapes pour copier la plupart de vos données avant la migration de transition. Cela réduit la durée de la migration de transition. • Choisissez Cutover pour arrêter votre application sur le cluster source tout en déplaçant les ressources vers le cluster cible. Pour éviter d'arrêter l'application, vous pouvez décocher la case Arrêter les transactions sur le cluster source pendant la migration.	Administrateur AWS, AWS DevOps, administrateur système AWS

Résolution des problèmes

Problème	Solution
Problèmes de connectivité	Lorsque vous migrez vos charges de travail de conteneurs d'ARO vers ROSA, vous pouvez rencontrer des problèmes de connectivité qui

Problème	Solution
	doivent être résolus pour garantir une migration réussie. Pour résoudre ces problèmes de connectivité (répertoriés dans ce tableau) lors de la migration, une planification méticuleu se, une coordination avec votre réseau et vos équipes de sécurité, ainsi que des tests approfondis sont essentiels. La mise en œuvre d'une stratégie de migration progressive et la vérification de la connectivité à chaque étape permettront de minimiser les perturbat ions potentielles et d'assurer une transition harmonieuse d'ARO à ROSA.
Différences de configuration réseau	ARO et ROSA peuvent présenter des variation s dans leurs configurations réseau, telles que les paramètres du réseau virtuel (VNet), les sous-réseaux et les politiques réseau. Pour une communication correcte entre les services, assurez-vous que les paramètres réseau correspondent aux deux plateformes.
Règles de groupe de sécurité et de pare-feu	ROSA et ARO peuvent avoir des paramètre s de groupe de sécurité et de pare-feu par défaut différents. Assurez-vous d'ajuster et de mettre à jour ces règles pour autoriser le trafic nécessaire au maintien de la connectivité entre les conteneurs et les services pendant la migration.
Modifications d'adresse IP et de DNS	Lorsque vous migrez des charges de travail, les adresses IP et les noms DNS peuvent changer. Reconfigurez les applications qui s'appuient sur des noms DNS statiques IPs ou spécifiques.

Problème	Solution
Accès aux services externes	Si votre application dépend de services externes tels que des bases de données APIs, vous devrez peut-être mettre à jour leurs paramètres de connexion pour vous assurer qu'ils peuvent communiquer avec les nouveaux services de ROSA.
Configuration d'Azure Private Link	Si vous utilisez Azure Private Link ou des services de point de terminaison privés dans ARO, vous devrez configurer les fonctionnalités équivalentes dans ROSA pour garantir une connectivité privée entre les ressources.
AWS VPN ou AWS Direct Connect configura tion	S'il existe des AWS Direct Connect connexion s AWS VPN ou des connexions entre votre réseau local et ARO, vous devrez établir des connexions similaires avec ROSA pour une communication ininterrompue avec vos ressources locales.
Paramètres d'entrée et d'équilibrage de charge	Les configurations des contrôleurs d'entrée et des équilibreurs de charge peuvent différer entre ARO et ROSA. Reconfigurez ces paramètres pour conserver l'accès externe à vos services.
Gestion des certificats et du TLS	Si vos applications utilisent des certificats SSL ou TLS, assurez-vous que les certificats sont valides et correctement configurés dans ROSA.
Accès au registre des conteneurs	Si vos conteneurs sont hébergés dans un registre de conteneurs externe, configurez l'authentification et les autorisations d'accès appropriées pour ROSA.

Problème	Solution
Surveillance et journalisation	Mettez à jour les configurations de surveillance et de journalisation pour tenir compte de la nouvelle infrastructure de ROSA afin que vous puissiez continuer à surveiller efficacement l'état et les performances de vos conteneurs.

Ressources connexes

AWSréférences

- Qu'est-ce que c'est Red Hat OpenShift Service on AWS ? (documentation ROSA)
- Commencez avec ROSA (documentation ROSA)
- Red Hat OpenShift Service on AWS stratégies de mise en œuvre (AWS directives prescriptives)
- Red Hat OpenShift Service on AWS Now GA (article de AWS blog)
- Atelier ROSA
- FAQ SUR ROSA
- FAQ sur l'atelier ROSA
- Tarifs ROSA

OpenShift Documentation Red Hat

- Installation rapide d'un cluster sur AWS
- Installation d'un cluster AWS sur un réseau restreint
- Installation d'un cluster AWS dans un VPC existant
- Installation d'un cluster sur une infrastructure provisionnée par l'utilisateur à l'aide de AWS modèles CloudFormation
- Installation d'un cluster sur AWS un réseau restreint avec une infrastructure provisionnée par l'utilisateur
- Installation d'un cluster AWS avec des personnalisations
- Commencer à utiliser la OpenShift CLI

Informations supplémentaires

Choix entre les options de redéploiement du pipeline MTC et CI/CD

La migration d'applications d'un OpenShift cluster à un autre nécessite un examen attentif. Idéalement, vous souhaiteriez une transition fluide en utilisant un pipeline CI/CD pour redéployer l'application et gérer la migration des données de volume persistantes. Cependant, dans la pratique, une application en cours d'exécution sur un cluster est susceptible de subir des changements imprévus au fil du temps. Ces modifications peuvent entraîner une déviation progressive de l'application par rapport à son état de déploiement initial. MTC propose une solution pour les scénarios dans lesquels le contenu exact d'un espace de noms est incertain et où une migration fluide de tous les composants de l'application vers un nouveau cluster est importante.

Pour faire le bon choix, il faut évaluer votre scénario spécifique et évaluer les avantages de chaque approche. Ce faisant, vous pouvez garantir une migration réussie et fluide qui correspond à vos besoins et à vos priorités. Voici des directives supplémentaires pour choisir entre les deux options.

Redéploiement du pipeline CI/CD

La méthode du pipeline CI/CD est l'approche recommandée si votre application peut être redéployée en toute confiance à l'aide d'un pipeline. Cela garantit que la migration est contrôlée, prévisible et alignée sur vos pratiques de déploiement existantes. Lorsque vous choisissez cette méthode, vous pouvez utiliser des stratégies de déploiement bleu/vert ou Canary pour transférer progressivement la charge vers les déploiements sur ROSA. Pour ce scénario, ce modèle suppose que Jenkins orchestre les déploiements d'applications à partir de l'environnement sur site.

Avantages :

- Vous n'avez pas besoin d'un accès administratif au cluster ARO source ni de déployer d'opérateurs sur le cluster source ou de destination.
- Cette approche vous permet de changer de trafic progressivement en utilisant une DevOps stratégie.

Inconvénients :

- Il faut déployer davantage d'efforts pour tester les fonctionnalités de votre application.
- Si votre application contient des données persistantes, des étapes supplémentaires sont nécessaires pour copier les données à l'aide AWS DataSync d'autres outils.

Migration MTC

Dans le monde réel, les applications en cours d'exécution peuvent subir des modifications imprévues qui les éloignent du déploiement initial. Choisissez l'option MTC lorsque vous n'êtes pas sûr de l'état actuel de votre application sur le cluster source. Par exemple, si votre écosystème d'applications couvre différents composants, configurations et volumes de stockage de données, nous vous recommandons de choisir MTC pour garantir une migration complète couvrant l'application et l'ensemble de son environnement.

Avantages :

- MTC fournit une sauvegarde et une restauration complètes de la charge de travail.
- Il copiera les données persistantes de la source vers la cible lors de la migration de la charge de travail.
- Il ne nécessite pas d'accès au référentiel du code source.

Inconvénients :

- Vous devez disposer de privilèges administratifs pour installer l'opérateur MTC sur les clusters source et de destination.
- L' DevOps équipe a besoin d'une formation pour utiliser l'outil MTC et effectuer des migrations.

Optimisation des images Docker générées par AWS App2Container

Créée par Varun Sharma (AWS)

Récapitulatif

AWS App2Container est un outil de ligne de commande qui permet de transformer des applications existantes exécutées sur site ou sur des machines virtuelles en conteneurs, sans qu'il soit nécessaire de modifier le code.

En fonction du type d'application, App2Container adopte une approche conservatrice pour identifier les dépendances. En mode processus, tous les fichiers du serveur d'applications sont inclus dans l'image du conteneur. Dans de tels cas, une image assez grande peut être générée.

Ce modèle fournit une approche pour optimiser les images de conteneur générées par App2Container. Il s'applique à toutes les applications Java découvertes par App2Container en mode processus. Le flux de travail défini dans le modèle est conçu pour être exécuté sur le serveur d'applications.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Application Java exécutée sur un serveur d'applications sur un serveur Linux
- App2Container installé et configuré, avec toutes les conditions requises remplies, sur le serveur Linux

Architecture

Pile technologique source

- Une application Java exécutée sur un serveur Linux

Pile technologique cible

- Une image Docker générée par App2Container

Flux d'architecture cible

1. Découvrez les applications qui s'exécutent sur le serveur d'applications et analysez-les.
2. Conteneurisez les applications.
3. Évaluez la taille de l'image Docker. Si l'image est trop grande, passez à l'étape 4.
4. Utilisez le script shell (joint) pour identifier les fichiers volumineux.
5. Mettez à jour les `appSpecificFiles` listes `appExcludedFiles` et du `analysis.json` fichier.

Outils

Outils

- AWS App2Container — AWS App2Container (A2C) est un outil en ligne de commande destiné à vous aider à transférer des applications exécutées dans votre centre de données sur site ou sur des machines virtuelles, afin qu'elles s'exécutent dans des conteneurs gérés par Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS).

Code

Le script `optimizeImage.sh` shell et un `analysis.json` fichier d'exemple sont joints.

Le `optimizeImage.sh` fichier est un script utilitaire permettant de consulter le contenu du fichier généré par App2Container. `ContainerFiles.tar` L'examen identifie les fichiers ou les sous-répertoires volumineux qui peuvent être exclus. Le script est un wrapper pour la commande tar suivante.

```
tar -Ptvf <path>|tr -s ' '|cut -d ' ' -f3,6| awk '$2 ~/<filetype>$/'| awk '$2 ~/
^<toplevel>/'| cut -f1-<depth> -d'/'|awk '{ if ($1>= <size>) arr[$2]+=$1 } END { for
 (key in arr) { if(<verbose>) printf("%-50s\t%-50s\n", key, arr[key]) else printf("%s,
\n", key) } } '|sort -k2 -nr
```

Dans la commande tar, le script utilise les valeurs suivantes :

`path`	Le chemin vers `ContainerFiles.tar`
`filetype`	Le type de fichier correspondant

`toplevel`	Le répertoire de premier niveau à associer
`depth`	La profondeur du chemin absolu
`size`	La taille de chaque fichier

Le script effectue les opérations suivantes :

1. Il permet `tar -Ptvf` de lister les fichiers sans les extraire.
2. Il filtre les fichiers par type de fichier, en commençant par le répertoire de premier niveau.
3. Sur la base de la profondeur, il génère le chemin absolu sous forme d'indice.
4. Sur la base de l'index et des magasins, il fournit la taille totale du sous-répertoire.
5. Elle affiche la taille du sous-répertoire.

Vous pouvez également remplacer les valeurs manuellement dans la commande tar.

Épopées

Découvrez, analysez et conteneurisez les applications

Tâche	Description	Compétences requises
Découvrez les applications Java locales.	Pour découvrir toutes les applications exécutées sur le serveur d'applications, exécutez la commande suivante. `sudo app2container inventory`	AWS DevOps
Analysez les applications découvertes.	Pour analyser chaque applicati on à l'aide de `applicati on-id` ce qui a été obtenu lors de la phase d'inventa	AWS DevOps

Tâche	Description	Compétences requises
	ire, exécutez la commande suivante. `sudo app2container analyze --application-id <java-app-id>`	
Conteneurisez les applications analysées.	Pour conteneuriser une application, exécutez la commande suivante. `sudo app2container containerize --application-id <application-id>` La commande génère l'image Docker ainsi qu'un bundle tar dans l'emplacement de l'espace de travail. Si l'image Docker est trop grande, passez à l'étape suivante.	AWS DevOps

Identifier appExcludedFiles et appSpecificFiles extraire le fichier tar d'App2Container

Tâche	Description	Compétences requises
Identifiez la taille du fichier tar des artefacts.	Identifiez le `Container Files.tar` fichier dans `{workspace}/{java-app-id}/Artifacts` lequel se `workspace` trouve l'espace de travail App2Conta	AWS DevOps

Tâche	Description	Compétences requises
	iner et l'ID `java-app-id` de l'application. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Il s'agit de la taille totale du fichier tar après optimisation.	

Tâche	Description	Compétences requises

Répertoriez les sous-répertoires situés sous le répertoire/ainsi que leurs tailles.	Pour identifier les tailles des principaux sous-répertoires du répertoire de / premier niveau, exécutez la commande suivante.
	`./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 1 -t / -s 1000000 -v`
	`/var`
	`554144711`
	`/usr`
	`2097300819`
	`/tmp`
	`18579660`
	`/root`
	`43645397`
	`/opt`
	`222320534`
	`/home`
	`65212518`
	`/etc`
	`11357677`
		AWS DevOps

Tâche	Description	Compétences requises
Identifiez les sous-répertoires volumineux sous le répertoire/.	Pour chaque sous-répertoire principal répertorié dans la commande précédente, identifiez la taille de ses sous-répertoires. `-d`À utiliser pour augmenter la profondeur et `-t` pour indiquer le répertoire de premier niveau. Par exemple, utilisez-le `/var` comme répertoire de premier niveau. Ci-dessous`/var`, identifiez tous les grands sous-répertoires et leur taille. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 2 -t /var -s 1000000 -v` Répétez ce processus pour chaque sous-répertoire répertorié à l'étape précédente (par exemple,`/usr`, `/tmp`/`opt`, et`/home`).	AWS DevOps

Tâche	Description	Compétences requises
Analysez le dossier volumineux de chaque sous-répertoire du répertoire /.	Pour chaque sous-répertoire répertorié à l'étape précédente, identifiez les dossiers nécessaires à l'exécution de l'application. Par exemple, en utilisant les sous-répertoires de l'étape précédente, listez tous les sous-répertoires du `/var` répertoire ainsi que leur taille. Identifiez tous les sous-répertoires dont l'application a besoin. `/var/tmp 237285851 /var/lib 24489984 /var/cache 237285851` Pour exclure les sous-répertoires dont l'application n'a pas besoin, ajoutez ces sous-répertoires dans le `analysis.json` fichier dans la `appExcludedFiles` section ci-dessous. `containerParameters` Un `analysis.json` fichier d'exemple est joint.	AWS DevOps

Tâche	Description	Compétences requises
Identifiez les fichiers nécessaires dans la liste AppExcludes.	Pour chaque sous-répertoire ajouté à la liste AppExcludes, identifiez tous les fichiers de ce sous-répertoire requis par l'application. Dans le fichier analysis.json, ajoutez les fichiers ou sous-répertoires spécifiques dans la section ci-dessous. `appSpecificFiles containerParameters` Par exemple, si le `/usr/lib` répertoire est ajouté à la liste des exclusions, mais `/usr/lib/jvm` que l'application en a besoin, ajoutez-le `/usr/lib/jvm` à la `appSpecificFiles` section.	AWS DevOps

Extrayez et conteneurisez à nouveau l'application

Tâche	Description	Compétences requises
Conteneurisez l'application analysée.	Pour conteneuriser l'application, exécutez la commande suivante. `sudo app2container containerize --application-id <application-id>` La commande génère l'image Docker ainsi qu'un bundle	AWS DevOps

Tâche	Description	Compétences requises
	tar dans l'emplacement de l'espace de travail.	
Identifiez la taille du fichier tar des artefacts.	Identifiez le `Container Files.tar` fichier dans `{workspace}/{java-app-id}/Artifacts` lequel se `workspace` trouve l'espace de travail App2Container et l'ID `java-app-id` de l'application. `./optimizeImage.sh -p /{workspace}/{java-app-id}/Artifacts/ContainerFiles.tar -d 0 -t / -v` Il s'agit de la taille totale du fichier tar après optimisation.	AWS DevOps
Exécutez l'image Docker.	Pour vérifier que l'image démarre sans erreur, exécutez l'image Docker localement à l'aide des commandes suivantes. Pour identifier `imageId` le contenant, utilisez`docker images |grep java-app-id` . Pour faire fonctionner le conteneur, utilisez`docker run -d <image id>`.	AWS DevOps

Ressources connexes

- Qu'est-ce qu'App2Container ?
- AWS App2Container — Un nouvel outil de conteneurisation pour les applications Java et .NET (article de blog)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Placez des pods Kubernetes sur Amazon EKS en utilisant l'affinité, les entorses et les tolérances des nœuds

Créée par Hitesh Parikh (AWS) et Raghu Bhamidimarri (AWS)

Récapitulatif

Ce modèle illustre l'utilisation de l'affinité des nœuds Kubernetes, de l'altération des nœuds et des tolérances des pods pour planifier intentionnellement des pods d'application sur des nœuds de travail spécifiques d'un cluster Amazon Elastic Kubernetes Service (Amazon EKS) sur le cloud Amazon Web Services (AWS).

Une souillure est une propriété de nœud qui permet aux nœuds de rejeter un ensemble de modules. Une tolérance est une propriété de Pod qui permet au planificateur Kubernetes de planifier des Pods sur des nœuds présentant les mêmes caractéristiques.

Cependant, les tolérances ne peuvent à elles seules empêcher un planificateur de placer un Pod sur un nœud de travail qui ne présente aucune trace. Par exemple, un pod à forte intensité de calcul assorti d'une tolérance peut involontairement être programmé sur un nœud non contaminé à usage général. Dans ce scénario, la propriété d'affinité de nœud d'un Pod indique au planificateur de placer le Pod sur un nœud qui répond aux critères de sélection de nœuds spécifiés dans l'affinité de nœud.

Ensemble, les entailles, les tolérances et l'affinité des nœuds indiquent au planificateur de planifier les pods de manière cohérente sur les nœuds avec les taches correspondantes et les étiquettes des nœuds qui correspondent aux critères de sélection des nœuds d'affinité de nœud spécifiés sur le pod.

Ce modèle fournit un exemple de fichier manifeste de déploiement de Kubernetes, ainsi que les étapes à suivre pour créer un cluster EKS, déployer une application et valider le placement du Pod.

Conditions préalables et limitations

Prérequis

- Un compte AWS avec des informations d'identification configurées pour créer des ressources sur votre compte AWS
- Interface de ligne de commande AWS (AWS CLI)
- eksctl

- kubectl
- Docker a été installé (pour le système d'exploitation utilisé) et le moteur a démarré (pour plus d'informations sur les exigences de licence Docker, consultez le site Docker)
- Java version 11 ou ultérieure
- Un microservice Java exécuté sur votre environnement de développement intégré (IDE) préféré ; par exemple, IntelliJ IDEA Community Edition ou Eclipse (si vous n'avez pas de microservice Java, consultez le modèle Déployer un exemple de microservice Java sur Amazon EKS et Microservices with Spring pour obtenir de l'aide sur la création du microservice)

Limites

- Ce modèle ne fournit pas le code Java et suppose que vous êtes déjà familiarisé avec Java. Pour créer un microservice Java de base, consultez Déployer un exemple de microservice Java sur Amazon EKS.
- Les étapes décrites dans cet article créent des ressources AWS qui peuvent entraîner des coûts. Assurez-vous de nettoyer les ressources AWS une fois que vous avez terminé les étapes de mise en œuvre et de validation du modèle.

Architecture

Pile technologique cible

- Amazon EKS
- Java
- Docker
- Amazon Elastic Container Registry (Amazon ECR)

Architecture cible

Le schéma d'architecture de la solution montre Amazon EKS avec deux pods (déploiement 1 et déploiement 2) et deux groupes de nœuds (ng1 et ng2) avec deux nœuds chacun. Les pods et les nœuds possèdent les propriétés suivantes.

	Déploiement : 1 pod	Déploiement 2 Pod	Groupe de nœuds 1 (ng1)	Groupe de nœuds 2 (ng2)

Tolérance	clé : classified_workload, valeur : true, effet : NoSchedule clé : machine_learning_workload, valeur : vrai, effet : NoSchedule	Aucun		
Affinité des nœuds	clé : alpha.eksctl.io/nodegroup-name = ng1 ;	Aucun	NodeGroups.name = ng1	
Souillure			clé : classified_workload, valeur : true, effet : NoSchedule clé : machine_learning_workload, valeur : vrai, effet : NoSchedule	Aucun

1. Le pod Deployment 1 a des tolérances et une affinité de nœud définies, ce qui indique au planificateur Kubernetes de placer les pods de déploiement sur les nœuds du groupe de nœuds 1 (ng1).
2. Le groupe de nœuds 2 (ng2) n'a pas d'étiquette de nœud correspondant à l'expression du sélecteur de nœuds d'affinité pour le déploiement 1. Les pods ne seront donc pas planifiés sur les nœuds ng2.

3. Aucune tolérance ou affinité de nœud n'est définie dans le manifeste de déploiement pour le module Deployment 2. Le planificateur refusera de planifier le déploiement de 2 pods sur le groupe de nœuds 1 en raison des entorses sur les nœuds.
4. Les pods Deployment 2 seront plutôt placés sur le groupe de nœuds 2, car les nœuds ne présentent aucune trace.

Ce modèle montre qu'en utilisant des nuances et des tolérances, associées à l'affinité des nœuds, vous pouvez contrôler le placement des pods sur des ensembles spécifiques de nœuds de travail.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- eksctl est l'équivalent AWS de kubectl et aide à créer EKS.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- kubectl est une interface de ligne de commande qui vous permet d'exécuter des commandes sur des clusters Kubernetes.

Épopées

Création du cluster EKS

Tâche	Description	Compétences requises

Créez le fichier cluster.yaml.	Créez un fichier appelé `cluster.yaml` avec le code suivant.
	
	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
	
	`metadata:`
	`  name: eks-taint-demo`
	`  region: us-west-1`
	
	`# Unmanaged nodegroups with and without taints.`
	`nodeGroups:`
	`  - name: ng1`
	`  instanceType: m5.xlarge`
	`  minSize: 2`
	`  maxSize: 3`
	`  taints:`
	`  - key: classified_workload`
	`  value: "true"`
	`  effect: NoSchedule`
	`  - key: machine_learning_workload`
	`  value: "true"`
	`  effect: NoSchedule`
	
	`  - name: ng2`
	`  instanceType: m5.xlarge`
		Propriétaire de l'application, AWS DevOps, administrateur du cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	`minSize: 2` `maxSize: 3`	
Créez le cluster à l'aide de eksctl.	Exécutez le `cluster.yaml` fichier pour créer le cluster EKS. La création du cluster peut prendre quelques minutes. `eksctl create cluster -f cluster.yaml`	AWS DevOps, administrateur système AWS, développeur d'applications

Créez une image et chargez-la sur Amazon ECR

Tâche	Description	Compétences requises
Créez un référentiel privé Amazon ECR.	Pour créer un référentiel Amazon ECR, consultez Création d'un référentiel privé. Notez l'URI du dépôt.	AWS DevOps, DevOps ingénieur, développeur d'applications
Créez le Dockerfile.	Si vous avez une image de conteneur Docker existante que vous souhaitez utiliser pour tester le modèle, vous pouvez ignorer cette étape. Pour créer un Dockerfile, utilisez l'extrait suivant comme référence. Si vous rencontrez des erreurs, consultez la section Dépannage.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	`FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`
	
	`RUN apk add maven`
	`WORKDIR /code`
	
	`# Prepare by downloading dependencies`
	`ADD pom.xml /code/pom.xml`
	`RUN ["mvn", "dependency:resolve"]`
	`RUN ["mvn", "verify"]`
	
	`# Adding source, compile and package into a fat jar`
	`ADD src /code/src`
	`RUN ["mvn", "package"]`
	
	`EXPOSE 4567`
	`CMD ["java", "-jar", "target/eksExample-jar-with-dependencies.jar"]`	

Créez le fichier pom.xml et les fichiers source, puis créez et publiez l'image Docker.	Pour créer le `pom.xml` fichier et le fichier source Java, consultez la section Déployer un exemple de microservice Java sur le modèle Amazon EKS. Utilisez les instructions de ce modèle pour créer et envoyer l'image Docker.	AWS DevOps, DevOps ingénieur, développeur d'applications

Déploiement sur Amazon EKS

Tâche	Description	Compétences requises
Créez le fichier deploymen t.yaml.	Pour créer le `deploymen t.yaml` fichier, utilisez le code de la section Informati ons supplémentaires. Dans le code, la clé de l'affinité des nœuds est toute étiquette que vous créez lors de la création de groupes de nœuds. Ce modèle utilise l'étiquette par défaut créée par eksctl. Pour plus d'informa tions sur la personnalisation des étiquettes, consultez la section Affectation de pods à des nœuds dans la documentation de Kubernetes. La valeur de la clé d'affinité de nœud est le nom du groupe de nœuds créé par`cluster.y aml` . Pour obtenir la clé et la valeur de la tache, exécutez la commande suivante. `kubectl get nodes -o json | jq '.items[] .spec.taints'` L'image est l'URI du référenti el Amazon ECR que vous	AWS DevOps, DevOps ingénieur, développeur d'applications

Tâche	Description	Compétences requises
	avez créé lors d'une étape précédente.	
Déployez le fichier.	Pour effectuer un déploiement sur Amazon EKS, exécutez la commande suivante. `kubectl apply -f deployment.yaml`	Développeur d'applications, DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises

Vérifiez le déploiement.	1. Pour vérifier si les pods sont prêts, exécutez la commande suivante.
	`kubectl get pods -o wide`
	Si le POD est prêt, la sortie doit ressembler à ce qui suit, avec le code « STATUS En cours d'exécution ».
	`NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES`
	`<pod_name> 1/1 Running 0 12d 192.168.18.50 ip-192-168-20-110.us-west-1.compute.internal <none> <none>`
	Notez le nom du Pod et le nom du nœud. Vous pouvez ignorer l'étape suivante.
	2. (Facultatif) Pour obtenir des informations supplémentaires sur le Pod et vérifier les tolérances sur le Pod,
		Développeur d'applications, DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises

	exécutez la commande suivante.
	
	`kubectl describe pod <pod_name>`
	
	Un exemple de sortie se trouve dans la section Informations supplémentaires.
	3. Pour vérifier que le placement du Pod sur le nœud est correct, exécutez la commande suivante.
	
	`kubectl describe node <node name> | grep -A 1 "Taints"`
	
	Vérifiez que la souillure du nœud correspond à la tolérance et que l'étiquette du nœud correspond à l'affinité du nœud définie dans. `deployment.yaml`
	
	Le pod avec les tolérances et l'affinité des nœuds doit être placé sur un nœud avec les teintes correspondantes et les étiquettes d'affinité des nœuds. La commande précédente vous indique les taches sur	

Tâche	Description	Compétences requises

	le nœud. Voici un exemple de sortie.
	
	`kubectl describe node ip-192-168-29-181.us-west-1.compute.internal | grep -A 1 "Taints"`
	`Taints: classifled_workload=true:NoSchedule`
	
	`machine_learning_workload=true:NoSchedule`
	
	En outre, exécutez la commande suivante pour vérifier que le nœud sur lequel le Pod est placé possède une étiquette correspondant à celle du nœud d'affinité du nœud.
	
	`kubectl get node <node name> --show-labels`
	
	4. Pour vérifier que l'application fait ce qu'elle est censée faire, consultez les journaux du Pod en exécutant la commande suivante.
	
	`kubectl logs -f <name-of-the-pod>`	

Tâche	Description	Compétences requises

Créez un deuxième fichier de déploiement .yaml sans tolérance ni affinité de nœud.	Cette étape supplémentaire consiste à valider que lorsqu'aucune affinité ou tolérance de nœud n'est spécifiée dans le fichier manifeste de déploiement, le Pod résultant n'est pas planifié sur un nœud présentant des entaches. (Il doit être planifié sur un nœud qui ne présente aucune trace). Utilisez le code suivant pour créer un nouveau fichier de déploiement appelé`deploy_no_taint.yaml` .
	
	`apiVersion: apps/v1`
	`kind: Deployment`
	`metadata:`
	`  name: microservice-deployment-non-tainted`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app.kubernetes.io/name: java-microservice-no-taint`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app.kubernetes.io/name: java-microservice-no-taint`
	`  spec:`
	`  containers:`
		Développeur d'applications, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>- name: java-microservice-container-2
	image: <account_number>.dkr.ecr<region>.amazonaws.com/<repository_name>:latest
	ports:
	- containerPort: 4567</pre>	

Tâche	Description	Compétences requises

Déployez le deuxième fichier .yaml de déploiement et validez le placement du Pod	1. Exécutez la commande suivante.
	`kubectl apply -f deploy_no_taint.yaml`
	2. Une fois le déploiement réussi, exécutez les mêmes commandes que celles que vous avez exécutées précédemment pour vérifier le placement du Pod dans un groupe de nœuds sans aucune altération.
	`kubectl describe node <node_name> | grep "Taints"`
	Le résultat doit être le suivant.
	`Taints: <none>`
	Ceci termine le test.
		Développeur d'applications, AWS DevOps, DevOps ingénieur

Nettoyage des ressources

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour éviter d'avoir à payer des frais AWS pour les ressources qui restent en cours d'exécuti	AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises
	on, utilisez la commande suivante. `eksctl delete cluster --name <Name of the cluster> --region <region-code>`	

Résolution des problèmes

Problème	Solution
Certaines de ces commandes risquent de ne pas s'exécuter si votre système utilise l'architecture arm64 (en particulier si vous l'exécutez sur un Mac M1). Il se peut que la ligne suivante comporte une erreur. `FROM adoptopenjdk/openjdk11:jdk-11.0.14.1_1-alpine`	Si vous rencontrez des erreurs lors de l'exécution du Dockerfile, remplacez la `FROM` ligne par la ligne suivante. `FROM bellsoft/liberica-openjdk-alpine-musl:17`

Ressources connexes

- Déployer un exemple de microservice Java sur Amazon EKS
- Création d'un référentiel privé Amazon ECR
- Affectation de pods à des nœuds (documentation Kubernetes)
- Atteintes et tolérances (documentation Kubernetes)
- Amazon EKS
- Amazon ECR
- AWS CLI
- Docker
- IntelliJ IDEA CE

- Eclipse

Informations supplémentaires

deployment.yaml

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: microservice-deployment
spec:
  replicas: 1
  selector:
    matchLabels:
      app.kubernetes.io/name: java-microservice
  template:
    metadata:
      labels:
        app.kubernetes.io/name: java-microservice
    spec:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: alpha.eksctl.io/nodegroup-name
                    operator: In
                    values:
                      - <node-group-name-from-cluster.yaml>
      tolerations: #only this pod has toleration and is viable to go to ng with taint
        - key: "<Taint key>" #classified_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
        - key: "<Taint key>" #machine_learning_workload in our case
          operator: Equal
          value: "<Taint value>" #true
          effect: "NoSchedule"
      containers:
        - name: java-microservice-container
          image: <account_number>.dkr.ecr<region>.amazonaws.com/
<repository_name>:latest
          ports:
```

```
            - containerPort: 4567
```

décrire un exemple de sortie du pod

```
Name:         microservice-deployment-in-tainted-nodes-5684cc495b-vpcfx
Namespace:    default
Priority:     0
Node:         ip-192-168-29-181.us-west-1.compute.internal/192.168.29.181
Start Time:   Wed, 14 Sep 2022 11:06:47 -0400
Labels:       app.kubernetes.io/name=java-microservice-taint
              pod-template-hash=5684cc495b
Annotations:  kubernetes.io/psp: eks.privileged
Status:       Running
IP:           192.168.13.44
IPs:
  IP:           192.168.13.44
Controlled By:  ReplicaSet/microservice-deployment-in-tainted-nodes-5684cc495b
Containers:
  java-microservice-container-1:
    Container ID:
 docker://5c158df8cc160de8f57f62f3ee16b12725a87510a809d90a1fb9e5d873c320a4
    Image:          934188034500.dkr.ecr.us-east-1.amazonaws.com/java-eks-apg
    Image ID:       docker-pullable://934188034500.dkr.ecr.us-east-1.amazonaws.com/
java-eks-apg@sha256:d223924aca8315aab20d54eddf3443929eba511b6433017474d01b63a4114835
    Port:           4567/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Wed, 14 Sep 2022 11:07:02 -0400
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-ddvvw (ro)
Conditions:
  Type              Status
  Initialized       True
  Ready             True
  ContainersReady   True
  PodScheduled      True
Volumes:
  kube-api-access-ddvvw:
    Type:                    Projected (a volume that contains injected data from
 multiple sources)
```

```
    TokenExpirationSeconds:  3607
    ConfigMapName:           kube-root-ca.crt
    ConfigMapOptional:       <nil>
    DownwardAPI:             true
QoS Class:                   BestEffort
Node-Selectors:              <none>
Tolerations:                 classifled_workload=true:NoSchedule
                             machine_learning_workload=true:NoSchedule
                             node.kubernetes.io/not-ready:NoExecute op=Exists for 300s
                             node.kubernetes.io/unreachable:NoExecute op=Exists for
 300s
Events:                      <none>
```

Répliquez les images filtrées des conteneurs Amazon ECR sur plusieurs comptes ou régions

Créée par Abdal Garuba (AWS)

Récapitulatif

Amazon Elastic Container Registry (Amazon ECR) peut répliquer toutes les images de conteneurs d'un référentiel d'images dans les régions Amazon Web Services (AWS) et les comptes AWS de manière native, en utilisant les fonctionnalités de réplication entre régions et entre comptes. (Pour plus d'informations, consultez le billet de blog AWS intitulé Cross region replication in Amazon ECR has landed.) Cependant, il n'existe aucun moyen de filtrer les images copiées entre les régions ou les comptes AWS en fonction de critères.

Ce modèle décrit comment répliquer des images de conteneurs stockées dans Amazon ECR sur des comptes et des régions AWS, sur la base de modèles de balises d'image. Le modèle utilise Amazon CloudWatch Events pour écouter les événements push relatifs aux images dotées d'une balise personnalisée prédéfinie. Un événement push démarre un CodeBuild projet AWS et lui transmet les détails de l'image. Le CodeBuild projet copie les images du registre Amazon ECR source vers le registre de destination en fonction des informations fournies.

Ce modèle copie les images dotées de balises spécifiques sur tous les comptes. Par exemple, vous pouvez utiliser ce modèle pour copier uniquement des images sécurisées prêtes à être produites sur le compte AWS de production. Dans le compte de développement, une fois les images testées de manière approfondie, vous pouvez ajouter une balise prédéfinie aux images sécurisées et suivre les étapes de ce modèle pour copier les images marquées sur le compte de production.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif pour les registres Amazon ECR source et de destination
- Autorisations administratives pour les outils utilisés dans ce modèle
- Docker installé sur votre machine locale à des fins de test
- AWS Command Line Interface (AWS CLI), pour l'authentification auprès d'Amazon ECR

Limites

- Ce modèle surveille les événements push du registre source dans une seule région AWS. Vous pouvez déployer ce modèle dans d'autres régions pour surveiller les registres de ces régions.
- Dans ce modèle, une règle Amazon CloudWatch Events écoute un seul modèle de balise d'image. Si vous souhaitez vérifier la présence de plusieurs modèles, vous pouvez ajouter des événements afin de détecter d'autres modèles de balises d'image.

Architecture

Architecture cible

Automatisation et mise à l'échelle

Ce modèle peut être automatisé à l'aide d'un script d'infrastructure en tant que code (IaC) et déployé à grande échelle. Pour utiliser des CloudFormation modèles AWS afin de déployer ce modèle, téléchargez la pièce jointe et suivez les instructions de la section Informations supplémentaires.

Vous pouvez rediriger plusieurs CloudWatch événements Amazon Events (avec différents modèles d'événements personnalisés) vers le même CodeBuild projet AWS afin de répliquer plusieurs modèles de balises d'image, mais vous devrez mettre à jour la validation secondaire dans le `buildspec.yaml` fichier (qui est incluse dans la pièce jointe et dans la section Outils) comme suit pour prendre en charge plusieurs modèles.

```
...
if [[ ${IMAGE_TAG} != release-* ]]; then
...
```

Outils

Services Amazon

- IAM — AWS Identity and Access Management (IAM) vous permet de gérer l'accès aux services et ressources AWS en toute sécurité. Dans ce modèle, vous devez créer le rôle IAM entre comptes qu'AWS CodeBuild assumera lors du transfert d'images de conteneurs vers le registre de destination.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un registre de conteneurs entièrement géré qui facilite le stockage, la gestion, le partage et le déploiement de vos images et artefacts de conteneurs où que vous soyez. Les actions d'envoi d'images vers le registre source

envoient les détails des événements du système au bus d'événements qui est récupéré par Amazon CloudWatch Events.

- AWS CodeBuild — AWS CodeBuild est un service d'intégration continue entièrement géré qui fournit la puissance de calcul nécessaire pour effectuer des tâches telles que la compilation du code source, l'exécution de tests et la production d'artefacts prêts à être déployés. Ce modèle utilise AWS CodeBuild pour effectuer l'action de copie depuis le registre Amazon ECR source vers le registre de destination.
- CloudWatch Événements — Amazon CloudWatch Events fournit un flux d'événements système décrivant les modifications apportées aux ressources AWS. Ce modèle utilise des règles pour associer les actions push Amazon ECR à un modèle de balise d'image spécifique.

Outils

- Docker CLI — Docker est un outil qui facilite la création et la gestion de conteneurs. Les conteneurs regroupent une application et toutes ses dépendances dans une unité ou un package qui peut être facilement déployé sur n'importe quelle plate-forme prenant en charge le runtime du conteneur.

Code

Vous pouvez implémenter ce modèle de deux manières :

- Configuration automatisée : déployez les deux CloudFormation modèles AWS fournis dans la pièce jointe. Pour obtenir des instructions, consultez la section Informations supplémentaires.
- Configuration manuelle : suivez les étapes décrites dans la section Epics.

Exemple de buildspec.yaml

Si vous utilisez les CloudFormation modèles fournis avec ce modèle, le `buildspec.yaml` fichier est inclus dans les CodeBuild ressources.

```
version: 0.2
env:
  shell: bash
phases:
  install:
    commands:
      - export CURRENT_ACCOUNT=$(echo ${CODEBUILD_BUILD_ARN} | cut -d':' -f5)
```

```
        - export CURRENT_ECR_REGISTRY=${CURRENT_ACCOUNT}.dkr.ecr.
${AWS_REGION}.amazonaws.com
        - export DESTINATION_ECR_REGISTRY=${DESTINATION_ACCOUNT}.dkr.ecr.
${DESTINATION_REGION}.amazonaws.com
    pre_build:
      on-failure: ABORT
      commands:
        - echo "Validating Image Tag ${IMAGE_TAG}"
        - |
          if [[ ${IMAGE_TAG} != release-* ]]; then
            aws codebuild stop-build --id ${CODEBUILD_BUILD_ID}
            sleep 60
            exit 1
          fi
        - aws ecr get-login-password --region ${AWS_REGION} | docker login -u AWS --
password-stdin ${CURRENT_ECR_REGISTRY}
        - docker pull ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
    build:
      commands:
        - echo "Assume cross-account role"
        - CREDENTIALS=$(aws sts assume-role --role-arn ${CROSS_ACCOUNT_ROLE_ARN} --
role-session-name Rolesession)
        - export AWS_DEFAULT_REGION=${DESTINATON_REGION}
        - export AWS_ACCESS_KEY_ID=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.AccessKeyId')
        - export AWS_SECRET_ACCESS_KEY=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SecretAccessKey')
        - export AWS_SESSION_TOKEN=$(echo ${CREDENTIALS} | jq -r
 '.Credentials.SessionToken')
        - echo "Logging into cross-account registry"
        - aws ecr get-login-password --region ${DESTINATION_REGION} | docker login -u
 AWS --password-stdin ${DESTINATION_ECR_REGISTRY}
        - echo "Check if Destination Repository exists, else create"
        - |
          aws ecr describe-repositories --repository-names ${REPO_NAME} --region
 ${DESTINATION_REGION} \
          || aws ecr create-repository --repository-name ${REPO_NAME} --region
 ${DESTINATION_REGION}
        - echo "retag image and push to destination"
        - docker tag ${CURRENT_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
 ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
        - docker push ${DESTINATION_ECR_REGISTRY}/${REPO_NAME}:${IMAGE_TAG}
```

Épopées

Création de rôles IAM

Tâche	Description	Compétences requises

Créez un rôle CloudWatch Events.	Dans le compte AWS source, créez un rôle IAM à assumer par Amazon CloudWatch Events. Le rôle doit être autorisé à démarrer un CodeBuild projet AWS.
	
	Pour créer le rôle à l'aide de l'AWS CLI, suivez les instructions de la documentation IAM.
	
	Exemple de politique de confiance (`trustpolicy.json`) :
	
	`{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": {"Service": "events.amazonaws.com"}, "Action": "sts:AssumeRole" } }`
	
	Exemple de politique d'autorisation (`permissionpolicy.json`) :
	
	`{`
		Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>{
	  "Version": "2012-10-17",
	  "Statement": {
	  "Effect": "Allow",
	  "Action": "codebuild:StartBuild",
	  "Resource": "<CodeBuild Project ARN>"
	  }
	}</pre>	

Tâche	Description	Compétences requises
Créez un CodeBuild rôle.	Créez un rôle IAM CodeBuild à assumer par AWS, en suivant les instructions de la documentation IAM. Le rôle doit disposer des autorisations suivantes : • Autorisation d'assumer le rôle multicompte de destination • Autorisation de créer des groupes de journaux et des flux de journaux, et de mettre des événements de journal • Autorisations en lecture seule pour tous les référentiels Amazon ECR, en ajoutant la politique EC2 ContainerRegistryReadOnly gérée par Amazon au rôle • Permission d'arrêter CodeBuild Exemple de politique de confiance (`trustpolicy.json`) : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`	Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	<pre>"Service": "codebuild.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> Exemple de politique d'autorisation (`permissionpolicy.json`) : <pre>{ "Version": "2012-10-17", "Statement": [{ "Action": ["codebuild:StartBuild", "codebuild:StopBuild", "codebuild:Get*", "codebuild:List*", "codebuild:BatchGet*"], "Resource": "*", "Effect": "Allow" }, { "Action": [</pre>	

Tâche	Description	Compétences requises
	"logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"], "Resource": "*", "Effect": "Allow" }, { "Action": "sts:AssumeRole", "Resource": "<ARN of destination role>", "Effect": "Allow", "Sid": "AssumeCrossAccountArn" }] } Attachez la politique gérée `AmazonEC2ContainerRegistryReadOnly` à la commande CLI comme suit : ~$ aws iam attach-role-policy \ --policy-arn arn:aws:iam::aws:policy/AmazonEC2ContainerRegistryReadOnly \	

Tâche	Description	Compétences requises
	`--role-name <name of CodeBuild Role>`	

Tâche	Description	Compétences requises
Créez un rôle multicompte.	Dans le compte AWS de destination, créez un rôle IAM pour le CodeBuild rôle AWS que le compte source doit assumer. Le rôle multi-comptes doit permettre aux images de conteneur de créer un nouveau référentiel et de télécharger des images de conteneur sur Amazon ECR. Pour créer le rôle IAM à l'aide de l'AWS CLI, suivez les instructions de la documentation IAM. Pour autoriser le CodeBuild projet AWS de l'étape précédente, appliquez la politique de confiance suivante : `{ "Version": "2012-10-17", "Statement": { "Effect": "Allow", "Principal": { "AWS": "<ARN of source codebuild role>" }, "Action": "sts:AssumeRole" } }`	Administrateur AWS, AWS DevOps, administrateur cloud, architecte cloud, DevOps ingénieur, administrateur système AWS

Tâche	Description	Compétences requises
	Pour autoriser le CodeBuild projet AWS de l'étape précédente à enregistrer des images dans le registre de destination, appliquez la politique d'autorisation suivante : `{ "Version": "2012-10-17", "Statement": [ { "Action": [ "ecr:GetDownloadUrlForLayer", "ecr:BatchCheckLayerAvailability", "ecr:PutImage", "ecr:InitiateLayerUpload", "ecr:UploadLayerPart", "ecr:CompleteLayerUpload", "ecr:GetRepositoryPolicy", "ecr:DescribeRepositories", "ecr:GetAuthorizationToken",`	

Tâche	Description	Compétences requises

	<pre>"ecr:CreateRepository"
	            ],
	            "Resource": "*",
	            "Effect": "Allow"
	        }
	    ]
	}</pre>	

Créez le CodeBuild projet

Tâche	Description	Compétences requises
Créez un CodeBuild projet.	Créez un CodeBuild projet AWS dans le compte source en suivant les instructions de la CodeBuild documentation AWS. Le projet doit se trouver dans la même région que le registre source. Configurez le projet comme suit : • Type d'environnement : `LINUX CONTAINER` • Rôle du service : `CodeBuild Role` • Mode privilégié : `true` • Image de l'environnement : `aws/codebuild/standard:x.x` (utilisez la dernière image disponible)	Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

	• Variables d'environnement :
	  • `CROSS_ACCOUNT_ROLE_ARN` : le nom de ressource Amazon (ARN) du rôle multicompte
	  • `DESTINATION_REGION` : le nom de la région à comptes multiples
	  • `DESTINATION_ACCOUNT` : le numéro du compte de destination
	• Spécifications de construction : utilisez le `buildspec.yaml` fichier répertorié dans la section Outils.	

Créez l'événement

Tâche	Description	Compétences requises
Créez une règle d'événements.	Comme le modèle utilise la fonctionnalité de filtrage de contenu, vous devez créer l'événement à l'aide d'Amazon EventBridge. Créez l'événement et la cible en suivant les instructions de la EventBridge documentation, avec quelques modifications : • Pour Définir le modèle, choisissez Modèle d'événement, puis sélectionnez Modèle personnalisé.	Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

	• Copiez l'exemple de code du modèle d'événements personnalisés suivant dans la zone de texte prévue à cet effet :
	
	`{ "source": ["aws.ecr "], "detail-type": ["ECR Image Action"], "detail": { "action-type": ["PUSH"], "result": ["SUCCESS"], "image-ta g": [{ "prefix": "release-"}] } }`
	
	• Pour Select targets, choisissez le CodeBuild projet AWS et collez l'ARN du CodeBuild projet AWS que vous avez créé dans l'épopée précédente.
	• Pour Configurer l'entrée, choisissez Input Transform er.
	• Dans la zone de texte Chemin d'entrée, collez :
	
	`{"IMAGE_TAG":"$.de tail.image-tag","R EPO_NAME":"$.detai`	

Tâche	Description	Compétences requises

	<pre>l.repository-name"
	}</pre>
	• Dans la zone de texte Modèle de saisie, collez :
	<pre>{"environmentVariablesOverride":
	[{"name":
	"IMAGE_TAG",
	"value":<IMAGE_TAG>},{"name":"REPO_NAME","value":<REPO_NAME>}]}</pre>
	• Choisissez Utiliser le rôle existant, puis choisissez le nom du rôle CloudWatch Événements que vous avez créé précédemment dans l'épique Créer des rôles IAM.	

Valider

Tâche	Description	Compétences requises
Authentifiez-vous auprès d'Amazon ECR.	Authentifiez-vous auprès des registres source et de destination en suivant les étapes de la documentation Amazon ECR.	Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, DevOps ingénieur, architecte cloud
Testez la réplication des images.	Dans votre compte source, envoyez une image de conteneur vers un référentiel source Amazon ECR	Administrateur AWS, AWS DevOps, administrateur système AWS, administr

Tâche	Description	Compétences requises
	nouveau ou existant avec une balise d'image préfixée par. `release-` Pour envoyer l'image, suivez les étapes décrites dans la documentation Amazon ECR. Vous pouvez suivre la progression du CodeBuild projet dans la CodeBuild console. Une fois le CodeBuild projet terminé avec succès, connectez-vous au compte AWS de destination, ouvrez la console Amazon ECR et vérifiez que l'image existe dans le registre Amazon ECR de destination.	ateur cloud, architecte cloud, DevOps ingénieur
Testez l'exclusion des images.	Dans votre compte source, envoyez une image de conteneur vers un référentiel source Amazon ECR nouveau ou existant avec une balise d'image ne comportant pas de préfixe personnalisé. Vérifiez que le CodeBuild projet n'est pas démarré et qu'aucune image de conteneur n'apparaît dans le registre de destination.	Administrateur AWS, AWS DevOps, administrateur système AWS, administr ateur cloud, architecte cloud, DevOps ingénieur

Ressources connexes

- Commencer avec CodeBuild
- Commencer à utiliser Amazon EventBridge
- Filtrage basé sur le contenu dans les modèles d'événements Amazon EventBridge
- Déléguez l'accès entre les comptes AWS à l'aide de rôles IAM
- Réplication d'images privées

Informations supplémentaires

Pour déployer automatiquement les ressources correspondant à ce modèle, procédez comme suit :

1. Téléchargez la pièce jointe et extrayez les deux CloudFormation modèles : `part-1-copy-tagged-images.yaml` et`part-2-destination-account-role.yaml`.
2. Connectez-vous à la CloudFormation console AWS et déployez `part-1-copy-tagged-images.yaml` dans le même compte AWS et dans la même région que les registres Amazon ECR sources. Mettez à jour les paramètres selon vos besoins. Le modèle déploie les ressources suivantes :
   - Rôle IAM dans Amazon CloudWatch Events
   - Rôle IAM dans le CodeBuild projet AWS
   - CodeBuild projet AWS
   - Règle CloudWatch relative aux événements AWS
3. Prenez note de la valeur de `SourceRoleName` dans l'onglet Sorties. Vous aurez besoin de cette valeur à l'étape suivante.
4. Déployez le second CloudFormation modèle`part-2-destination-account-role.yaml`, dans le compte AWS sur lequel vous souhaitez copier les images du conteneur Amazon ECR. Mettez à jour les paramètres selon vos besoins. Pour le `SourceRoleName` paramètre, spécifiez la valeur de l'étape 3. Ce modèle déploie le rôle IAM entre comptes.
5. Validez la réplication et l'exclusion des images, comme décrit dans la dernière étape de la section Epics.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Rotation des informations d'identification de base de données sans redémarrer les conteneurs

Créée par Josh Joy (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), vous pouvez utiliser AWS Secrets Manager pour alterner, gérer et récupérer les informations d'identification des bases de données tout au long de leur cycle de vie. Les utilisateurs et les applications récupèrent les secrets en appelant l'API Secrets Manager, ce qui évite de devoir coder en dur les informations sensibles en texte brut.

Si vous utilisez des conteneurs pour les charges de travail de microservices, vous pouvez stocker les informations d'identification en toute sécurité dans AWS Secrets Manager. Pour séparer la configuration du code, ces informations d'identification sont généralement injectées dans le conteneur. Cependant, il est important de changer régulièrement et automatiquement vos informations d'identification. Il est également important de soutenir la possibilité d'actualiser les informations d'identification après la révocation. Dans le même temps, les applications doivent pouvoir alterner les informations d'identification tout en réduisant tout impact potentiel sur la disponibilité en aval.

Ce modèle décrit comment alterner vos secrets sécurisés avec AWS Secrets Manager au sein de vos conteneurs sans avoir à redémarrer vos conteneurs. En outre, ce modèle réduit le nombre de recherches d'informations d'identification vers Secrets Manager en utilisant le composant de mise en cache côté client de Secrets Manager. Lorsque vous utilisez le composant de mise en cache côté client pour actualiser les informations d'identification dans l'application, le conteneur n'a pas besoin d'être redémarré pour récupérer les informations d'identification modifiées.

Cette approche fonctionne pour Amazon Elastic Kubernetes Service (Amazon EKS) et Amazon Elastic Container Service (Amazon ECS).

Deux scénarios sont abordés. Dans le scénario mono-utilisateur, les informations d'identification de base de données sont actualisées lors d'une rotation secrète en détectant les informations d'identification expirées. Le cache d'informations d'identification reçoit l'ordre d'actualiser le secret, puis l'application rétablit la connexion à la base de données. Le composant de mise en cache côté client met en cache les informations d'identification dans l'application et permet d'éviter de contacter Secrets Manager pour chaque recherche d'informations d'identification. Les informations d'identification sont modifiées dans l'application sans qu'il soit nécessaire de forcer l'actualisation des informations d'identification en redémarrant le conteneur.

Le second scénario fait alterner le secret en alternant entre deux utilisateurs. Le fait d'avoir deux utilisateurs actifs réduit les risques d'indisponibilité, car les informations d'identification d'un utilisateur sont toujours actives. La rotation des informations d'identification entre deux utilisateurs est utile lorsque vous avez un déploiement de grande envergure avec des clusters dans lesquels le délai de propagation des mises à jour des informations d'identification peut être faible.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Application exécutée dans un conteneur dans Amazon EKS ou Amazon ECS.
- Informations d'identification stockées dans Secrets Manager, avec rotation activée.
- Un deuxième ensemble d'informations d'identification stockées dans Secrets Manager, en cas de déploiement de la solution à deux utilisateurs. Des exemples de code peuvent être trouvés dans le GitHub repo aws-secrets-manager-rotation-lambdas.
- Une base de données Amazon Aurora.

Limites

- Cet exemple est destiné aux applications Python. Pour les applications Java, vous pouvez utiliser le composant de mise en cache côté client Java ou la bibliothèque de mise en cache côté client JDBC pour Secrets Manager.

Architecture

Architecture cible

Scénario 1 — Rotation d'un identifiant pour un seul utilisateur

Dans le premier scénario, un seul identifiant de base de données est périodiquement modifié par Secrets Manager. Le conteneur d'applications s'exécute dans Fargate. Lorsque la première connexion à la base de données est établie, le conteneur de l'application récupère les informations d'identification de base de données pour Aurora. Le composant de mise en cache de Secrets Manager met ensuite en cache les informations d'identification pour l'établissement de futures connexions. Lorsque la période de rotation est écoulée, les informations d'identification expirent et la

base de données renvoie une erreur d'authentification. L'application récupère ensuite les informations d'identification modifiées, invalide le cache et met à jour le cache des informations d'identification via le composant de mise en cache côté client de Secrets Manager.

Dans ce scénario, les perturbations peuvent être minimes lors de la rotation des informations d'identification et lorsque les connexions périmées utilisent des informations d'identification périmées. Ce problème peut être résolu en utilisant le scénario à deux utilisateurs.

Scénario 2 — Rotation des informations d'identification pour deux utilisateurs

Dans le second scénario, les informations d'identification de deux utilisateurs de base de données (celles d'Alice et de Bob) sont périodiquement modifiées par Secrets Manager. Le conteneur d'applications s'exécute dans un cluster Fargate. Lorsque la première connexion à la base de données est établie, le conteneur de l'application récupère les informations d'identification de la base de données Aurora pour le premier utilisateur (Alice). Le composant de mise en cache de Secrets Manager met ensuite en cache les informations d'identification pour l'établissement de futures connexions.

Bien qu'il y ait deux utilisateurs et deux identifiants, un seul identifiant actif est géré par Secrets Manager. Dans ce cas, le composant de mise en cache expire périodiquement et récupère les dernières informations d'identification. Si la période de rotation de Secrets Manager est plus longue que le délai d'expiration du cache, le composant de mise en cache récupère les informations d'identification modifiées pour le deuxième utilisateur (Bob). Par exemple, si l'expiration du cache est mesurée en minutes et que la période de rotation est mesurée en jours, le composant de mise en cache récupère les nouvelles informations d'identification dans le cadre de son actualisation périodique du cache. De cette façon, le temps d'arrêt est réduit au minimum car les informations d'identification de chaque utilisateur sont actives pendant une rotation de Secrets Manager.

Automatisation et mise à l'échelle

Vous pouvez utiliser AWS CloudFormation pour déployer ce modèle en utilisant l'infrastructure comme code. Cela construit et crée le conteneur d'applications, crée la tâche Fargate, déploie le conteneur dans Fargate et installe et configure Secrets Manager avec Aurora. Pour les instructions de step-by-step déploiement, consultez le fichier readme.

Outils

Outils

- AWS Secrets Manager permet de remplacer les informations d'identification codées en dur, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret. Comme Secrets Manager peut automatiquement alterner le secret selon un calendrier, vous pouvez remplacer les secrets à long terme par des secrets à court terme, réduisant ainsi le risque de compromission.
- Docker aide les développeurs à emballer, expédier et exécuter n'importe quelle application sous la forme d'un conteneur léger, portable et autonome.

Code

Exemple de code Python

Ce modèle utilise le composant de mise en cache côté client Python pour que Secrets Manager récupère les informations d'authentification lors de l'établissement de la connexion à la base de données. Le composant de mise en cache côté client permet d'éviter de contacter Secrets Manager à chaque fois.

Désormais, à l'expiration de la période de rotation, les informations d'identification mises en cache expirent et la connexion à la base de données entraîne une erreur d'authentification. Pour MySQL, le code d'erreur d'authentification est 1045. Cet exemple utilise Amazon Aurora pour MySQL, mais vous pouvez utiliser un autre moteur tel que PostgreSQL. En cas d'erreur d'authentification, le code de gestion des exceptions de connexion à la base de données détecte l'erreur. Il demande ensuite au composant de mise en cache côté client de Secrets Manager d'actualiser le secret, puis de réauthentifier et de rétablir la connexion à la base de données. Si vous utilisez PostgreSQL ou un autre moteur, vous devez rechercher le code d'erreur d'authentification correspondant.

L'application du conteneur peut désormais mettre à jour le mot de passe de la base de données avec le mot de passe modifié sans redémarrer le conteneur.

Placez le code suivant dans le code de votre application qui gère les connexions aux bases de données. Cet exemple utilise Django et sous-classe le backend de base de données avec un wrapper de base de données pour les connexions. Si vous utilisez un autre langage de programmation ou une autre bibliothèque de connexion à la base de données, consultez votre bibliothèque de connexions à la base de données pour savoir comment sous-classer la récupération des connexions à la base de données.

```
    def get_new_connection(self, conn_params):
        try:
```

```
            logger.info("get connection")
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn =super(DatabaseWrapper,self).get_new_connection(conn_params)
            return conn
        except MySQLdb.OperationalError as e:
            error_code=e.args[0]
            if error_code!=1045:
                raise e

            logger.info("Authentication error. Going to refresh secret and try again.")
            databasecredentials.refresh_now()
            databasecredentials.get_conn_params_from_secrets_manager(conn_params)
            conn=super(DatabaseWrapper,self).get_new_connection(conn_params)
            logger.info("Successfully refreshed secret and established new database
connection.")
            return conn
```

Code AWS CloudFormation et Python

- https://github.com/aws-samples/aws-secrets-manager-credential-rotation-without-container-restart

Épopées

Maintenir la disponibilité des applications pendant la rotation des accréditations

Tâche	Description	Compétences requises
Installez le composant de mise en cache.	Téléchargez et installez le composant de mise en cache côté client Secrets Manager pour Python. Pour le lien de téléchargement, consultez la section Ressources connexes.	Developer
Mettez en cache les informati ons d'identification de travail.	Utilisez le composant de mise en cache côté client de Secrets Manager pour mettre en cache les informati ons d'identification de travail localement.	Developer

Tâche	Description	Compétences requises
Mettez à jour le code de l'application pour actualiser les informations d'identification en cas d'erreur non autorisée lors de la connexion à la base de données.	Mettez à jour le code de l'application afin d'utiliser Secrets Manager pour récupérer et actualiser les informations d'identification de la base de données. Ajoutez la logique permettant de gérer les codes d'erreur non autorisés, puis récupérez les informations d'identification récemment modifiées. Consultez la section Exemple de code Python.	Developer

Ressources connexes

Création d'un secret dans le Gestionnaire de Secrets

- Création de clés dans AWS KMS
- Créez et gérez des secrets avec AWS Secrets Manager

Création d'un cluster Amazon Aurora

- Création d'une instance de base de données Amazon RDS

Création des composants Amazon ECS

- Création d'un cluster à l'aide de la console classique
- Création d'une image Docker
- Création d'un dépôt privé
- Registre privé Amazon ECR
- Envoyer une image Docker
- Définitions des tâches Amazon ECS

- Création d'un service Amazon ECS dans la console classique

Téléchargez et installez le composant de mise en cache côté client de Secrets Manager

- Client de mise en cache Python

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Exécutez des tâches Amazon ECS sur Amazon WorkSpaces avec Amazon ECS Anywhere

Créée par Akash Kumar (AWS)

Récapitulatif

Amazon Elastic Container Service (Amazon ECS) Anywhere prend en charge le déploiement de tâches Amazon ECS dans n'importe quel environnement, y compris l'infrastructure gérée par Amazon Web Services (AWS) et l'infrastructure gérée par le client. Vous pouvez le faire en utilisant un plan de contrôle entièrement géré par AWS, exécuté dans le cloud et toujours à jour.

Les entreprises utilisent souvent Amazon WorkSpaces pour développer des applications basées sur des conteneurs. Cela a nécessité Amazon Elastic Compute Cloud (Amazon EC2) ou AWS Fargate avec un cluster Amazon ECS pour tester et exécuter des tâches ECS. Désormais, en utilisant Amazon ECS Anywhere, vous pouvez ajouter Amazon WorkSpaces en tant qu'instances externes directement à un cluster ECS, et vous pouvez exécuter vos tâches directement. Cela réduit votre temps de développement, car vous pouvez tester votre conteneur avec un cluster ECS localement sur Amazon WorkSpaces. Vous pouvez également économiser sur le coût d'utilisation EC2 des instances Fargate pour tester vos applications de conteneurs.

Ce modèle montre comment déployer des tâches ECS sur Amazon WorkSpaces avec Amazon ECS Anywhere. Il configure le cluster ECS et utilise AWS Directory Service Simple AD pour lancer le WorkSpaces. Ensuite, l'exemple de tâche ECS lance NGINX dans le. WorkSpaces

Conditions préalables et limitations

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI)
- Informations d'identification AWS configurées sur votre machine

Architecture

Pile technologique cible

- Un cloud privé virtuel (VPC)
- Un cluster Amazon ECS

- Amazon WorkSpaces
- AWS Directory Service avec Simple AD

Architecture cible

L'architecture inclut les services et ressources suivants :

- Un cluster ECS avec des sous-réseaux publics et privés dans un VPC personnalisé
- Simple AD dans le VPC pour permettre aux utilisateurs d'accéder à Amazon WorkSpaces
- Amazon WorkSpaces provisionné dans le VPC à l'aide de Simple AD
- AWS Systems Manager est activé pour ajouter Amazon en WorkSpaces tant qu'instances gérées
- À l'aide d'Amazon ECS et d'AWS Systems Manager Agent (agent SSM), Amazon WorkSpaces a ajouté à Systems Manager et au cluster ECS
- Exemple de tâche ECS à exécuter WorkSpaces dans le cluster ECS

Outils

- AWS Directory Service Simple Active Directory (Simple AD) est un annuaire géré autonome alimenté par un serveur compatible Samba 4 Active Directory. Simple AD fournit un sous-ensemble des fonctionnalités proposées par AWS Managed Microsoft AD, notamment la possibilité de gérer les utilisateurs et de se connecter en toute sécurité aux EC2 instances Amazon.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Systems Manager vous aide à gérer vos applications et votre infrastructure exécutées dans le cloud AWS. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos ressources AWS en toute sécurité à grande échelle.
- Amazon vous WorkSpaces aide à fournir des postes de travail Microsoft Windows ou Amazon Linux virtuels basés sur le cloud pour vos utilisateurs, connus sous WorkSpacesle nom de. WorkSpaces élimine le besoin d'acheter et de déployer du matériel ou d'installer des logiciels complexes.

Épopées

Configuration du cluster ECS

Tâche	Description	Compétences requises
Créez et configurez le cluster ECS.	Pour créer le cluster ECS, suivez les instructions de la documentation AWS, notamment les étapes suivantes : • Pour sélectionner la compatibilité du cluster, choisissez Networking only, qui prendra en charge un Amazon WorkSpace en tant qu'instance externe du cluster ECS. • Choisissez de créer un nouveau VPC.	Architecte du cloud

Lancez Amazon WorkSpaces

Tâche	Description	Compétences requises
Configurez Simple AD et lancez Amazon WorkSpaces.	Pour configurer un répertoire Simple AD pour votre VPC nouvellement créé et lancer Amazon WorkSpaces, suivez les instructions de la documentation AWS.	Architecte du cloud

Configuration d'AWS Systems Manager pour un environnement hybride

Tâche	Description	Compétences requises
Téléchargez les scripts ci-joints.	Sur votre ordinateur local, téléchargez les `ssm-activation.json` fichiers `ssm-trust-policy.json` et qui se trouvent dans la section Pièces jointes.	Architecte du cloud

Ajoutez le rôle IAM.	Ajoutez des variables d'environnement en fonction des besoins de votre entreprise.
	`export AWS_DEFAULT_REGION=${AWS_REGION_ID}`
	`export ROLE_NAME=${ECS_TASK_ROLE}`
	`export CLUSTER_NAME=${ECS_CLUSTER_NAME}`
	`export SERVICE_NAME=${ECS_CLUSTER_SERVICE_NAME}`
	Exécutez la commande suivante.
	`aws iam create-role --role-name $ROLE_NAME --assume-role-policy-document file://ssm-trust-policy.json`
		Architecte du cloud

Ajoutez la SSMManaged InstanceCore politique Amazon au rôle IAM.	Exécutez la commande suivante.	Architecte du cloud

Tâche	Description	Compétences requises
	`aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore`	
Ajoutez la politique Amazon EC2 ContainerServicefor EC2 Role au rôle IAM.	Exécutez la commande suivante. `aws iam attach-role-policy --role-name $ROLE_NAME --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEC2ContainerServiceforEC2Role`	Architecte du cloud
Vérifiez le rôle IAM.	Pour vérifier le rôle IAM, exécutez la commande suivante. `aws iam list-attached-role-policies --role-name $ROLE_NAME`	Architecte du cloud
Activez Systems Manager.	Exécutez la commande suivante. `aws ssm create-activation --iam-role $ROLE_NAME | tee ssm-activation.json`	Architecte du cloud

Ajouter WorkSpaces au cluster ECS

Tâche	Description	Compétences requises
Connect à votre WorkSpaces.	Pour vous connecter à vos espaces de travail et les configurer, suivez les instructions de la documentation AWS.	Développeur d'applications
Téléchargez le script d'installation ecs-anywhere.	À l'invite de commande, exécutez la commande suivante. `curl -o "ecs-anywhere-install.sh" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh" && sudo chmod +x ecs-anywhere-install.sh`	Développeur d'applications
Vérifiez l'intégrité du script shell.	(Facultatif) Exécutez la commande suivante. `curl -o "ecs-anywhere-install.sh.sha256" "https://amazon-ecs-agent-packages-preview.s3.us-east-1.amazonaws.com/ecs-anywhere-install.sh.sha256" && sha256sum -c ecs-anywhere-install.sh.sha256`	Développeur d'applications

Tâche	Description	Compétences requises
Ajoutez un référentiel EPEL sur Amazon Linux.	Pour ajouter un référentiel EPEL (Extra Packages for Enterprise Linux), exécutez la commande`sudo amazon-linux-extras install epel -y`.	Développeur d’applications
Installez Amazon ECS Anywhere.	Pour exécuter le script d'installation, utilisez la commande suivante. `sudo ./ecs-anywhere-install.sh --cluster $CLUSTER_NAME --activation-id $ACTIVATION_ID --activation-code $ACTIVATION_CODE --region $AWS_REGION`	
Vérifiez les informations d'instance à partir du cluster ECS.	Pour vérifier les informations relatives à l'instance de cluster Systems Manager et ECS et valider WorkSpaces celles qui ont été ajoutées au cluster, exécutez la commande suivante depuis votre ordinateur local. `aws ssm describe-instance-information" && "aws ecs list-container-instances --cluster $CLUSTER_NAME`	Développeur d’applications

Ajoutez une tâche ECS pour WorkSpaces

Tâche	Description	Compétences requises
Créez un rôle IAM d'exécution de tâches.	Téléchargez `task-execution-assume-role.json` et `external-task-definition.json` depuis la section Pièces jointes. Sur votre ordinateur local, exécutez la commande suivante. `aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	Architecte du cloud
Ajoutez la politique au rôle d'exécution.	Exécutez la commande suivante. `aws iam --region $AWS_DEFAULT_REGION attach-role-policy --role-name $ECS_TASK_EXECUTION_ROLE --policy-arn arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy`	Architecte du cloud
Créez un rôle de tâche.	Exécutez la commande suivante.	Architecte du cloud

Tâche	Description	Compétences requises
	`aws iam --region $AWS_DEFAULT_REGION create-role --role-name $ECS_TASK_EXECUTION_ROLE --assume-role-policy-document file://task-execution-assume-role.json`	
Enregistrez la définition de tâche dans le cluster.	Sur votre ordinateur local, exécutez la commande suivante. `aws ecs register-task-definition --cli-input-json file://external-task-definition.json`	Architecte du cloud
Exécutez la tâche.	Sur votre ordinateur local, exécutez la commande suivante. `aws ecs run-task --cluster $CLUSTER_NAME --launch-type EXTERNAL --task-definition nginx`	Architecte du cloud

Tâche	Description	Compétences requises

Validez l'état d'exécution de la tâche.	Pour récupérer l'ID de tâche, exécutez la commande suivante.
	`export TEST_TASKID= $(aws ecs list-tasks -- cluster $CLUSTER_NAME | jq -r '.taskArns[0]')`
	À l'aide de l'ID de tâche, exécutez la commande suivante.
	`aws ecs describe-tasks --cluster $CLUSTER_ NAME --tasks ${TEST_TA SKID}`
		Architecte du cloud

Vérifiez la tâche sur le WorkSpace.	Pour vérifier que NGINX s'exécute sur le WorkSpace , exécutez la commande. `curl http://lo calhost:8080`	Développeur d’applications

Ressources connexes

- Clusters ECS
- Configuration d'un environnement hybride
- Amazon WorkSpaces
- Simple AD

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Exécuter un conteneur Docker d'API Web ASP.NET Core sur une instance Amazon Linux EC2

Créée par Vijai Anand Ramalingam (AWS) et Sreelaxmi Pai (AWS)

Récapitulatif

Ce modèle s'adresse aux personnes qui commencent à conteneuriser leurs applications sur le cloud Amazon Web Services (AWS). Lorsque vous commencez à conteneuriser des applications dans le cloud, aucune plateforme d'orchestration de conteneurs n'est généralement configurée. Ce modèle vous permet de configurer rapidement une infrastructure sur AWS pour tester vos applications conteneurisées sans avoir besoin d'une infrastructure d'orchestration de conteneurs élaborée.

La première étape du processus de modernisation consiste à transformer l'application. S'il s'agit d'une ancienne application .NET Framework, vous devez d'abord remplacer le moteur d'exécution par ASP.NET Core. Ensuite, procédez comme suit :

- Création de l'image du conteneur Docker
- Exécutez le conteneur Docker à l'aide de l'image créée
- Validez l'application avant de la déployer sur une plateforme d'orchestration de conteneurs, telle qu'Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS).

Ce modèle couvre les aspects liés à la création, à l'exécution et à la validation du développement d'applications modernes sur une instance Linux Amazon Elastic Compute Cloud (Amazon EC2).

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- Un rôle AWS Identity and Access Management (IAM) avec un accès suffisant pour créer des ressources AWS correspondant à ce modèle
- Visual Studio Community 2022 ou version ultérieure téléchargé et installé
- Un projet .NET Framework modernisé vers ASP.NET Core
- Un GitHub référentiel

Versions du produit

- Visual Studio Community 2022 ou version ultérieure

Architecture

Architecture cible

Ce modèle utilise un CloudFormation modèle AWS pour créer l'architecture hautement disponible illustrée dans le schéma suivant. Une instance Amazon EC2 Linux est lancée dans un sous-réseau privé. Le gestionnaire de session AWS Systems Manager est utilisé pour accéder à l'instance privée Amazon EC2 Linux et pour tester l'API exécutée dans le conteneur Docker.

1. Accès à l'instance Linux via le gestionnaire de session

Outils

Services AWS

- Interface de ligne de commande AWS — L'interface de ligne de commande AWS (AWS CLI) est un outil open source permettant d'interagir avec les services AWS via des commandes dans votre shell de ligne de commande. Avec une configuration minimale, vous pouvez exécuter des commandes de l'interface de ligne de commande AWS qui mettent en œuvre des fonctionnalités équivalentes à celles fournies par la console de gestion AWS basée sur un navigateur.
- AWS Management Console — L'AWS Management Console est une application Web qui comprend et fait référence à une vaste collection de consoles de service pour la gestion des ressources AWS. Lors de votre première connexion, vous accédez à la page d'accueil de la console. La page d'accueil donne accès à chaque console de service et propose un emplacement unique pour accéder aux informations dont vous avez besoin pour effectuer vos tâches liées à AWS.
- Gestionnaire de session AWS Systems Manager — Le gestionnaire de session est une fonctionnalité AWS Systems Manager entièrement gérée. Avec Session Manager, vous pouvez gérer vos instances Amazon Elastic Compute Cloud (Amazon EC2). Le gestionnaire de session fournit une gestion des nœuds sécurisée et vérifiable sans qu'il soit nécessaire d'ouvrir les ports entrants, de gérer les hôtes Bastion ou de gérer les clés SSH.

Autres outils

- Visual Studio 2022 — Visual Studio 2022 est un environnement de développement intégré (IDE).
- Docker — Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.

Code

```
FROM mcr.microsoft.com/dotnet/aspnet:5.0 AS base
 WORKDIR /app
EXPOSE 80
EXPOSE 443

FROM mcr.microsoft.com/dotnet/sdk:5.0 AS build
WORKDIR /src
COPY ["DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj", "DemoNetCoreWebAPI/"]
RUN dotnet restore "DemoNetCoreWebAPI/DemoNetCoreWebAPI.csproj"
COPY . .
WORKDIR "/src/DemoNetCoreWebAPI"
RUN dotnet build "DemoNetCoreWebAPI.csproj" -c Release -o /app/build

FROM build AS publish
RUN dotnet publish "DemoNetCoreWebAPI.csproj" -c Release -o /app/publish

FROM base AS final
WORKDIR /app
COPY --from=publish /app/publish .
ENTRYPOINT ["dotnet", "DemoNetCoreWebAPI.dll"]
```

Épopées

Développement de l'API Web ASP.NET Core

Tâche	Description	Compétences requises
Créez un exemple d'API Web ASP.NET Core à l'aide de Visual Studio.	Pour créer un exemple d'API Web ASP.NET Core, procédez comme suit :	Développeur d’applications

Tâche	Description	Compétences requises

	1. Ouvrez Visual Studio 2022.
	2. Choisissez Créer un projet.
	3. Sélectionnez le modèle de projet ASP.NET Core Web API, puis choisissez Next.
	4. Pour le nom du projet, entrez DemoNetCo reWebAPI, puis choisissez Next.
	5. Choisissez Créer.
	6. Pour exécuter le projet localement, appuyez sur F5.
	7. Vérifiez que le point de terminaison de WeatherFo recastl'API par défaut renvoie les résultats à l'aide de Swagger.
	8. Ouvrez l'invite de commande, accédez au dossier du projet .csproj et exécutez les commandes suivantes pour transférer la nouvelle API Web vers votre référentiel. GitHub
	`git add --all`
	`git commit -m “Initial Version”`
	`git push`	

Tâche	Description	Compétences requises
Créez un fichier Dockerfile.	Pour créer un Dockerfile, effectuez l'une des opérations suivantes : • Créez le Dockerfile manuellement à l'aide de l'exemple de Dockerfile dans la section Code. En fonction des exigences , sélectionnez l'image de base .NET appropriée. Pour plus d'informations sur les images associées à .NET et ASP.NET Core, consultez Docker hub. • Créez le Dockerfile à l'aide de Visual Studio et Docker Desktop. Dans l'explorateur de solutions , cliquez avec le bouton droit sur le projet, choisisse z Ajouter -> Support Docker. Pour le système d'exploit ation cible, sélectionnez Linux. Assurez-vous que le nouveau Dockerfile se trouve dans le même chemin que le fichier de solution (.sln). Pour appliquer les modificat ions à votre GitHub dépôt, exécutez la commande suivante.	Développeur d’applications

Tâche	Description	Compétences requises

	`git add --all`
	`git commit -m “Dockerfile added”`
	`git push`	

Configuration de l'instance Amazon EC2 Linux

Tâche	Description	Compétences requises
Configurez l'infrastructure.	Lancez le CloudFormation modèle AWS pour créer l'infrastructure, qui inclut les éléments suivants : • Un cloud privé virtuel (VPC) utilisant le service AWS VPC Quick Start, avec deux sous-réseaux publics et deux sous-réseaux privés répartis sur deux zones de disponibilité. • Le rôle IAM requis pour activer AWS Systems Manager. • Dans l'un des sous-réseaux privés, une instance de démonstration Amazon Linux 2 dotée de la dernière version de l'agent SSM. Bien que cette instance ne dispose d'aucune connectivité directe depuis Internet, elle est accessible en toute sécurité à l'aide d'AWS	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	Systems Manager Session Manager sans avoir besoin d'un hôte bastion. **Note** Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs. Pour en savoir plus sur l'accès à une EC2 instance Amazon privée à l'aide du gestionnaire de session sans avoir besoin d'un hôte bastion, consultez le billet de blog Toward a bastion-less world.	

Tâche	Description	Compétences requises
Connectez-vous à l'instance Amazon EC2 Linux.	Pour vous connecter à l'instance Amazon EC2 Linux dans le sous-réseau privé, procédez comme suit : 1. Ouvrez la EC2 console Amazon. 2. Dans le panneau de navigation, choisissez Instances. 3. Sélectionnez l'instance de démonstration Amazon Linux 2, puis sélectionnez Connect. **Note** Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs. 4. Choisissez Session Manager. 5. Choisissez Connect pour ouvrir une nouvelle fenêtre de terminal. 6. Exécutez la commande suivante. `sudo su`	Développeur d’applications

Tâche	Description	Compétences requises

Installez et démarrez Docker.	Pour installer et démarrer Docker dans l'instance Amazon EC2 Linux, procédez comme suit :
	1. Pour installer Docker, exécutez la commande suivante.
	`yum install -y docker`
	2. Pour démarrer le service Docker, exécutez la commande suivante.
	`service docker start`
	3. Pour vérifier l'installation de Docker, exécutez la commande suivante.
	`docker info`
		Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

Installez Git et clonez le dépôt.	Pour installer Git sur l'instance Amazon EC2 Linux et cloner le référentiel à partir de GitHub celui-ci, procédez comme suit.
	1. Pour installer Git, exécutez la commande suivante.
	`yum install git -y`
	2. Pour cloner le dépôt, exécutez la commande suivante.
	`git clone https://github.com/<username>/<repo-name>.git`
	3. Pour accéder au Dockerfile, exécutez la commande suivante.
	`cd <repo-name>/DemoNetCoreWebAPI/`
		Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

Créez et exécutez le conteneur Docker.	Pour créer l'image Docker et exécuter le conteneur dans l'instance Amazon EC2 Linux, procédez comme suit :
	1. Pour créer l'image Docker, exécutez la commande suivante.
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Pour afficher toutes les images Docker, exécutez la commande suivante.
	`docker images`
	3. Pour créer et exécuter le conteneur, exécutez la commande suivante.
	`docker run -d -p 80:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
		Développeur d'applications, administrateur AWS, AWS DevOps

Testez l'API Web

Tâche	Description	Compétences requises
Testez l'API Web à l'aide de la commande curl.	Pour tester l'API Web, exécutez la commande suivante.	Développeur d’applications

Tâche	Description	Compétences requises
	`curl -X GET "http://localhost/WeatherForecast" -H "accept: text/plain"` Vérifiez la réponse de l'API. **Note** Vous pouvez obtenir les commandes curl pour chaque point de terminaison auprès de Swagger lorsque vous l'exécutez localement.	

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez toutes les ressources.	Supprimez la pile pour supprimer toutes les ressources. Cela garantit que vous n'êtes pas facturé pour les services que vous n'utilisez pas.	Administrateur AWS, AWS DevOps

Ressources connexes

- Connectez-vous à votre instance Linux depuis Windows à l'aide de PuTTY
- Création d'une API Web avec ASP.NET Core
- Vers un monde sans bastions

Exécutez des charges de travail basées sur les messages à grande échelle à l'aide d'AWS Fargate

Créée par Stan Zubarev (AWS)

Récapitulatif

Ce modèle montre comment exécuter des charges de travail basées sur des messages à grande échelle dans le cloud AWS à l'aide de conteneurs et d'AWS Fargate.

L'utilisation de conteneurs pour traiter les données peut être utile lorsque la quantité de données traitée par une application dépasse les limites des services de calcul sans serveur basés sur les fonctions. Par exemple, si une application nécessite une capacité de calcul ou un temps de traitement supérieurs à ceux proposés par AWS Lambda, l'utilisation de Fargate peut améliorer les performances.

L'exemple de configuration suivant utilise l'AWS Cloud Development Kit (AWS CDK) TypeScript pour configurer et déployer les ressources suivantes dans le cloud AWS :

- Un service Fargate
- Une file d'attente Amazon Simple Queue Service (Amazon SQS)
- Une table Amazon DynamoDB.
- Un tableau de CloudWatch bord Amazon

Le service Fargate reçoit et traite les messages provenant de la file d'attente Amazon SQS, puis les stocke dans la table Amazon DynamoDB. Vous pouvez contrôler le nombre de messages Amazon SQS traités et le nombre d'éléments DynamoDB créés par Fargate à l'aide du tableau de bord. CloudWatch

> **Note**
>
> Vous pouvez également utiliser l'exemple de code de ce modèle pour créer des charges de travail de traitement de données plus complexes dans des architectures sans serveur pilotées par des événements. Pour plus d'informations, consultez Exécuter des charges de travail planifiées et pilotées par des événements à grande échelle avec AWS Fargate.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- La dernière version de l'interface de ligne de commande AWS (AWS CLI), installée et configurée sur votre machine locale
- Git, installé et configuré sur votre machine locale
- Le kit AWS CDK, installé et configuré sur votre machine locale
- Go, installé et configuré sur votre machine locale
- Docker, installé et configuré sur votre machine locale

Architecture

Pile technologique cible

- Amazon SQS
- AWS Fargate
- Amazon DynamoDB

Architecture cible

Le schéma suivant montre un exemple de flux de travail pour exécuter des charges de travail basées sur des messages à grande échelle dans le cloud AWS à l'aide de Fargate :

Le schéma suivant illustre le flux de travail suivant :

1. Le service Fargate utilise de longues interrogations Amazon SQS pour recevoir des messages provenant d'une file d'attente Amazon SQS.
2. Le service Fargate traite ensuite les messages Amazon SQS et les stocke dans une table DynamoDB.

Automatisation et mise à l'échelle

Pour automatiser le dimensionnement de votre nombre de tâches Fargate, vous pouvez configurer Amazon Elastic Container Service (Amazon ECS) Service Auto Scaling. Il est recommandé de

configurer la politique de dimensionnement en fonction du nombre de messages visibles dans la file d'attente Amazon SQS de votre application.

Pour plus d'informations, consultez la section Mise à l'échelle basée sur Amazon SQS dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

Outils

Services AWS

- AWS Fargate vous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou d'instances Amazon Elastic Compute Cloud (Amazon EC2). Il est utilisé conjointement avec Amazon Elastic Container Service (Amazon ECS).
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.

Code

Le code de ce modèle est disponible dans le dépôt GitHub sqs-fargate-ddb-cdk-go.

Épopées

Créez et déployez les ressources à l'aide du kit AWS CDK

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Clonez le dépôt GitHub sqs-fargate-ddb-cdk-go sur votre machine locale en exécutant la commande suivante : `git clone https://github.com/aws-samp`	Développeur d’applications

Tâche	Description	Compétences requises
	`les/sqs-fargate-dd b-cdk-go.git`	

Tâche	Description	Compétences requises
Vérifiez que l'AWS CLI est configurée sur le bon compte AWS et que le CDK AWS dispose des autorisations requises.	Pour vérifier si les paramètres de configuration de votre AWS CLI sont corrects, vous pouvez exécuter la commande Amazon Simple Storage Service (Amazon S3) ls suivante : `aws s3 ls` Cette procédure nécessite également que le CDK AWS dispose des autorisations nécessaires pour provisionner l'infrastructure au sein de votre compte AWS. Pour accorder les autorisations requises, vous devez créer un profil AWS nommé dans la CLI AWS et l'exporter en tant que variable d'AWS_PROFILEenvironnement. **Note** Si vous n'avez jamais utilisé le CDK AWS dans votre compte AWS auparavant, vous devez d'abord provisionner les ressources du CDK AWS requises. Pour plus d'informations, consultez la section	Développeur d’applications

Tâche	Description	Compétences requises
	Bootstrapping dans le guide du développeur AWS CDK v2.	

Déployez la pile AWS CDK sur votre compte AWS.	1. Créez une image de conteneur en exécutant la commande AWS CLI suivante :
	`docker build -t go-fargate .`
	2. Ouvrez le répertoire AWS CDK en exécutant la commande suivante :
	`cd cdk`
	3. Installez les modules npm requis en exécutant la commande suivante :
	`npm i`
	4. Déployez le modèle AWS CDK sur votre compte AWS en exécutant la commande suivante :
	`cdk deploy --profile ${AWS_PROFILE}`
		Développeur d'applications

Tester la configuration

Tâche	Description	Compétences requises
Envoyez un message de test à la file d'attente Amazon SQS.	Pour obtenir des instructi ons, consultez la section	Développeur d'applications

Tâche	Description	Compétences requises
	Envoyer des messages à une file d'attente (console) dans le manuel Amazon SQS Developer Guide. Exemple de message de test Amazon SQS `{ "message": "hello, Fargate" }`	
Vérifiez que le message de test apparaît dans les journaux du service Fargate. CloudWatch	Suivez les instructions de la section Visualisation CloudWatch des journaux du manuel Amazon ECS Developer Guide. Assurez-vous de consulter les journaux du groupe de go-fargate-servicejournaux dans le cluster go-service-clusterECS.	Développeur d'applications

Tâche	Description	Compétences requises
Vérifiez que le message de test apparaît dans le tableau DynamoDB.	1. Ouvrez la console DynamoDB. 2. Dans le volet de navigation de gauche, choisissez Tables. Sélectionnez ensuite le tableau suivant dans la liste : sqs-fargate-ddb-table. 3. Sélectionnez Explore table items (Explorer les éléments de la table). 4. Vérifiez que le message de test apparaît dans la liste des articles renvoyés.	Développeur d'applications

Tâche	Description	Compétences requises
Vérifiez que le service Fargate envoie des messages à Logs. CloudWatch	1. Ouvrez la CloudWatch console. 2. Dans le volet de navigation de gauche, sélectionnez Tableaux de bord. 3. Dans la liste des tableaux de bord personnalisés, sélectionnez le tableau de bord nommé go-service-dashboard. 4. Vérifiez que le message de test apparaît dans les journaux. **Note** Le CDK AWS crée automatiquement le CloudWatch tableau de bord dans votre compte AWS.	Développeur d'applications

Nettoyage

Tâche	Description	Compétences requises
Supprimez la pile AWS CDK.	1. Ouvrez votre répertoire AWS CDK dans la CLI AWS en exécutant la commande suivante : `cd cdk`	Développeur d'applications

Tâche	Description	Compétences requises
	2. Supprimez la pile AWS CDK en exécutant la commande suivante : `cdk destroy --profile ${AWS_PROFILE}`	
Vérifiez que la pile AWS CDK est supprimée.	Pour vous assurer que la pile a été supprimée, exécutez la commande suivante : `aws cloudformation list-stacks --query \ "StackSummaries[?contains(StackName,'SqsFargate')].StackStatus" \ --profile ${AWS_PROFILE}` La `StackStatus` valeur renvoyée dans la sortie de commande correspond `DELETE_COMPLETE` à la suppression de la pile. Pour plus d'informations, consultez la section Exemples de commandes d'opérations de CloudFormation pile pour le AWS CLI et PowerShell dans le guide de CloudFormation l'utilisateur AWS.	Développeur d’applications

Ressources connexes

- Configuration de l'interface de ligne de commande AWS (Guide de l'utilisateur de l'interface de ligne de commande AWS pour la version 2)
- Référence d'API (référence d'API AWS CDK)
- SDK AWS pour Go v2 (documentation Go)

Exécutez des charges de travail dynamiques avec un stockage de données persistant en utilisant Amazon EFS sur Amazon EKS avec AWS Fargate

Créée par Ricardo Morais (AWS), Rodrigo Bersa (AWS) et Lucio Pereira (AWS)

Récapitulatif

Ce modèle fournit des conseils pour activer Amazon Elastic File System (Amazon EFS) en tant que périphérique de stockage pour les conteneurs exécutés sur Amazon Elastic Kubernetes Service (Amazon EKS) en utilisant AWS Fargate pour provisionner vos ressources informatiques.

La configuration décrite dans ce modèle suit les meilleures pratiques en matière de sécurité et assure la sécurité au repos et la sécurité en transit par défaut. Pour chiffrer votre système de fichiers Amazon EFS, celui-ci utilise une clé AWS Key Management Service (AWS KMS), mais vous pouvez également spécifier un alias de clé qui gère le processus de création d'une clé KMS.

Vous pouvez suivre les étapes de ce modèle pour créer un espace de noms et un profil Fargate pour proof-of-concept une application (PoC), installer le pilote Amazon EFS Container Storage Interface (CSI) utilisé pour intégrer le cluster Kubernetes à Amazon EFS, configurer la classe de stockage et déployer l'application PoC. Ces étapes aboutissent à un système de fichiers Amazon EFS partagé entre plusieurs charges de travail Kubernetes et exécuté sur Fargate. Le modèle est accompagné de scripts qui automatisent ces étapes.

Vous pouvez utiliser ce modèle si vous souhaitez conserver les données dans vos applications conteneurisées et éviter toute perte de données lors des opérations de dimensionnement. Par exemple :

- DevOps outils — Un scénario courant consiste à développer un outil d'intégration et de livraison continues (CI/CD) strategy. In this case, you can use Amazon EFS as a shared file system to store configurations among different instances of the CI/CD tool or to store a cache (for example, an Apache Maven repository) for pipeline stages among different instances of the CI/CDoutil).
- Serveurs Web — Un scénario courant consiste à utiliser Apache comme serveur Web HTTP. Vous pouvez utiliser Amazon EFS en tant que système de fichiers partagé pour stocker des fichiers statiques partagés entre différentes instances du serveur Web. Dans cet exemple de scénario, les modifications sont appliquées directement au système de fichiers au lieu d'intégrer des fichiers statiques dans une image Docker.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cluster Amazon EKS existant avec Kubernetes version 1.17 ou ultérieure (testé jusqu'à la version 1.27)
- Un système de fichiers Amazon EFS existant pour lier un Kubernetes StorageClass et approvisionner des systèmes de fichiers de manière dynamique
- Autorisations d'administration du cluster
- Contexte configuré pour pointer vers le cluster Amazon EKS souhaité

Limites

- Certaines limites doivent être prises en compte lorsque vous utilisez Amazon EKS avec Fargate. Par exemple, l'utilisation de certaines constructions Kubernetes, telles que les conteneurs privilégiés, n'est DaemonSets pas prise en charge. Pour plus d'informations sur les limites de Fargate, consultez les considérations relatives à AWS Fargate dans la documentation Amazon EKS.
- Le code fourni avec ce modèle prend en charge les postes de travail qui exécutent Linux ou macOS.

Versions du produit

- Interface de ligne de commande AWS (AWS CLI) version 2 ou ultérieure
- pilote Amazon EFS CSI version 1.0 ou ultérieure (testé jusqu'à la version 2.4.8)
- eksctl version 0.24.0 ou ultérieure (testé jusqu'à la version 0.158.0)
- jq version 1.6 ou ultérieure
- kubectl version 1.17 ou ultérieure (testé jusqu'à la version 1.27)
- Kubernetes version 1.17 ou ultérieure (testé jusqu'à la version 1.27)

Architecture

L'architecture cible comprend l'infrastructure suivante :

- Un cloud privé virtuel (VPC)
- Deux zones de disponibilité
- Un sous-réseau public avec une passerelle NAT qui fournit un accès à Internet
- Un sous-réseau privé avec un cluster Amazon EKS et des cibles de montage Amazon EFS (également appelées points de montage)
- Amazon EFS au niveau du VPC

L'infrastructure environnementale du cluster Amazon EKS est la suivante :

- Profils AWS Fargate adaptés aux constructions Kubernetes au niveau de l'espace de noms
- Un espace de noms Kubernetes avec :
  - Deux modules d'applications répartis dans les zones de disponibilité
  - Une réclamation de volume persistant (PVC) liée à un volume persistant (PV) au niveau du cluster
- Un PV à l'échelle du cluster qui est lié au PVC dans l'espace de noms et qui pointe vers les cibles de montage Amazon EFS dans le sous-réseau privé, en dehors du cluster

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source que vous pouvez utiliser pour interagir avec les services AWS depuis la ligne de commande.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS. Dans ce modèle, il fournit un système de fichiers simple, évolutif, entièrement géré et partagé à utiliser avec Amazon EKS.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter Kubernetes sur AWS sans avoir à installer ou à exploiter vos propres clusters.
- AWS Fargate est un moteur de calcul sans serveur pour Amazon EKS. Il crée et gère les ressources de calcul pour vos applications Kubernetes.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- eksctl est un utilitaire de ligne de commande permettant de créer et de gérer des clusters Kubernetes sur Amazon EKS.
- kubectl est une interface de ligne de commande qui vous permet d'exécuter des commandes sur des clusters Kubernetes.
- jq est un outil en ligne de commande pour analyser le JSON.

Code

Le code de ce modèle est fourni dans la configuration de GitHub persistance avec Amazon EFS sur Amazon EKS à l'aide du référentiel AWS Fargate. Les scripts sont organisés par épopée, dans les dossiers `epic01` suivants`epic06`, conformément à l'ordre indiqué dans la section Epics de ce modèle.

Bonnes pratiques

L'architecture cible inclut les services et composants suivants, et elle suit les meilleures pratiques d'AWS Well-Architected Framework :

- Amazon EFS, qui fournit un système de fichiers NFS élastique simple, évolutif et entièrement géré. Il est utilisé comme système de fichiers partagé entre toutes les réplications de l'application PoC exécutées dans des pods, qui sont distribués dans les sous-réseaux privés du cluster Amazon EKS choisi.
- Une cible de montage Amazon EFS pour chaque sous-réseau privé. Cela fournit une redondance par zone de disponibilité au sein du cloud privé virtuel (VPC) du cluster.
- Amazon EKS, qui exécute les charges de travail Kubernetes. Vous devez provisionner un cluster Amazon EKS avant d'utiliser ce modèle, comme décrit dans la section Conditions préalables.
- AWS KMS, qui fournit un chiffrement au repos pour le contenu stocké dans le système de fichiers Amazon EFS.
- Fargate, qui gère les ressources de calcul des conteneurs afin que vous puissiez vous concentrer sur les exigences de l'entreprise plutôt que sur la charge de l'infrastructure. Le profil Fargate est créé pour tous les sous-réseaux privés. Il fournit une redondance par zone de disponibilité au sein du cloud privé virtuel (VPC) du cluster.
- Kubernetes Pods, pour valider que le contenu peut être partagé, consommé et écrit par différentes instances d'une application.

Épopées

Provisionner un cluster Amazon EKS (facultatif)

Tâche	Description	Compétences requises
Créez un cluster Amazon EKS.	**Note** Si vous avez déjà déployé un cluster, passez à l'épopée suivante. Créez un cluster Amazon EKS dans votre compte AWS existant. Dans le GitHub répertoire, utilisez l'un des modèles pour déployer un cluster Amazon EKS à l'aide de Terraform ou eksctl. Pour plus d'informations, consultez la section Création d'un cluster Amazon EKS dans la documentation Amazon EKS. Le modèle Terraform contient également des exemples montrant comment : lier des profils Fargate à votre cluster Amazon EKS, créer un système de fichiers Amazon EFS et déployer le pilote	Administrateur AWS, administrateur Terraform ou eksctl, administrateur Kubernetes

Tâche	Description	Compétences requises
	Amazon EFS CSI dans votre cluster Amazon EKS.	

Tâche	Description	Compétences requises

Exportez les variables d'environnement.	Exécutez le script env.sh. Cela fournit les informations requises lors des prochaines étapes.
	`source ./scripts/env.sh`
	`Inform the AWS Account ID: <13-digit-account-id>`
	`Inform your AWS Region: <aws-Region-code>`
	`Inform your Amazon EKS Cluster Name: <amazon-eks-cluster-name>`
	`Inform the Amazon EFS Creation Token: <self-genereated-uuid>`
	Si ce n'est pas encore le cas, vous pouvez obtenir toutes les informations demandées ci-dessus à l'aide des commandes CLI suivantes .
	`# ACCOUNT ID`
	`aws sts get-calle r-identity --query "Account" --output text`
	`# REGION CODE`
	`aws configure get region`
	`# CLUSTER EKS NAME`
		Administrateur système AWS

Tâche	Description	Compétences requises

	`aws eks list-clusters --query "clusters" --output text`
	
	`# GENERATE EFS TOKEN uuidgen`	

Création d'un espace de noms Kubernetes et d'un profil Fargate lié

Tâche	Description	Compétences requises
Créez un espace de noms Kubernetes et un profil Fargate pour les charges de travail des applications.	Créez un espace de noms pour recevoir les charges de travail des applications qui interagissent avec Amazon EFS. Exécutez le script `create-k8s-ns-and-linked-fargate-profile.sh` . Vous pouvez choisir d'utiliser un nom d'espace de noms personnalisé ou l'espace de noms `poc-efs-eks-fargate` fourni par défaut. Avec un nom d'espace de noms d'application personnalisé : `export $APP_NAMESPACE=<CUSTOM_NAME> ./scripts/epic01/create-k8s-ns-and-linked-fargate-profile.sh \`	Utilisateur Kubernetes disposant d'autorisations accordées

Tâche	Description	Compétences requises

	`-c "$CLUSTER_NAME" -n "$APP_NAMESPACE"`
	
	Sans nom d'espace de noms d'application personnalisé :
	
	`./scripts/epic01/create-k8s-ns-and-linked-fargate-profile.sh \ -c "$CLUSTER_NAME"`
	
	où `$CLUSTER_NAME` est le nom de votre cluster Amazon EKS. Le `-n <NAMESPACE>` paramètre est facultatif ; si vous n'en êtes pas informé, un nom d'espace de noms généré par défaut sera fourni.	

Créer un système de fichiers Amazon EFS

Tâche	Description	Compétences requises
Générez un jeton unique.	Amazon EFS nécessite un jeton de création pour garantir un fonctionnement idempotent (appeler l'opération avec le même jeton de création n'a aucun effet). Pour répondre à cette exigence, vous devez générer un jeton unique à l'aide d'une technique disponible. Par exemple, vous pouvez générer un identifia	Administrateur système AWS

Tâche	Description	Compétences requises
	nt unique universel (UUID) à utiliser comme jeton de création.	

Tâche	Description	Compétences requises
Créez un système de fichiers Amazon EFS.	Créez le système de fichiers pour recevoir les fichiers de données lus et écrits par les charges de travail de l'application. Vous pouvez créer un système de fichiers chiffré ou non chiffré. (Il est recommandé que le code de ce modèle crée un système crypté pour activer le chiffrement au repos par défaut.) Vous pouvez utiliser une clé AWS KMS unique et symétrique pour chiffrer votre système de fichiers. Si aucune clé personnalisée n'est spécifiée, une clé gérée par AWS est utilisée. Utilisez le script create-efs.sh pour créer un système de fichiers Amazon EFS chiffré ou non chiffré, après avoir généré un jeton unique pour Amazon EFS. Avec le chiffrement au repos, sans clé KMS : `./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"`	Administrateur système AWS

Tâche	Description	Compétences requises

	où `$CLUSTER_NAME` est le nom de votre cluster Amazon EKS et `$EFS_CREATION_TOKEN` est un jeton de création unique pour le système de fichiers.
	
	Avec le chiffrement au repos, avec une clé KMS :
	
	`./scripts/epic02/create-efs.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"`
	
	où `$CLUSTER_NAME` est le nom de votre cluster Amazon EKS, `$EFS_CREATION_TOKEN` est un jeton de création unique pour le système de fichiers et `$KMS_KEY_ALIAS` est l'alias de la clé KMS.
	
	Sans cryptage :
	
	`./scripts/epic02/create-efs.sh -d \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"`	

Tâche	Description	Compétences requises
	où `$CLUSTER_NAME` est le nom de votre cluster Amazon EKS, `$EFS_CREATION_TOKEN` est un jeton de création unique pour le système de fichiers et `–d` désactive le chiffrement au repos.	
Créez un groupe de sécurité.	Créez un groupe de sécurité pour autoriser le cluster Amazon EKS à accéder au système de fichiers Amazon EFS.	Administrateur système AWS
Mettez à jour la règle de trafic entrant pour le groupe de sécurité.	Mettez à jour les règles entrantes du groupe de sécurité pour autoriser le trafic entrant pour les paramètres suivants : • Protocole TCP — port 2049 • Source : plages de blocs CIDR pour les sous-réseaux privés du VPC contenant le cluster Kubernetes	Administrateur système AWS
Ajoutez une cible de montage pour chaque sous-réseau privé.	Pour chaque sous-réseau privé du cluster Kubernetes, créez une cible de montage pour le système de fichiers et le groupe de sécurité.	Administrateur système AWS

Installation des composants Amazon EFS dans le cluster Kubernetes

Tâche	Description	Compétences requises
Déployez le pilote Amazon EFS CSI.	Déployez le pilote Amazon EFS CSI dans le cluster. Le pilote provisionne le stockage en fonction des demandes de volume persistantes créées par les applications. Exécutez le `create-k8s-efs-csi-sc.sh` script pour déployer le pilote Amazon EFS CSI et la classe de stockage dans le cluster. `./scripts/epic03/create-k8s-efs-csi-sc.sh` Ce script utilise l'`kubectl`utilitaire. Assurez-vous donc que le contexte a été configuré et qu'il pointe vers le cluster Amazon EKS souhaité.	Utilisateur Kubernetes disposant d'autorisations accordées
Déployez la classe de stockage.	Déployez la classe de stockage dans le cluster pour le fournisseur Amazon EFS (efs.csi.aws.com).	Utilisateur Kubernetes disposant d'autorisations accordées

Installez l'application PoC dans le cluster Kubernetes

Tâche	Description	Compétences requises
Déployez le volume persistant.	Déployez le volume persistant et liez-le à la classe de stockage créée et à l'ID du système de fichiers Amazon EFS. L'application utilise le volume persistant pour lire et écrire du contenu. Vous pouvez spécifier n'importe quelle taille pour le volume persistant dans le champ de stockage. Kubernetes requiert ce champ, mais Amazon EFS étant un système de fichiers élastique, il n'impose aucune capacité du système de fichiers. Vous pouvez déployer le volume persistant avec ou sans chiffrement. (Le pilote Amazon EFS CSI active le chiffrement par défaut, conformément à la meilleure pratique.) Exécutez le `deploy-poc-app.sh` script pour déployer le volume persistant, la demande de volume persistant et les deux charges de travail. Avec le chiffrement en transit : `./scripts/epic04/deploy-poc-app.sh \`	Utilisateur Kubernetes disposant d'autorisations accordées

Tâche	Description	Compétences requises

	`-t "$EFS_CREATION_TOKEN"`
	
	où `$EFS_CREATION_TOKEN` est le jeton de création unique pour le système de fichiers.
	
	Sans chiffrement pendant le transport :
	
	`./scripts/epic04/deploy-poc-app.sh -d \ -t "$EFS_CREATION_TOKEN"`
	
	où se `$EFS_CREATION_TOKEN` trouve le jeton de création unique pour le système de fichiers et `-d` désactive le chiffrement en transit.	

Tâche	Description	Compétences requises
Déployez la réclamation de volume persistante demandée par l'application.	Déployez la demande de volume persistant demandée par l'application et liez-la à la classe de stockage. Utilisez le même mode d'accès que le volume persistant que vous avez créé précédemm ent. Vous pouvez spécifier n'importe quelle taille pour la réclamation de volume persistant dans le champ de stockage. Kubernetes requiert ce champ, mais Amazon EFS étant un système de fichiers élastique, il n'impose aucune capacité du système de fichiers.	Utilisateur Kubernetes disposant d'autorisations accordées
Déployer la charge de travail 1.	Déployez le pod qui représent e la charge de travail 1 de l'application. Cette charge de travail écrit du contenu dans le fichier`/data/out1.txt` .	Utilisateur Kubernetes disposant d'autorisations accordées
Déployer la charge de travail 2.	Déployez le pod qui représent e la charge de travail 2 de l'application. Cette charge de travail écrit du contenu dans le fichier`/data/out2.txt` .	Utilisateur Kubernetes disposant d'autorisations accordées

Validation de la persistance, de la durabilité et de la capacité de partage du système de fichiers

Tâche	Description	Compétences requises
Vérifiez l'état du`PersistentVolume` .	Entrez la commande suivante pour vérifier l'état du`PersistentVolume` . `kubectl get pv` Pour un exemple de sortie, consultez la section Informations supplémentaires.	Utilisateur Kubernetes disposant d'autorisations accordées
Vérifiez l'état du`PersistentVolumeClaim` .	Entrez la commande suivante pour vérifier l'état du`PersistentVolumeClaim` . `kubectl -n poc-efs-eks-fargate get pvc` Pour un exemple de sortie, consultez la section Informations supplémentaires.	Utilisateur Kubernetes disposant d'autorisations accordées
Vérifiez que la charge de travail 1 peut écrire dans le système de fichiers.	Entrez la commande suivante pour vérifier que le workload 1 écrit sur`/data/out1.txt` . `kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -f /data/out1.txt` Les résultats sont similaires aux suivants :	Utilisateur Kubernetes disposant d'autorisations accordées

Tâche	Description	Compétences requises
	``` ... Thu Sep 3 15:25:07 UTC 2023 - PoC APP 1 Thu Sep 3 15:25:12 UTC 2023 - PoC APP 1 Thu Sep 3 15:25:17 UTC 2023 - PoC APP 1 ... ```	
Vérifiez que la charge de travail 2 peut écrire dans le système de fichiers.	Entrez la commande suivante pour vérifier que la charge de travail 2 écrit sur `/data/out 2.txt` . ``` kubectl -n $APP_NAME SPACE exec -ti poc-app2 -- tail -f /data/out 2.txt ``` Les résultats sont similaires aux suivants : ``` ... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ... ```	Utilisateur Kubernetes disposant d'autorisations accordées

Tâche	Description	Compétences requises

Vérifiez que la charge de travail 1 peut lire le fichier écrit par la charge de travail 2.	Entrez la commande suivante pour vérifier que la charge de travail 1 peut lire le `/data/out2.txt` fichier écrit par la charge de travail 2.
	`kubectl exec -ti poc-app1 -n poc-efs-eks-fargate -- tail -n 3 /data/out2.txt`
	Les résultats sont similaires aux suivants :
	`... Thu Sep 3 15:26:48 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:53 UTC 2023 - PoC APP 2 Thu Sep 3 15:26:58 UTC 2023 - PoC APP 2 ...`
		Utilisateur Kubernetes disposant d'autorisations accordées

Tâche	Description	Compétences requises

Vérifiez que la charge de travail 2 peut lire le fichier écrit par la charge de travail 1.	Entrez la commande suivante pour vérifier que la charge de travail 2 peut lire le `/data/out1.txt` fichier écrit par la charge de travail 1.
	`kubectl -n $APP_NAMESPACE exec -ti poc-app2 -- tail -n 3 /data/out1.txt`
	Les résultats sont similaires aux suivants :
	`... Thu Sep 3 15:29:22 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:27 UTC 2023 - PoC APP 1 Thu Sep 3 15:29:32 UTC 2023 - PoC APP 1 ...`
		Utilisateur Kubernetes disposant d'autorisations accordées

Tâche	Description	Compétences requises

Vérifiez que les fichiers sont conservés après avoir supprimé les composants de l'application.	Ensuite, vous utilisez un script pour supprimer les composants de l'application (volume persistant, réclamation de volume persistant et pods) et pour vérifier que les fichiers `/data/out1.txt` `/data/out2.txt` sont conservés dans le système de fichiers. Exécutez le script `validate-efs-content.sh` à l'aide de la commande suivante.
	`./scripts/epic05/validate-efs-content.sh \`
	`-t "$EFS_CREATION_TOKEN"`
	où `$EFS_CREATION_TOKEN` est le jeton de création unique pour le système de fichiers.
	Les résultats sont similaires aux suivants :
	`pod/poc-app-validation created`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
	`Waiting for pod get Running state...`
	`Results from execution of 'find /data' on`
		Utilisateur Kubernetes avec autorisations accordées, administrateur système

Tâche	Description	Compétences requises
	validation process pod: /data /data/out2.txt /data/out1.txt	

Surveiller les opérations

Tâche	Description	Compétences requises
Surveillez les journaux des applications.	Dans le cadre d'une opération du deuxième jour, envoyez les journaux des applications à Amazon CloudWatch pour qu'ils soient surveillés.	Administrateur système AWS, utilisateur de Kubernetes avec autorisations accordées
Surveillez les conteneurs Amazon EKS et Kubernetes avec Container Insights.	Dans le cadre d'une opération de deux jours, surveillez les systèmes Amazon EKS et Kubernetes à l'aide d'Amazon Container Insights. CloudWatch Cet outil collecte, agrège et résume les métriques des applications conteneurisées à différents niveaux et dimensions. Pour plus d'informations, consultez la section Ressources connexes.	Administrateur système AWS, utilisateur de Kubernetes avec autorisations accordées
Surveillez Amazon EFS avec CloudWatch.	Dans le cadre d'une opération de deux jours, surveillez les systèmes de fichiers à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes d'Amazon EFS pour en	Administrateur système AWS

Tâche	Description	Compétences requises
	faire des métriques lisibles en temps quasi réel. Pour plus d'informations, consultez la section Ressources connexes.	

Nettoyage des ressources

Tâche	Description	Compétences requises
Nettoyez toutes les ressources créées pour le modèle.	Une fois ce schéma terminé, nettoyez toutes les ressources afin d'éviter d'avoir à payer des frais AWS. Exécutez le `clean-up-resources.sh` script pour supprimer toutes les ressources une fois que vous avez fini d'utiliser l'application PoC. Complétez l'une des options suivantes. Avec le chiffrement au repos, avec une clé KMS : `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN" \ -k "$KMS_KEY_ALIAS"` où `$CLUSTER_NAME` est le nom de votre cluster Amazon EKS, `$EFS_CREATION_TOKEN` le jeton	Utilisateur Kubernetes avec autorisations accordées, administrateur système

Tâche	Description	Compétences requises
	de création du système de fichiers et `$KMS_KEY_ALIAS` l'alias de la clé KMS. Sans chiffrement au repos : `./scripts/epic06/clean-up-resources.sh \ -c "$CLUSTER_NAME" \ -t "$EFS_CREATION_TOKEN"` où `$CLUSTER_NAME` est le nom de votre cluster Amazon EKS et `$EFS_CREATION_TOKEN` le jeton de création du système de fichiers.	

Ressources connexes

Références

- AWS Fargate pour Amazon EKS est désormais compatible avec Amazon EFS (annonce)
- Comment capturer les journaux d'applications lors de l'utilisation d'Amazon EKS sur AWS Fargate (article de blog)
- Utilisation de Container Insights (CloudWatch documentation Amazon)
- Configuration de Container Insights sur Amazon EKS et Kubernetes (documentation Amazon) CloudWatch
- Métriques Amazon EKS et Kubernetes Container Insights (documentation Amazon) CloudWatch
- Surveillance d'Amazon EFS avec Amazon CloudWatch (documentation Amazon EFS)

GitHub tutoriels et exemples

- Provisionnement statique
- Chiffrement en transit
- Accès au système de fichiers à partir de plusieurs modules
- Utilisation d'Amazon EFS dans StatefulSets
- Sous-chemins de montage
- Utilisation des points d'accès Amazon EFS
- Blueprints Amazon EKS pour Terraform

Outils nécessaires

- Installation de la version 2 de l'interface de ligne de commande AWS
- Installation d'eksctl
- Installation de kubectl
- Installation de jq

Informations supplémentaires

Voici un exemple de sortie de la `kubectl get pv` commande.

```
NAME         CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM
            STORAGECLASS   REASON   AGE
poc-app-pv   1Mi        RWX            Retain           Bound    poc-efs-eks-fargate/
poc-app-pvc   efs-sc                  3m56s
```

Voici un exemple de sortie de la `kubectl -n poc-efs-eks-fargate get pvc` commande.

```
NAME          STATUS   VOLUME       CAPACITY   ACCESS MODES   STORAGECLASS   AGE
poc-app-pvc   Bound    poc-app-pv   1Mi        RWX            efs-sc         4m34s
```

Configurez le dimensionnement automatique piloté par les événements dans Amazon EKS à l'aide d'Amazon EKS Pod Identity et KEDA

Créée par Dipen Desai (AWS), Abhay Diwan (AWS), Kamal Joshi (AWS) et Mahendra asiddappa (AWS)

Récapitulatif

Les plateformes d'orchestration, telles qu'Amazon Elastic Kubernetes Service (Amazon EKS), ont rationalisé la gestion du cycle de vie des applications basées sur des conteneurs. Cela permet aux entreprises de se concentrer sur le développement, la sécurisation, l'exploitation et la maintenance d'applications basées sur des conteneurs. Les déploiements pilotés par des événements devenant de plus en plus courants, les entreprises adaptent de plus en plus fréquemment les déploiements Kubernetes en fonction de diverses sources d'événements. Cette méthode, associée à la mise à l'échelle automatique, peut permettre de réaliser d'importantes économies en fournissant des ressources de calcul à la demande et une mise à l'échelle efficace adaptée à la logique des applications.

KEDA est un autoscaler piloté par les événements basé sur Kubernetes. KEDA vous aide à dimensionner n'importe quel conteneur dans Kubernetes en fonction du nombre d'événements à traiter. Il est léger et s'intègre à n'importe quel cluster Kubernetes. Il fonctionne également avec les composants standard de Kubernetes, tels que Horizontal Pod Autoscaling (HPA). KEDA propose TriggerAuthenticationégalement une fonctionnalité qui vous permet de déléguer l'authentification. Il vous permet de décrire des paramètres d'authentification distincts des conteneurs ScaledObject et des conteneurs de déploiement.

AWS fournit des rôles AWS Identity and Access Management (IAM) qui prennent en charge diverses options de déploiement de Kubernetes, notamment Amazon EKS, Amazon EKS Anywhere Red Hat OpenShift Service on AWS (ROSA), et des clusters Kubernetes autogérés sur Amazon Elastic Compute Cloud (Amazon). EC2 Ces rôles utilisent des structures IAM, telles que les fournisseurs d'identité OpenID Connect (OIDC) et les politiques de confiance IAM, pour fonctionner dans différents environnements sans s'appuyer directement sur les services Amazon EKS ou. APIs Pour plus d'informations, consultez les rôles IAM pour les comptes de service dans la documentation Amazon EKS.

Amazon EKS Pod Identity simplifie le processus permettant aux comptes de service Kubernetes d'assumer des rôles IAM sans avoir besoin de fournisseurs OIDC. Il permet de gérer les informations d'identification de vos applications. Au lieu de créer et de distribuer vos AWS informations

d'identification aux conteneurs ou d'utiliser le rôle de l' EC2 instance Amazon, vous associez un rôle IAM à un compte de service Kubernetes et configurez vos Pods pour utiliser le compte de service. Cela vous permet d'utiliser un rôle IAM sur plusieurs clusters et simplifie la gestion des politiques en permettant la réutilisation des politiques d'autorisation entre les rôles IAM.

En implémentant KEDA avec Amazon EKS Pod Identity, les entreprises peuvent bénéficier d'une mise à l'échelle automatique efficace axée sur les événements et d'une gestion simplifiée des informations d'identification. Les applications évoluent en fonction de la demande, ce qui optimise l'utilisation des ressources et réduit les coûts.

Ce modèle vous permet d'intégrer Amazon EKS Pod Identity à KEDA. Il montre comment vous pouvez utiliser le compte de `keda-operator` service et déléguer l'authentification avec`TriggerAuthentication`. Il décrit également comment établir une relation de confiance entre un rôle IAM pour l'opérateur KEDA et un rôle IAM pour l'application. Cette relation de confiance permet à KEDA de surveiller les messages dans les files d'attente d'événements et d'ajuster le dimensionnement pour les objets Kubernetes de destination.

Conditions préalables et limitations

Prérequis

- AWS Command Line Interface (AWS CLI) version 2.13.17 ou ultérieure, installée
- Python version 3.11.5 ou ultérieure, installée
- AWS SDK pour Python (Boto3) version 1.34.135 ou ultérieure, installée
- Helm version 3.12.3 ou ultérieure, installée
- kubectl version 1.25.1 ou ultérieure, installée
- Docker Engine version 26.1.1 ou ultérieure, installé
- Un cluster Amazon EKS version 1.24 ou ultérieure, créé
- Conditions préalables à la création de l'agent Amazon EKS Pod Identity, remplies

Limites

- Vous devez établir une relation de confiance entre le `keda-operator` rôle et le `keda-identity` rôle. Les instructions sont fournies dans la section Epics de ce modèle.

Architecture

Dans ce modèle, vous créez les AWS ressources suivantes :

- Référentiel Amazon Elastic Container Registry (Amazon ECR) — Dans ce modèle, ce dépôt est nommé. `keda-pod-identity-registry` Ce dépôt privé est utilisé pour stocker des images Docker de l'exemple d'application.
- File d'attente Amazon Simple Queue Service (Amazon SQS) — Dans ce modèle, cette file d'attente est nommée. `event-messages-queue` La file d'attente agit comme un tampon de messages qui collecte et stocke les messages entrants. KEDA surveille les métriques de file d'attente, telles que le nombre de messages ou la longueur de la file d'attente, et adapte automatiquement l'application en fonction de ces métriques.
- Rôle IAM pour l'application : dans ce modèle, ce rôle est nommé`keda-identity`. Le `keda-operator` rôle assume ce rôle. Ce rôle permet d'accéder à la file d'attente Amazon SQS.
- Rôle IAM pour l'opérateur KEDA — Dans ce modèle, ce rôle est nommé. `keda-operator` L'opérateur KEDA utilise ce rôle pour effectuer les appels d' AWS API requis. Ce rôle est autorisé à assumer ce `keda-identity` rôle. En raison de la relation de confiance entre les `keda-identity` rôles `keda-operator` et, le `keda-operator` rôle dispose des autorisations Amazon SQS.

Par le biais des ressources personnalisées `TriggerAuthentication` et de `ScaledObject` Kubernetes, l'opérateur utilise le `keda-identity` rôle pour se connecter à une file d'attente Amazon SQS. En fonction de la taille de la file d'attente, KEDA adapte automatiquement le déploiement de l'application. Il ajoute 1 pod pour 5 messages non lus dans la file d'attente. Dans la configuration par défaut, s'il n'y a aucun message non lu dans la file d'attente Amazon SQS, l'application est réduite à 0 pods. L'opérateur KEDA surveille la file d'attente à un intervalle que vous spécifiez.

L'image suivante montre comment utiliser Amazon EKS Pod Identity pour fournir au `keda-operator` rôle un accès sécurisé à la file d'attente Amazon SQS.

Le schéma suivant illustre le flux de travail suivant :

1. Vous installez l'agent Amazon EKS Pod Identity dans le cluster Amazon EKS.
2. Vous déployez l'opérateur KEDA dans l'espace de noms KEDA du cluster Amazon EKS.

3. Vous créez les rôles `keda-operator` et `keda-identity` IAM dans la cible Compte AWS.
4. Vous établissez une relation de confiance entre les rôles IAM.
5. Vous déployez l'application dans l'espace de `security` noms.
6. L'opérateur KEDA interroge les messages dans une file d'attente Amazon SQS.
7. KEDA lance le HPA, qui redimensionne automatiquement l'application en fonction de la taille de la file d'attente.

Outils

Services AWS

- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

Autres outils

- KEDA est un autoscaler piloté par les événements basé sur Kubernetes.

Référentiel de code

Le code de ce modèle est disponible dans le dimensionnement GitHub automatique piloté par les événements à l'aide d'EKS Pod Identity et du référentiel KEDA.

Bonnes pratiques

Nous vous recommandons de respecter les bonnes pratiques ci-dessous :

- Bonnes pratiques d'Amazon EKS
- Bonnes pratiques de sécurité dans IAM

- Bonnes pratiques relatives à Amazon SQS

Épopées

Créez des AWS ressources

Tâche	Description	Compétences requises
Créez le rôle IAM pour l'opérateur KEDA.	1. Connectez-vous à la console IAM AWS Management Console, puis ouvrez-la. 2. Dans le panneau de navigation, choisissez Roles (Rôles). 3. Sélectionnez Create role (Créer un rôle). 4. Choisissez le type de rôle Custom trust policy (Politique d'approbation personnalisée). 5. Dans la section Politique de confiance personnalisée, entrez la politique de confiance personnalisée suivante pour ce rôle : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`	Administrateur AWS

Tâche	Description	Compétences requises

	<pre>"Service": "pods.eks.amazonaws.com"
	},
	"Action":
	[
	"sts:AssumeRole",
	"sts:TagSession"
	]
	}
	]
	}</pre>
	6. Sur la page Ajouter des autorisations, sélectionnez Suivant. Vous n'ajoutez aucune politique à ce rôle.
	7. Pour le Nom du rôle, saisissez `keda-operator` .
	8. Choisissez Créer un rôle.	

Tâche	Description	Compétences requises
Créez le rôle IAM pour l'exemple d'application.	1. Dans la console IAM, dans le volet de navigation, sélectionnez Rôles. 2. Choisissez Créer un rôle. 3. Choisissez le type de rôle Custom trust policy (Politique d'approbation personnalisée). 4. Dans la section Politique de confiance personnalisée, entrez la politique de confiance personnalisée suivante pour ce rôle. Remplacez `<account number>` par votre numéro de compte cible : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "pods.eks.amazonaws.com", "AWS": "arn:aws:iam::<account number>:role/keda-operator" }, "Action": [`	Administrateur AWS

Tâche	Description	Compétences requises

	<pre>"sts:AssumeRole",
	
	"sts:TagSession"
	]
	}
	]
	}</pre>
	5. Sur la page Ajouter des autorisations, ajoutez les politiques AWS gérées suivantes au rôle :
	• `AmazonSQSReadOnlyAccess`
	• `AWSLambdaSQSQueueExecutionRole`
	6. Choisissez Suivant.
	7. Pour le Nom du rôle, saisissez `keda-identity` .
	8. Choisissez Créer un rôle.	

Tâche	Description	Compétences requises
Créez une file d'attente Amazon SQS.	1. Ouvrez la console Amazon SQS. 2. Choisissez Créez une file d'attente. 3. Pour Type, choisissez Standard. 4. Sur la page Créer une file d'attente, pour Nom, entrez`event-messages-queue` . 5. Choisissez Créez une file d'attente. Vous ne modifiez aucun des paramètres par défaut de cette file d'attente .	AWS général
Créez un référentiel Amazon ECR.	1. Ouvrez la console Amazon ECR. 2. Choisissez Créer un référentiel. 3. Dans Nom du référentiel, entrez`keda-pod-identity-registry` . 4. Choisissez Créer un référentiel. Vous ne modifiez aucun des paramètres par défaut de ce référentiel.	AWS général

Configuration du cluster Amazon EKS

Tâche	Description	Compétences requises
Déployez l'agent Amazon EKS Pod Identity.	Pour le cluster Amazon EKS cible, configurez l'agent Amazon EKS Pod Identity. Suivez les instructions de la section Configurer l'agent d'identité Amazon EKS Pod dans la documentation Amazon EKS.	AWS DevOps

Déployez KEDA.	1. Entrez les commandes suivantes pour déployer KEDA sur le cluster Amazon EKS cible :
	`# Add Helm Repo for Keda`
	`helm repo add kedacore https://kedacore.github.io/charts`
	`# Update Helm repo`
	`helm repo update`
	`# Install Keda`
	`helm install keda kedacore/keda --namespace keda --create-namespace`
	Pour plus d'informations, consultez la section Déploiement avec Helm dans la documentation KEDA.
	2. Une fois le déploiement réussi, dans le résultat, validez que trois déploieme
		DevOps ingénieur

Tâche	Description	Compétences requises
	nts ont été créés pour l'opérateur KEDA. Voici un exemple de sortie : `NAME READY UP-TO-DATE AVAILABLE AGE keda-admission-webhooks 1/1 1 1 89s keda-operator 1/1 1 1 89s keda-operator-metrics-apiserver 1/1 1 1 89s`	
Attribuez le rôle IAM au compte de service Kubernetes.	Suivez les instructions de la section Attribuer un rôle IAM à un compte de service Kubernetes dans la documentation Amazon EKS. Utilisez les valeurs suivantes : • Pour le rôle IAM, entrez`keda-operator` . • Pour l'espace de noms Kubernetes, entrez. `keda` • Pour le compte de service Kubernetes, entrez. `keda-operator`	AWS DevOps

Tâche	Description	Compétences requises
Créez un espace de noms .	Entrez la commande suivante pour créer un espace de `security` noms dans le cluster Amazon EKS cible : `kubectl create ns security`	DevOps ingénieur

Déploiement de l'exemple d'application

Tâche	Description	Compétences requises
Clonez les fichiers de l'application.	Entrez la commande suivante pour cloner le dimensionnement automatique piloté par les événements à l'aide d'EKS Pod Identity et du référentiel KEDA à partir de : GitHub `git clone https://github.com/aws-samples/event-driven-autoscaling-using-podidentity-and-keda.git`	DevOps ingénieur
Développez l'image Docker.	1. Entrez la commande suivante pour accéder au référentiel cloné : `cd event-driven-autoscaling-using-podidentity-and-keda`	DevOps ingénieur

Tâche	Description	Compétences requises
	2. Entrez la commande suivante pour créer l'image Docker pour l'exemple d'application : `docker build -t keda-pod-identity-registry .`	

Tâche	Description	Compétences requises

Transférez l'image Docker vers Amazon ECR.	1. Dans le terminal où vous avez créé l'image Docker, entrez la commande suivante pour vous connecter à Amazon ECR. Remplacez <AWS_REGION> et <AWS_ACCOUNT_ID> par des valeurs issues de votre AWS environnement :
	`aws ecr get-login-password \ --region <AWS_REGION> | docker login \ --username AWS \ --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com`
	2. Entrez la commande suivante pour étiqueter l'image. Remplacez <AWS_REGION> et <AWS_ACCOUNT_ID> par des valeurs issues de votre AWS environnement :
	`docker tag keda-pod-identity-registry:latest <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-id`
		DevOps ingénieur

Tâche	Description	Compétences requises

	`entity-registry:latest`
	3. Entrez la commande suivante pour envoyer l'image vers Amazon ECR. Remplacez `<AWS_REGION>` et `<AWS_ACCOUNT_ID>` par des valeurs issues de votre AWS environnement :
	`docker push <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/keda-pod-identity-registry:latest`
	Note
	Vous pouvez trouver les commandes push en accédant à la page du référentiel Amazon ECR, puis en choisissant Afficher les commandes push.	

Tâche	Description	Compétences requises
Déployez un exemple d'application	1. Dans le référentiel cloné, ouvrez le fichier deploy.yaml. 2. Remplacez <AWS_ACCOUNT_ID> et <AWS_REGION> par des valeurs issues de votre environnement. 3. Enregistrez et fermez le fichier deploy.yaml. 4. Entrez la commande suivante pour déployer l'exemple d'application sur le cluster Amazon EKS cible : `kubectl apply -f deploy.yaml` Cette commande crée un compte de déploiement et de service dans le cluster.	DevOps ingénieur

Tâche	Description	Compétences requises

Attribuez le rôle IAM au compte du service d'application.	Procédez de l'une des manières suivantes pour associer le rôle `keda-identity` IAM au compte de service de l'exemple d'application :
	• Suivez les instructions de la section Attribuer un rôle IAM à un compte de service Kubernetes dans la documentation Amazon EKS. Utilisez les valeurs suivantes :
	  • Pour le rôle IAM, entrez`keda-identity` .
	  • Pour l'espace de noms Kubernetes, entrez. `security`
	  • Pour le compte de service Kubernetes, entrez. `my-sqs-read-msgs`
	• Entrez la AWS CLI commande suivante. Remplacez `<cluster-name>` par le nom du cluster Amazon EKS cible et remplacez `<role-ARN>` par le nom de ressource Amazon (ARN) du `keda-identity` rôle :
		DevOps ingénieur

Tâche	Description	Compétences requises
	`aws eks create-pod-identity-association \ --cluster-name <cluster-name> \ --role-arn <role-ARN> \ --namespace security \ --service-account my-sqs-read-msgs`	

Tâche	Description	Compétences requises
Déployez `ScaledObject` et`TriggerAuthentication` .	1. Dans le dépôt cloné, ouvrez le fichier keda.yaml. 2. Remplacez `{{AWS_ACCOUNT_ID}}` par l'identifiant de votre cible Compte AWS. 3. `{{AWS_REGION}}` Remplacez-le par votre cible Région AWS. 4. (Facultatif) Dans les lignes 21 à 24, mettez à jour les paramètres de la politique de `ScaledObject` dimensionnement. Consultez ce qui suit pour plus d'informations sur ces paramètres : • Intervalle de sondage • Période de refroidissement • idleReplicaCount • minReplicaCount 5. Enregistrez et fermez le fichier keda.yaml. 6. Entrez la commande suivante pour déployer les `TriggerAuthentication` ressources `ScaledObject` et : `kubectl -n security apply -f keda.yaml`	DevOps ingénieur

Testez la mise à l'échelle automatique

Tâche	Description	Compétences requises

Envoyez des messages à la file d'attente Amazon SQS.	1. Entrez la commande suivante pour accéder au référentiel cloné :
	`cd event-driven-autoscaling-using-podidentity-and-keda`
	2. Entrez la commande suivante pour envoyer des messages de test à la file d'attente Amazon SQS :
	`python sqs_send_msg.py`
	Le script sqs_send_msg.py agit comme une application qui génère des messages pour tester l'autoscaling.
	Note
	Si vous utilisez Python 3, entrez`python3 sqs_send_msg.py .`
		DevOps ingénieur

Surveillez les modules de l'application.	1. Dans un autre terminal, entrez la commande suivante pour surveiller les pods :	DevOps ingénieur

Tâche	Description	Compétences requises

	`kubectl -n security get po`
	2. Pour 5 messages non lus dans la file d'attente Amazon SQS, KEDA ajoute un pod. Dans le résultat de la commande précédente, confirmez que de nouveaux pods sont ajoutés. Voici un exemple de sortie :
	`kubectl -n security get po`
	`NAME READY STATUS RESTARTS AGE`
	`q-read-797f4c7589-2bj76 1/1 Running 0 2s`
	`q-read-797f4c7589-4zxph 1/1 Running 0 49s`
	`q-read-797f4c7589-cg9dt 1/1 Running 0 18s`
	`q-read-797f4c7589-slc69 1/1 Running 0 33s`
	3. Lorsque vous avez terminé le test, dans le terminal d'origine, entrez CTRL +C (Windows) ou CMD+C	

Tâche	Description	Compétences requises
	(macOS). Cela arrête le script python sqs_send_msg.py.	

Résolution des problèmes

Problème	Solution

L'opérateur KEDA ne peut pas redimensionner l'application.	Entrez la commande suivante pour vérifier les journaux du rôle `keda-operator` IAM :
	`kubectl logs -n keda -l app=keda-operator -c keda-operator`
	
	S'il existe un code de `HTTP 403` réponse, cela signifie que l'application et le scaler KEDA ne disposent pas des autorisations suffisantes pour accéder à la file d'attente Amazon SQS. Procédez comme suit :
	1. Vérifiez les politiques et instructions IAM du `keda-identity` rôle afin de confirmer que l'accès en lecture à la file d'attente est accordé.
	2. Validez la relation de confiance entre les rôles IAM. Voici un exemple :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`

Problème	Solution

```
                "Service": "pods.eks
.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:TagSession"
            ]
        }
    ]
}
```

En cas d'`Assume-Role` erreur, le rôle IAM d'un nœud Amazon EKS ne peut pas assumer le rôle IAM défini pour. `TriggerAu thentication` Procédez comme suit :

1. Entrez la commande suivante pour supprimer le `keda-operator` module et en créer un nouveau :

```
kubectl delete pod keda-operator-
<alphenumeric-value> --namespace
 keda
```

2. Entrez la commande suivante pour vérifier l'identité assumée par le pod :

```
kubectl describe pod <keda-operator-
pod-name> --namespace keda
```

3. Lorsque le pod redémarre correctement, vérifiez que les deux variables suivantes sont ajoutées à la description du pod :
   - `AWS_CONTAINER_CREDENTIALS_F ULL_URI`
   - `AWS_CONTAINER_AUTHORIZATION _TOKEN_FILE`

Ressources connexes

- Configuration de l'agent d'identité Amazon EKS Pod (documentation Amazon EKS)
- Déploiement de KEDA (documentation KEDA)
- ScaledObject spécification (documentation KEDA)
- Authentification avec TriggerAuthentication (documentation KEDA)

Simplifiez les déploiements de PostgreSQL sur Amazon EKS à l'aide de PGO

Créée par Shalaka Dengale (AWS)

Récapitulatif

Ce modèle intègre l'opérateur Postgres de Crunchy Data (PGO) à Amazon Elastic Kubernetes Service (Amazon EKS) afin de rationaliser les déploiements de PostgreSQL dans les environnements cloud natifs. PGO fournit l'automatisation et l'évolutivité nécessaires à la gestion des bases de données PostgreSQL dans Kubernetes. Lorsque vous associez PGO à Amazon EKS, vous obtenez une plate-forme robuste pour déployer, gérer et dimensionner efficacement les bases de données PostgreSQL.

Cette intégration offre les principaux avantages suivants :

- Déploiement automatisé : simplifie le déploiement et la gestion des clusters PostgreSQL.
- Définitions de ressources personnalisées (CRDs) : utilise les primitives Kubernetes pour la gestion de PostgreSQL.
- Haute disponibilité : prend en charge le basculement automatique et la réplication synchrone.
- Sauvegardes et restaurations automatisées : rationalise les processus de sauvegarde et de restauration.
- Mise à l'échelle horizontale : permet une mise à l'échelle dynamique des clusters PostgreSQL.
- Mises à niveau des versions : facilite les mises à niveau continues avec un minimum de temps d'arrêt.
- Sécurité : applique le chiffrement, les contrôles d'accès et les mécanismes d'authentification.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée sous Linux, macOS ou Windows.
- Config de la CLI AWS, pour connecter AWS les ressources à partir de la ligne de commande.

- eksctl, installé et configuré sous Linux, macOS ou Windows.
- `kubectl`, installé et configuré pour accéder aux ressources de votre cluster Amazon EKS. Pour plus d'informations, consultez Configurer kubectl et eksctl dans la documentation Amazon EKS.
- Votre terminal informatique est configuré pour accéder au cluster Amazon EKS. Pour plus d'informations, consultez Configurer votre ordinateur pour communiquer avec votre cluster dans la documentation Amazon EKS.

Versions du produit

- Versions 1.21 à 1.24 ou ultérieures de Kubernetes (voir la documentation PGO).
- PostgreSQL version 10 ou ultérieure. Ce modèle utilise la version 16 de PostgreSQL.

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Pile technologique cible

- Amazon EKS
- Amazon Virtual Private Cloud (Amazon VPC)
- Amazon Elastic Compute Cloud (Amazon EC2)

Architecture cible

Ce modèle crée une architecture qui contient un cluster Amazon EKS avec trois nœuds. Chaque nœud s'exécute sur un ensemble d' EC2 instances dans le backend. Cette configuration de PostgreSQL suit une architecture de réplication principale, particulièrement efficace pour les cas d'utilisation nécessitant beaucoup de lecture. L'architecture inclut les composants suivants :

- Le conteneur de base de données principal (pg-primary) héberge l'instance principale de PostgreSQL vers laquelle toutes les opérations d'écriture sont dirigées.

- Les conteneurs de répliques secondaires (pg-replica) hébergent les instances PostgreSQL qui répliquent les données de la base de données principale et gèrent les opérations de lecture.
- PgBouncerest un pooler de connexions léger pour les bases de données PostgreSQL inclus dans PGO. Il se situe entre le client et le serveur PostgreSQL et sert d'intermédiaire pour les connexions aux bases de données.
- PGO automatise le déploiement et la gestion des clusters PostgreSQL dans cet environnement Kubernetes.
- Patroni est un outil open source qui gère et automatise les configurations de haute disponibilité pour PostgreSQL. Il est inclus dans PGO. Lorsque vous utilisez Patroni avec PGO dans Kubernetes, cela joue un rôle crucial pour garantir la résilience et la tolérance aux pannes d'un cluster PostgreSQL. Pour plus d'informations, consultez la documentation de Patroni.

Le flux de travail inclut les étapes suivantes :

- Déployez l'opérateur PGO. Vous déployez l'opérateur PGO sur votre cluster Kubernetes qui s'exécute sur Amazon EKS. Cela peut être fait à l'aide de manifestes Kubernetes ou de diagrammes de Helm. Ce modèle utilise des manifestes Kubernetes.
- Définissez les instances de PostgreSQL. Lorsque l'opérateur est en cours d'exécution, vous créez des ressources personnalisées (CRs) pour spécifier l'état souhaité des instances PostgreSQL. Cela inclut les configurations telles que les paramètres de stockage, de réplication et de haute disponibilité.
- Gestion des opérateurs. Vous interagissez avec l'opérateur via des objets de l'API Kubernetes, par exemple CRs pour créer, mettre à jour ou supprimer des instances PostgreSQL.
- Surveillance et maintenance. Vous pouvez surveiller l'état et les performances des instances PostgreSQL exécutées sur Amazon EKS. Les opérateurs fournissent souvent des métriques et des journaux à des fins de surveillance. Vous pouvez effectuer des tâches de maintenance de routine telles que les mises à niveau et les correctifs si nécessaire. Pour plus d'informations, consultez Surveiller les performances de votre cluster et consulter les journaux dans la documentation Amazon EKS.
- Mise à l'échelle et sauvegarde : vous pouvez utiliser les fonctionnalités fournies par l'opérateur pour dimensionner les instances PostgreSQL et gérer les sauvegardes.

Ce modèle ne couvre pas les opérations de surveillance, de maintenance et de sauvegarde.

Automatisation et mise à l'échelle

- Vous pouvez l'utiliser AWS CloudFormation pour automatiser la création de l'infrastructure. Pour plus d'informations, consultez la section Créer des ressources Amazon EKS avec AWS CloudFormation dans la documentation Amazon EKS.
- Vous pouvez utiliser GitVersion les numéros de build de Jenkins pour automatiser le déploiement des instances de base de données.

Outils

Services AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS via des commandes dans votre interface de ligne de commande.

Autres outils

- eksctl est un outil de ligne de commande simple permettant de créer des clusters sur Amazon EKS.
- kubectl est un utilitaire de ligne de commande permettant d'exécuter des commandes sur des clusters Kubernetes.
- PGO automatise et fait évoluer la gestion des bases de données PostgreSQL dans Kubernetes.

Bonnes pratiques

Suivez ces bonnes pratiques pour garantir un déploiement fluide et efficace :

- Sécurisez votre cluster EKS. Mettez en œuvre les meilleures pratiques de sécurité pour votre cluster EKS, telles que l'utilisation de rôles AWS Identity and Access Management (IAM) pour les comptes de service (IRSA), les politiques réseau et les groupes de sécurité VPC. Limitez l'accès au serveur API du cluster EKS et chiffrez les communications entre les nœuds et le serveur API à l'aide du protocole TLS.
- Assurez-vous de la compatibilité des versions entre PGO et Kubernetes s'exécutant sur Amazon EKS. Certaines fonctionnalités de PGO peuvent nécessiter des versions spécifiques de Kubernetes ou introduire des limitations de compatibilité. Pour plus d'informations, consultez la section Composants et compatibilité dans la documentation PGO.

- Planifiez l'allocation des ressources pour votre déploiement PGO, notamment le processeur, la mémoire et le stockage. Tenez compte des besoins en ressources de PGO et des instances PostgreSQL qu'il gère. Surveillez l'utilisation des ressources et adaptez les ressources en fonction des besoins.
- Conçu pour une haute disponibilité. Concevez votre déploiement PGO pour une haute disponibilité afin de minimiser les temps d'arrêt et de garantir la fiabilité. Déployez plusieurs répliques de PGO dans plusieurs zones de disponibilité pour garantir la tolérance aux pannes.
- Mettez en œuvre des procédures de sauvegarde et de restauration pour vos bases de données PostgreSQL gérées par PGO. Utilisez les fonctionnalités fournies par PGO ou des solutions de sauvegarde tierces compatibles avec Kubernetes et Amazon EKS.
- Configurez la surveillance et la journalisation de votre déploiement PGO afin de suivre les performances, l'état de santé et les événements. Utilisez des outils tels que Prometheus pour surveiller les métriques et Grafana pour la visualisation. Configurez la journalisation pour capturer les journaux PGO à des fins de dépannage et d'audit.
- Configurez correctement le réseau pour autoriser les communications entre PGO, les instances PostgreSQL et les autres services de votre cluster Kubernetes. Utilisez les fonctionnalités réseau Amazon VPC et les plug-ins réseau Kubernetes tels que Calico ou Amazon VPC CNI pour appliquer les politiques réseau et isoler le trafic.
- Choisissez les options de stockage appropriées pour vos bases de données PostgreSQL, en tenant compte de facteurs tels que les performances, la durabilité et l'évolutivité. Utilisez les volumes Amazon Elastic Block Store (Amazon EBS) AWS ou les services de stockage gérés pour le stockage persistant. Pour plus d'informations, consultez la section Stocker des volumes Kubernetes avec Amazon EBS dans la documentation Amazon EKS.
- Utilisez des outils d'infrastructure en tant que code (IaC), par exemple AWS CloudFormation pour automatiser le déploiement et la configuration de PGO sur Amazon EKS. Définissez les composants de l'infrastructure, notamment le cluster EKS, le réseau et les ressources PGO, sous forme de code pour garantir la cohérence, la répétabilité et le contrôle des versions.

Épopées

Créer un rôle IAM

Tâche	Description	Compétences requises
Créez un rôle IAM.	1. Créez un rôle IAM à l'aide de la commande suivante dans AWS CLI : `aws iam create-role \ --role-name {YourRoleName} \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "eks.amazonaws.com" }, "Action": "sts:AssumeRole" }] }' && \ aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/AmazonEKSClusterPolicy && \`	Administrateur AWS

Tâche	Description	Compétences requises

	`aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/AmazonEKSServicePolicy && \ aws iam attach-role-policy \ --role-name {YourRoleName}\ --policy-arn arn:aws:iam::aws:policy/CloudWatchFullAccess`
	2. Passez en revue le rôle dans AWS Management Console :
	a. Ouvrez la console IAM.
	b. Choisissez Rôles, puis recherchez le nom du rôle que vous avez créé.
	c. Vérifiez que les politiques suivantes sont associées :
	`AmazonEKSClusterPolicy`
	`AmazonEKSServicePolicy`
	`CloudWatchFullAccess`	

Création d'un cluster Amazon EKS

Tâche	Description	Compétences requises
Créez un cluster Amazon EKS.	Si vous avez déjà déployé un cluster, ignorez cette étape. Sinon, déployez un cluster Amazon EKS dans votre cluster actuel en Compte AWS utilisant `eksctl` Terraform ou. AWS CloudFormation Ce modèle est utilisé `eksctl` pour le déploiement de clusters. **Note** Ce modèle utilise Amazon EC2 comme groupe de nœuds pour Amazon EKS. Si vous souhaitez l'utiliser AWS Fargate, consultez la `managedNodeGroups` configuration dans la documentation eksctl. 1. Utilisez le fichier `eksctl` d'entrée suivant pour générer le cluster. `sample-cluster.yaml` :	Administrateur AWS, administrateur Terraform ou eksctl, administrateur Kubernetes

Tâche	Description	Compétences requises

	`apiVersion: eksctl.io/v1alpha5`
	`kind: ClusterConfig`
	`metadata:`
	`  name: postgresql`
	`  region: us-east-1`
	`  version: "1.29"`
	`accessConfig:`
	`  authenticationMode: API_AND_CONFIG_MAP`
	`availabilityZones:`
	`- us-east-1a`
	`- us-east-1b`
	`- us-east-1c`
	`nodeGroups:`
	`  - name: ng-1`
	`  instanceType: m5.16xlarge`
	`  desiredCapacity: 2`
	`  - name: ng-2`
	`  instanceType: m5.16xlarge`
	`  desiredCapacity: 2`
	`  - name: ng-3`
	`  instanceType: m5.16xlarge`
	`  desiredCapacity: 2`
	`vpc:`
	`  cidr: 192.168.0.0/16`
	`  clusterEndpoints:`
	`  publicAccess: true`
	`  nat:`
	`  gateway: HighlyAvailable`	

Tâche	Description	Compétences requises

	<pre>iamIdentity
	Mappings:
	  - arn: arn:aws:i
	am::<account-id>:r
	ole/<role-name> #
	 update the IAM role
	 ARN created in step 1
	    username: <user-
	name> # Enter the
	 user name per your
	 choice
	    noDuplicateARNs:
	 false</pre> 2. Exécutez la commande suivante pour créer le cluster (indiquez le chemin d'accès à votre `sample-cluster.yaml` fichier) : <pre>eksctl create
	 cluster -f sample-cl
	uster.yaml</pre>	

Validez le statut du cluster.	Exécutez la commande suivante pour connaître l'état actuel des nœuds du cluster : <pre>kubectl get nodes</pre> Si vous rencontrez des erreurs, consultez la section de résolution des problèmes de la documentation Amazon EKS.	Administrateur AWS, administrateur Terraform ou eksctl, administrateur Kubernetes

Création d'un fournisseur d'identité OIDC

Tâche	Description	Compétences requises
Activez le fournisseur IAM OIDC.	Comme condition préalable au pilote Amazon EBS Container Storage Interface (CSI), vous devez disposer d'un fournisseur IAM OpenID Connect (OIDC) existant pour votre cluster. Activez le fournisseur IAM OIDC à l'aide de la commande suivante : `eksctl utils associate -iam-oidc-provider --region={region} --cluster={YourClusterNameHere} --approve` Pour plus d'informations sur cette étape, consultez la documentation Amazon EKS.	Administrateur AWS
Créez un rôle IAM pour le pilote Amazon EBS CSI.	Utilisez la `eksctl` commande suivante pour créer le rôle IAM pour le pilote CSI : `eksctl create iamserviceaccount \ --region {RegionName} \ --name ebs-csi-controller-sa \ --namespace kube-system \`	Administrateur AWS

Tâche	Description	Compétences requises
	`--cluster {YourClusterNameHere} \ --attach-policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy \ --approve \ --role-only \ --role-name AmazonEKS_EBS_CSI_DriverRole` Si vous utilisez des disques Amazon EBS chiffrés, vous devez configurer la politique plus en détail. Pour obtenir des instructions, consultez la documentation du pilote Amazon EBS SCI.	
Ajoutez le pilote Amazon EBS CSI.	Utilisez la `eksctl` commande suivante pour ajouter le pilote Amazon EBS CSI : `eksctl create addon \ --name aws-ebs-csi-driver \ --cluster <YourClusterName> service-account-role-arn arn:aws:iam::$(aws sts get-caller-identity \ --query Account \ --output text):role/AmazonEKS_EBS_CSI_DriverRole \ --force`	Administrateur AWS

Installez PGO

Tâche	Description	Compétences requises
Clonez le dépôt PGO.	Clonez le GitHub dépôt pour PGO : `git clone https://github.com/CrunchyData/postgres-operator-examples.git`	AWS DevOps

Fournissez les détails du rôle pour la création du compte de service.	Pour accorder au cluster Amazon EKS l'accès aux AWS ressources requises, spécifiez le nom de ressource Amazon (ARN) du rôle OIDC que vous avez créé précédemment dans le `service_account.yaml` fichier. Ce fichier se trouve dans le dossier d'espace de noms du référentiel.
	`cd postgres-operator-examples`
	`---`
	`metadata:`
	`  annotations:`
	`    eks.amazonaws.com/role-arn: arn:aws:iam::<accountId>:role/<role_name> # Update the OIDC role ARN created earlier`
		Administrateur AWS, administrateur Kubernetes

Tâche	Description	Compétences requises

Créez l'espace de noms et les prérequis PGO.	1. Exécutez la commande suivante pour créer l'espace de noms .
	`kubectl apply -k kustomize/install/namespace`
	Cela permet d'établir un espace de noms dédié pour PGO. Si nécessaire, vous pouvez modifier le `namespace.yml` fichier et attribuer un autre nom à l'espace de noms.
	2. Exécutez la commande suivante pour appliquer la configuration par défaut au cluster :
	`kubectl apply --server-side -k kustomize/install/default`
	`kustomize/install/default` fournit la configuration par défaut pour le contrôle d'accès basé sur les rôles (RBAC) Kubernetes, la définition des ressources personnalisées (CRD) et les fichiers Kubernetes Manager.
		Administrateur Kunernetes

Tâche	Description	Compétences requises
Vérifiez la création des pods.	Vérifiez que l'espace de noms et la configuration par défaut ont été créés : `kubectl get pods -n postgres-operator`	Administrateur AWS, administrateur Kubernetes
Vérifiez PVCs.	Utilisez la commande suivante pour vérifier les demandes de volume persistantes (PVCs) : `kubectl describe pvc -n postgres-operator`	Administrateur AWS, administrateur Kubernetes

Création et déploiement d'un opérateur

Tâche	Description	Compétences requises

Créez un opérateur.	Révisez le contenu du fichier situé `/kustomize/postgres/postgres.yaml` à l'adresse suivante :
	`spec:`
	`  instances:`
	`  - name: pg-1`
	`  replicas: 3`
	`  patroni:`
	`  dynamicConfiguration:`
	`  postgresql:`
	`  pg_hba:`
	`  - "host all all 0.0.0.0/0 trust"`
	`  # this line enabled`
		Administrateur AWS, DBA, administrateur Kubernetes

Tâche	Description	Compétences requises

	<pre>logical replication
	with programmatic
	access
	- "host all
	postgres 127.0.0.1/32
	md5"
	synchronous_mode:
	true
	users:
	- name: replicator
	databases:
	- testdb
	options: "REPLICAT
	ION"</pre>
	Ces mises à jour permettent d'effectuer les opérations suivantes :
	• Ajustez les paramètres de configuration de PostgreSQL pour faciliter l'accès à l'instance de PostgreSQL.
	• Incluez des configurations pour l'utilisateur de réplication, l'utilisateur de base de données et le superutilisateur afin de permettre la réplication en continu, l'accès aux bases de données et la gestion des clusters.	

Tâche	Description	Compétences requises
Déployez l'opérateur.	Déployez l'opérateur PGO pour rationaliser la gestion et le fonctionnement des bases de données PostgreSQL dans les environnements Kubernetes : `kubectl apply -k kustomize/postgres`	Administrateur AWS, DBA, administrateur Kubernetes

Tâche	Description	Compétences requises

Vérifier le déploiement.	1. Vérifiez que l'opérateur a été déployé :
	`kubectl get pods -n postgres-operator --selector=postgres-operator.crunchydata.com/instance-set \ -L postgres-operator.crunchydata.com/role`
	2. Vérifiez que la ressource de service associée au pod opérateur a été créée :
	`kubectl get svc -n postgres-operator`
	Dans le résultat de la commande, notez le réplica principal (`primary_pod_name`) et le read replica (`read_pod_name`). Vous les utiliserez dans les prochaines étapes.
		Administrateur AWS, DBA, administrateur Kubernetes

Vérifier la réplication en streaming

Tâche	Description	Compétences requises
Écrivez des données dans le réplica principal.	Utilisez les commandes suivantes pour vous connecter à la réplique principale de PostgreSQL et écrire des	Administrateur AWS, administrateur Kubernetes

Tâche	Description	Compétences requises

	données dans la base de données :
	`kubectl exec -it <primary_pod_name> bash -n postgres-operator`
	`psql`
	`CREATE TABLE customers (firstname text, customer_id serial, date_created timestamp );`
	`\dt`	

Vérifiez que la réplique lue contient les mêmes données.	Connectez-vous à la réplique en lecture de PostgreSQL et vérifiez si la réplication en continu fonctionne correctement :
	`kubectl exec -it {read_pod_name} bash -n postgres-operator`
	`psql`
	`\dt`
	Le réplica lu doit contenir la table que vous avez créée dans le réplica principal à l'étape précédente.
		Administrateur AWS, administrateur Kubernetes

Résolution des problèmes

Problème	Solution

Le module ne démarre pas.	• Utilisez la commande suivante pour vérifier l'état du pod :
	`kubectl get pods -n your-namespace`
	• Inspectez les journaux pour détecter d'éventuelles erreurs :
	`kubectl logs your-pod-name -n your-namespace`
	• Vérifiez les événements des pods pour détecter tout événement anormal lié à vos pods :
	`kubectl describe pod your-pod-name -n your-namespace`

Les répliques accusent un retard important par rapport à la base de données principale.	• Vérifiez le décalage de réplication :
	`SELECT * FROM pg_stat_replication;`
	• Assurez-vous que les répliques disposent de suffisamment de ressources de processeur et de mémoire. Vérifiez les limites de ressources :
	`kubectl describe pod your-replica-pod -n your-namespace`
	• Vérifiez que le backend de stockage fonctionne de manière optimale. La lenteur des E/S sur le disque peut entraîner un retard de réplication.

Problème	Solution
Vous n'avez aucune visibilité sur les performances et l'état du cluster PostgreSQL.	• Activez Amazon CloudWatch Logs et assurez-vous que les journaux sont envoyés à Amazon CloudWatch pour analyse. Pour plus d'informations, consultez la documentation Amazon EKS. • Vérifiez **`pg_stat_activity`** : `SELECT * FROM pg_stat_activity;`

La réplication ne fonctionne pas.	• Vérifiez la configuration principale en consultant les paramètres de réplication dans `postgresql.conf` :
	`wal_level = replica`
	`max_wal_senders = 10`
	`wal_keep_size = 64  # or wal_keep_segments in older versions`
	• Vérifiez que cela `pg_hba.conf` inclut les autorisations de réplication :
	`host replication replica_user all md5`
	• Vérifiez la configuration de la réplique. Assurez-vous que les `recovery.conf` paramètres (`standby.signal` et `primary_conninfo`) équivalents sont correctement configurés sur les répliques.

Ressources connexes

- Amazon Elastic Kubernetes Service (présentation des options de déploiement dans le livre blanc AWS)
- AWS CloudFormation(Présentation des options de déploiement sur le livre blanc AWS)
- Commencez avec Amazon EKS — eksctl (Guide de l'utilisateur Amazon EKS)
- Configurer kubectl et eksctl (Guide de l'utilisateur Amazon EKS)
- Création d'un rôle pour la fédération OpenID Connect (Guide de l'utilisateur IAM)
- Configuration des paramètres du AWS CLI (Guide de AWS CLI l'utilisateur)
- Documentation de Crunchy Postgres pour Kubernetes
- Crunch & Learn : Crunchy Postgres pour Kubernetes 5.0 (vidéo)

Simplifiez l'authentification des applications avec le protocole TLS mutuel dans Amazon ECS en utilisant Application Load Balancer

Créée par Olawale Olaleye (AWS) et Shamanth Devagari (AWS)

Récapitulatif

Ce modèle vous permet de simplifier l'authentification de vos applications et de vous décharger des charges liées à la sécurité grâce au protocole TLS mutuel dans Amazon Elastic Container Service (Amazon ECS) en utilisant Application Load Balancer (ALB). Avec ALB, vous pouvez authentifier les certificats client X.509 auprès de. AWS Private Certificate Authority Cette puissante combinaison permet de sécuriser les communications entre vos services, réduisant ainsi le besoin de mécanismes d'authentification complexes au sein de vos applications. En outre, le modèle utilise Amazon Elastic Container Registry (Amazon ECR) pour stocker les images des conteneurs.

L'exemple de ce modèle utilise des images Docker provenant d'une galerie publique pour créer initialement les exemples de charges de travail. Par la suite, de nouvelles images Docker sont créées pour être stockées dans Amazon ECR. Pour la source, considérez un système basé sur Git tel que GitHub GitLab, ou Bitbucket, ou utilisez Amazon Simple Storage Service Amazon S3 (Amazon S3). Pour créer les images Docker, pensez à AWS CodeBuild les utiliser pour les images suivantes.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS ayant accès aux AWS CloudFormation piles de déploiement. Assurez-vous que vous disposez des autorisations d'utilisateur ou de rôle AWS Identity and Access Management (IAM) nécessaires au déploiement CloudFormation.
- AWS Command Line Interface (AWS CLI) installé. Configurez vos AWS informations d'identification sur votre machine locale ou dans votre environnement en utilisant AWS CLI ou en définissant les variables d'environnement dans le `~/.aws/credentials` fichier.
- OpenSSL installé.
- Docker installé.
- Connaissance de ce qui est Services AWS décrit dans la section Outils.
- Connaissance de Docker et NGINX.

Limites

- Le protocole TLS mutuel pour Application Load Balancer ne prend en charge que les certificats clients X.509v3. Les certificats client X.509v1 ne sont pas pris en charge.
- Le CloudFormation modèle fourni dans le référentiel de code de ce modèle n'inclut pas le provisionnement d'un CodeBuild projet dans le cadre de la pile.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Docker version 27.3.1 ou ultérieure
- AWS CLI version 2.14.5 ou ultérieure

Architecture

Le schéma suivant montre les composants de l'architecture de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Créez un dépôt Git et validez le code de l'application dans le référentiel.
2. Créez une autorité de certification (CA) privée dans AWS Private CA.
3. Créez un CodeBuild projet. Déclenché par les modifications de validation, crée l'image Docker et publie l'image créée sur Amazon ECR. CodeBuildproject
4. Copiez la chaîne de certificats et le corps du certificat depuis l'autorité de certification, puis téléchargez le bundle de certificats sur Amazon S3.
5. Créez un trust store avec le bundle CA que vous avez chargé sur Amazon S3. Associez le trust store aux écouteurs TLS mutuels sur l'Application Load Balancer (ALB).
6. Utilisez l'autorité de certification privée pour émettre des certificats clients pour les charges de travail des conteneurs. Créez également un certificat TLS privé à l'aide AWS Private CA de.
7. Importez le certificat TLS privé dans AWS Certificate Manager (ACM) et utilisez-le avec l'ALB.
8. La charge de travail du conteneur dans `ServiceTwo` utilise le certificat client émis pour s'authentifier auprès de l'ALB lorsqu'il communique avec la charge de travail du conteneur dans. `Service0ne`

9. La charge de travail du conteneur dans `ServiceOne` utilise le certificat client émis pour s'authentifier auprès de l'ALB lorsqu'il communique avec la charge de travail du conteneur dans. `ServiceTwo`

Automatisation et mise à l'échelle

Ce modèle peut être entièrement automatisé en utilisant ou CloudFormation en utilisant AWS Cloud Development Kit (AWS CDK) les opérations d'API d'un SDK pour provisionner les AWS ressources.

Vous pouvez l'utiliser AWS CodePipeline pour implémenter un pipeline d'intégration et de déploiement continus (CI/CD) CodeBuild afin d'automatiser le processus de création d'images de conteneur et de déployer de nouvelles versions sur les services de cluster Amazon ECS.

Outils

Services AWS

- AWS Certificate Manager (ACM) vous aide à créer, à stocker et à renouveler les certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et vos applications. AWS
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif permettant d'exécuter, d'arrêter et de gérer des conteneurs sur un cluster. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate. Pour mieux contrôler votre infrastructure, vous pouvez également exécuter vos tâches et services sur un cluster d'instances Amazon Elastic Compute Cloud (Amazon EC2) que vous gérez.
- Amazon ECS Exec vous permet d'interagir directement avec les conteneurs sans avoir à interagir au préalable avec le système d'exploitation du conteneur hôte, à ouvrir les ports entrants ou à gérer les clés SSH. Vous pouvez utiliser ECS Exec pour exécuter des commandes ou envoyer un shell à un conteneur exécuté sur une EC2 instance Amazon ou sur AWS Fargate.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les EC2 instances, les conteneurs et les adresses

IP Amazon, dans une ou plusieurs zones de disponibilité. ELB surveille l'état de santé de ses cibles enregistrées et achemine le trafic uniquement vers les cibles saines. ELB adapte votre équilibreur de charge en fonction de l'évolution de votre trafic entrant au fil du temps. Il peut s'adapter automatiquement à la majorité des charges de travail.

- AWS Fargatevous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou d' EC2 instances Amazon. Fargate est compatible avec Amazon ECS et Amazon Elastic Kubernetes Service (Amazon EKS). Vous pouvez exécuter vos tâches et services Amazon ECS avec le type de lancement Fargate ou avec un fournisseur de capacité Fargate. Pour ce faire, empaquetez votre application dans des conteneurs, spécifiez les exigences en termes de processeur et de mémoire, définissez les politiques réseau et IAM, puis lancez l'application. Chaque tâche Fargate possède sa propre limite d'isolation et ne partage pas le noyau sous-jacent, les ressources du processeur, les ressources de mémoire ou l'interface elastic network avec une autre tâche.
- AWS Private Certificate Authoritypermet de créer des hiérarchies d'autorités de certification (CA) privées, y compris racine et subordonnée CAs, sans les coûts d'investissement et de maintenance liés à l'exploitation d'une autorité de certification sur site.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- GitHub, GitLab, et Bitbucket font partie des systèmes de contrôle de source basés sur Git les plus couramment utilisés pour suivre les modifications du code source.
- NGINX Open Source est un équilibreur de charge, un cache de contenu et un serveur Web open source. Ce modèle l'utilise comme serveur Web.
- OpenSSL est une bibliothèque open source qui fournit des services utilisés par les implémentations OpenSSL de TLS et de CMS.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub MTLS-with-Application-Load-Balancer-in-Amazon-ECS.

Bonnes pratiques

- Utilisez Amazon ECS Exec pour exécuter des commandes ou envoyer un shell à un conteneur exécuté sur Fargate. Vous pouvez également utiliser ECS Exec pour collecter des informations de diagnostic pour le débogage.
- Utilisez des groupes de sécurité et des listes de contrôle d'accès réseau (ACLs) pour contrôler le trafic entrant et sortant entre les services. Les tâches Fargate reçoivent une adresse IP du sous-réseau configuré dans votre cloud privé virtuel (VPC).

Épopées

Création du référentiel

Tâche	Description	Compétences requises
Téléchargez le code source.	Pour télécharger le code source de ce modèle, dupliquez ou clonez le référentiel GitHub MTLS-with-Application-Load-Balancer-in-Amazon-ECS.	DevOps ingénieur
Créez un dépôt Git.	Pour créer un dépôt Git contenant le Dockerfile et les `buildspec.yaml` fichiers, procédez comme suit : 1. Créez un dossier dans votre environnement virtuel. Nommez-le avec le nom de votre projet. 2. Ouvrez un terminal sur votre ordinateur local et accédez à ce dossier. 3. Pour cloner le référentiel MTLS-with-Application-Load-Balancer-in-Amazon	DevOps ingénieur

Tâche	Description	Compétences requises
	-ECS dans le répertoire de votre projet, entrez la commande suivante : `git clone https://github.com/aws-samples/mTLS-with-Application-Load-Balancer-in-Amazon-ECS.git`	

Création d'une autorité de certification et génération de certificats

Tâche	Description	Compétences requises
Créez une autorité de certification privée dans AWS Private CA.	Pour créer une autorité de certification (CA) privée, exécutez les commandes suivantes dans votre terminal. Remplacez les valeurs des exemples de variables par vos propres valeurs. `export AWS_DEFAULT_REGION="us-west-2"` `export SERVICES_DOMAIN="www.example.com"` `export ROOT_CA_ARN=`aws acm-pca create-certificate-authority \` `--certificate-authority-type ROOT \`	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises

	`--certificate-authority-configuration \`
	`"KeyAlgorithm=RSA_2048,`
	`SigningAlgorithm=SHA256WITHRSA,`
	`Subject={`
	`Country=US,`
	`State=WA,`
	`Locality=Seattle,`
	`Organization=Build on AWS,`
	`OrganizationalUnit=mTLS Amazon ECS and ALB Example,`
	`CommonName=${SERVICES_DOMAIN}}" \`
	`--query CertificateAuthorityArn --output text`
	
	Pour plus de détails, voir Créer une autorité de certification privée AWS Private CA dans la AWS documentation.	

Tâche	Description	Compétences requises

Créez et installez votre certificat CA privé.	Pour créer et installer un certificat pour votre autorité de certification racine privée, exécutez les commandes suivantes dans votre terminal :
	
	1. Générez une demande de signature de certificat (CSR).
	
	`ROOT_CA_CSR=`aws acm-pca get-certificate-authority-csr \ --certificate-authority-arn ${ROOT_CA_ARN} \ --query Csr --output text``
	
	2. Émettez le certificat racine.
	
	`AWS_CLI_VERSION=$( aws --version 2>&1 | cut -d/ -f2 | cut -d. -f1) [[ ${AWS_CLI_VERSION} -gt 1 ]] && ROOT_CA_CSR="$(echo ${ROOT_CA_CSR} | base64)" ROOT_CA_CERT_ARN= `aws acm-pca issue-certificate \ --certificate-authority-arn ${ROOT_CA_ARN} \ --template-arn arn:aws:acm-pca::: template/RootCACertificate/V1 \`
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	<pre> --signing-
	algorithm SHA256WIT
	HRSA \
	    --validity
	 Value=10,Type=YEARS
	 \
	    --csr "${ROOT_C
	A_CSR}" \
	    --query Certifica
	teArn --output text`</pre> 3. Récupérez le certificat racine. <pre>ROOT_CA_CERT=`aws
	 acm-pca get-certi
	ficate \
	    --certificate-arn
	 ${ROOT_CA_CERT_ARN}
	 \
	    --certificate-
	authority-arn
	 ${ROOT_CA_ARN} \
	    --query Certifica
	te --output text`
	
	# store for later use
	aws acm-pca get-certi
	ficate \
	    --certificate-arn
	 ${ROOT_CA_CERT_ARN}
	 \
	    --certificate-
	authority-arn
	 ${ROOT_CA_ARN} \
	    --query Certifica
	te --output text >
	 ca-cert.pem</pre> 4. Importez le certificat de l'autorité de certification	

Tâche	Description	Compétences requises

	racine pour l'installer sur l'autorité de certification.
	
	`[[ ${AWS_CLI_VERSION} -gt 1 ]] && ROOT_CA_CERT="$(echo ${ROOT_CA_CERT} | base64)"`
	
	`aws acm-pca import-certificate-authority-certificate \ --certificate-authority-arn $ROOT_CA_ARN \ --certificate "${ROOT_CA_CERT}"`
	
	Pour plus de détails, consultez la section Installation du certificat CA dans la AWS documentation.	

Tâche	Description	Compétences requises
Demandez un certificat géré.	Pour demander un certificat privé AWS Certificate Manager à utiliser avec votre ALB privé, utilisez la commande suivante : `export TLS_CERTIFICATE_ARN=`aws acm request-certificate \ --domain-name "*.${DOMAIN_DOMAIN}" \ --certificate-authority-arn ${ROOT_CA_ARN} \ --query CertificateArn --output text``	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises

Utilisez l'autorité de certification privée pour émettre un certificat client.	• Pour créer une demande de signature de certificat (CSR) pour les deux services, utilisez la AWS CLI commande suivante :
	
	`openssl req -out client_csr1.pem -new -newkey rsa:2048 -nodes -keyout client_private-key1.pem`
	
	`openssl req -out client_csr2.pem -new -newkey rsa:2048 -nodes -keyout client_private-key2.pem`
	
	Cette commande renvoie le CSR et la clé privée pour les deux services.
	
	• Pour délivrer un certificat pour les services, exécutez les commandes suivantes pour utiliser l'autorité de certification privée que vous avez créée :
	
	`SERVICE_ONE_CERT_ARN=`aws acm-pca issue-certificate \`
		DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	`--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr1.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text` `echo "SERVICE_ONE_CERT_ARN: ${SERVICE_ONE_CERT_ARN}"` `aws acm-pca get-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--certificate-arn ${SERVICE_ONE_CERT_ARN} \` `| jq -r '.Certificate' > client_cert1.cert` `SERVICE_TWO_CERT_ARN=`aws acm-pca issue-certificate \` `--certificate-authority-arn ${ROOT_CA_ARN} \` `--csr fileb://client_csr2.pem \` `--signing-algorithm "SHA256WITHRSA" \` `--validity Value=5,Type="YEARS" --query CertificateArn --output text`	

Tâche	Description	Compétences requises

	``
	echo "SERVICE_TWO_CERT_
	ARN: ${SERVICE
	_TWO_CERT_ARN}"
	
	aws acm-pca get-certi
	ficate \
	    --certificate-auth
	ority-arn ${ROOT_CA
	_ARN} \
	    --certificate-arn
	 ${SERVICE_TWO_CERT
	_ARN} \
	     | jq -r '.Certifi
	cate' > client_ce
	rt2.cert
	``
	
	Pour plus d'informations, consultez la section Émettre des certificats d'entité finale privés dans la AWS documentation.	

Fournir des services AWS

Tâche	Description	Compétences requises
Fourniture Services AWS avec le CloudFormation modèle.	Pour provisionner le cloud privé virtuel (VPC), le cluster Amazon ECS, les services Amazon ECS, Application Load Balancer et Amazon Elastic Container Registry (Amazon ECR), utilisez le modèle. CloudFormation	DevOps ingénieur

Tâche	Description	Compétences requises

Obtenez des variables.	Vérifiez que vous disposez d'un cluster Amazon ECS avec deux services en cours d'exécution. Pour récupérer les détails des ressources et les stocker sous forme de variables, utilisez les commandes suivantes :
	
	`export LoadBalancerDNS=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`LoadBalancerDNS`].OutputValue')`
	
	`export ECRRepositoryUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepositoryUri`].OutputValue')`
	
	`export ECRRepositoryServiceOneUri=$(aws cloudformation describe-stacks --stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputKey==`ECRRepository`
		DevOps ingénieur

Tâche	Description	Compétences requises
	ServiceOneUri`].Ou tputValue')  export ECRReposi toryServiceTwoUri= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`ECRRepository ServiceTwoUri`].Ou tputValue')  export ClusterName= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`ClusterName`] .OutputValue')  export BucketName= $(aws cloudformation  describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0 ].Outputs[?OutputK ey==`BucketName`]. OutputValue') export Service1L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \	

Tâche	Description	Compétences requises
	--query 'Stacks[0].Outputs[?OutputK ey==`Service1Liste nerArn`].OutputVal ue') export Service2L istenerArn=$(aws cloudformation describe-stacks -- stack-name ecs-mtls \ --output text \ --query 'Stacks[0].Outputs[?OutputK ey==`Service2Liste nerArn`].OutputVal ue')	

Tâche	Description	Compétences requises
Créez un CodeBuild projet.	Pour utiliser un CodeBuild projet afin de créer les images Docker pour vos services Amazon ECS, procédez comme suit : 1. Connectez-vous à la CodeBuild console et AWS Management Console ouvrez-la à l'adresse https://console.aws.amazon.com/codesuite/codebuild/. 2. Crée un projet. Pour Source, choisissez le dépôt Git que vous avez créé. Pour plus d'informations sur les différents types d'intégration du référentiel Git, consultez la section Utilisation des connexions dans la AWS documentation. 3. Vérifiez que le mode privilégié est activé. Pour créer des images Docker, ce mode est nécessaire. Dans le cas contraire, l'image ne sera pas créée correctement. 4. Utilisez le `buildspec.yaml` fichier personnalisé partagé pour chaque service.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	5. Entrez des valeurs pour le nom et la description du projet. Pour plus de détails, voir Créer un projet de construction AWS CodeBuild dans la AWS documentation.	

Tâche	Description	Compétences requises

Créez les images Docker.	Vous pouvez l'utiliser CodeBuild pour exécuter le processus de création d'image. CodeBuild a besoin d'autorisations pour interagir avec Amazon ECR et pour travailler avec Amazon S3.
	
	Dans le cadre du processus , l'image Docker est créée et envoyée au registre Amazon ECR. Pour plus de détails sur le modèle et le code, consultez la section Informations supplémentaires.
	
	(Facultatif) Pour créer localement à des fins de test, utilisez la commande suivante :
	
	`# login to ECR`
	`aws ecr get-login`
	`-password | docker`
	`login --username`
	`AWS --password-stdin`
	`$ECRRepositoryUri`
	
	`# build image for`
	`service one`
	`cd /service1`
	`aws s3 cp s3://$Buc`
	`ketName/serviceone/`
	`service1/ --recursive`
	`docker build -t`
	`$ECRRepositoryServ`
	`iceOneUri .`
		DevOps ingénieur

Tâche	Description	Compétences requises

	`docker push $ECRRepositoryServiceOneUri`
	
	`# build image for service two`
	`cd ../service2`
	`aws s3 cp s3://$BucketName/servicetwo/service2/ --recursive`
	`docker build -t $ECRRepositoryServiceTwoUri .`
	`docker push $ECRRepositoryServiceTwoUri`	

Activer le protocole TLS mutuel

Tâche	Description	Compétences requises
Téléchargez le certificat CA sur Amazon S3.	Pour télécharger le certificat CA dans le compartiment Amazon S3, utilisez l'exemple de commande suivant : `aws s3 cp ca-cert.pem s3://$BucketName/acm-trust-store/`	AWS DevOps, DevOps ingénieur
Créez le trust store.	Pour créer le trust store, utilisez l'exemple de commande suivant : `TrustStoreArn=`aws elbv2 create-trust-store --name acm-pca-trust-certs \`	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	`--ca-certificates-bundle-s3-bucket $BucketName \ --ca-certificates-bundle-s3-key acm-trust-store/ca-cert.pem --query 'TrustStores[].TrustStoreArn' --output text`	

Téléchargez les certificats clients.	Pour télécharger des certificats clients sur Amazon S3 pour des images Docker, utilisez l'exemple de commande suivant :
	`# for service one aws s3 cp client_cert1.cert s3://$BucketName/serviceone/ aws s3 cp client_private-key1.pem s3://$BucketName/serviceone/`
	`# for service two aws s3 cp client_cert2.cert s3://$BucketName/servicetwo/ aws s3 cp client_private-key2.pem s3://$BucketName/servicetwo/`
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

Modifiez l'écouteur.	Pour activer le protocole TLS mutuel sur l'ALB, modifiez les écouteurs HTTPS à l'aide des commandes suivantes :
	
	`aws elbv2 modify-listener \ --listener-arn $Service1ListenerArn \ --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \ --ssl-policy ELBSecurityPolicy-2016-08 \ --protocol HTTPS \ --port 8080 \ --mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false`
	
	`aws elbv2 modify-listener \ --listener-arn $Service2ListenerArn \ --certificates CertificateArn=$TLS_CERTIFICATE_ARN_TWO \ --ssl-policy ELBSecurityPolicy-2016-08 \ --protocol HTTPS \ --port 8090 \`
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	`--mutual-authentication Mode=verify,TrustStoreArn=$TrustStoreArn,IgnoreClientCertificateExpiry=false` Pour plus d'informations, consultez la section Configuration du protocole TLS mutuel sur un Application Load Balancer dans AWS la documentation.	

Mettre à jour les services

Tâche	Description	Compétences requises
Mettez à jour la définition de tâche Amazon ECS.	Pour mettre à jour la définition de tâche Amazon ECS, modifiez le `image` paramètre dans la nouvelle révision. Pour obtenir les valeurs des services respectifs, mettez à jour les définitions de tâches avec le nouvel URI des images Docker que vous avez créé lors des étapes précédentes : ou `echo $ECRRepositoryServiceOneUri` `echo $ECRRepositoryServiceTwoUri`	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>"containerDefiniti
	ons": [
	{
	"name":
	"nginx",
	"image":
	"public.ecr.aws/ng
	inx/nginx:latest",
	# <----- change to new
	Uri
	"cpu": 0,</pre> Pour plus d'informations, consultez la section Mise à jour d'une définition de tâche Amazon ECS à l'aide de la console dans la AWS documentation.	

Tâche	Description	Compétences requises
Mettez à jour le service Amazon ECS.	Mettez à jour le service avec la dernière définition de tâche. Cette définition de tâche est le modèle pour les images Docker nouvellement créées, et elle contient le certificat client requis pour l'authent ification TLS mutuelle. Pour mettre à jour le service, procédez comme suit : 1. Ouvrez la console Amazon ECS dans la https://console.aws.amazon.com/ecs/version v2. 2. Sur la page Clusters, choisissez le cluster. 3. Sur la page des détails du cluster, dans la section Services, cochez la case à côté du service, puis choisissez Mettre à jour. 4. Pour que votre service démarre un nouveau déploiement, sélection nez Force new deploymen t (Forcer un nouveau déploiement). 5. Pour Définition des tâches, choisissez la famille de définitions de tâches et la dernière révision. 6. Choisissez Mettre à jour.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	Répétez les étapes pour l'autre service.	

Accédez à l'application

Tâche	Description	Compétences requises
Copiez l'URL de l'application.	Utilisez la console Amazon ECS pour consulter la tâche. Lorsque le statut de la tâche est passé à En cours d'exécution, sélectionnez la tâche. Dans la section Tâche, copiez l'ID de la tâche.	Administrateur AWS, AWS DevOps

Testez votre application.	Pour tester votre application, utilisez ECS Exec pour accéder aux tâches.
	1. Pour le premier service, utilisez la commande suivante :
	`container="nginx"`
	`ECS_EXEC_TASK_ARN="<TASK ARN>"`
	`aws ecs execute-command --cluster $ClusterName \ --task $ECS_EXEC_TASK_ARN \ --container $container \ --interactive \ --command "/bin/bash"`
		Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

	2. Dans le conteneur de la tâche du service 1, utilisez la commande suivante pour saisir l'équilibreur de charge interne `url` et le port d'écoute qui pointe vers le service 2. Spécifiez ensuite le chemin d'accès au certificat client pour tester l'application :
	`curl -kvs https://<internal-alb-url>:8090 --key /usr/local/share/ca-certificates/client.key --cert /usr/local/share/ca-certificates/client.crt`
	3. Dans le conteneur de la tâche du service 2, utilisez la commande suivante pour saisir l'équilibreur de charge interne `url` et le port d'écoute qui pointe vers le service 1. Spécifiez ensuite le chemin d'accès au certificat client pour tester l'application :
	`curl -kvs https://<internal-alb-url>:8080 --key /usr/local/share/ca-certificates/client.key --cert /usr/loca`	

Tâche	Description	Compétences requises
	`l/share/ca-certificates/client.crt` **Note** L'-kindicateur figurant dans les commandes curl (dans le cadre de-`kvs`) désactive la validation du certificat SSL. Vous pouvez supprimer cet indicateur lorsque vous utilisez un certificat SSL correspondant à votre nom de domaine, ce qui permet une validation correcte du certificat.	

Ressources connexes

Documentation Amazon ECS

- Création d'une définition de tâche Amazon ECS à l'aide de la console
- Création d'une image de conteneur à utiliser sur Amazon ECS
- Clusters Amazon ECS
- Amazon ECS pour AWS Fargate
- Bonnes pratiques de mise en réseau Amazon ECS
- Paramètres de définition du service Amazon ECS

Autres AWS ressources

- Comment utiliser AWS une autorité de certification privée pour configurer les MTL sur l'Application Load Balancer ? (AWS re:Post)

Informations supplémentaires

Modification du Dockerfile

Le code suivant montre les commandes que vous modifiez dans le Dockerfile pour le service 1 :

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 1: Ok" > /usr/share/nginx/html/index.html
ADD client_cert1.cert client_private-key1.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

Le code suivant montre les commandes que vous modifiez dans le Dockerfile pour le service 2 :

```
FROM public.ecr.aws/nginx/nginx:latest
WORKDIR /usr/share/nginx/html
RUN echo "Returning response from Service 2: Ok" > /usr/share/nginx/html/index.html
ADD client_cert2.cert client_private-key2.pem /usr/local/share/ca-certificates/
RUN chmod -R 400 /usr/local/share/ca-certificates/
```

Si vous créez les images Docker avec CodeBuild, le `buildspec` fichier utilise le numéro de CodeBuild version pour identifier de manière unique les versions de l'image en tant que valeur de balise. Vous pouvez modifier le `buildspec` fichier en fonction de vos besoins, comme indiqué dans le code `buildspec` personnalisé suivant :

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws ecr get-login-password --region $AWS_DEFAULT_REGION | docker login --
username AWS --password-stdin $ECR_REPOSITORY_URI
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=${COMMIT_HASH:=latest}
  build:
```

```
    commands:
        # change the S3 path depending on the service
      - aws s3 cp s3://$YOUR_S3_BUCKET_NAME/serviceone/ $CodeBuild_SRC_DIR/ --
recursive
      - echo Build started on `date`
      - echo Building the Docker image...
      - docker build -t $ECR_REPOSITORY_URI:latest .
      - docker tag $ECR_REPOSITORY_URI:latest $ECR_REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $ECR_REPOSITORY_URI:latest
      - docker push $ECR_REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      # for ECS deployment reference
      - printf '[{"name":"%s","imageUri":"%s"}]' $CONTAINER_NAME $ECR_REPOSITORY_URI:
$IMAGE_TAG > imagedefinitions.json

artifacts:
  files:
    - imagedefinitions.json
```

Plus de modèles

- Évaluez l'état de préparation des applications pour la migration vers le cloud AWS à l'aide de CAST Highlight
- Automatisez la suppression des AWS CloudFormation piles et des ressources associées
- Automatisez la gestion dynamique du pipeline pour le déploiement de solutions de correctifs dans les environnements Gitflow en utilisant et AWS Service CatalogAWS CodePipeline
- Créez automatiquement des pipelines CI/CD et des clusters Amazon ECS pour les microservices à l'aide d'AWS CDK
- Créez et envoyez des images Docker vers Amazon ECR à l'aide d' GitHub Actions et de Terraform
- Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age
- Créez un analyseur de journaux personnalisé pour Amazon ECS à l'aide d'un routeur de journaux Firelens
- Déployer un pipeline CI/CD pour les microservices Java sur Amazon ECS
- Déployez un cluster Amazon EKS depuis AWS Cloud9 à l'aide d'un profil d'instance EC2
- Déployez un environnement pour les applications Blu Age conteneurisées à l'aide de Terraform
- Déployez une logique de prétraitement dans un modèle de machine learning sur un seul point de terminaison à l'aide d'un pipeline d'inférence sur Amazon SageMaker
- Gérez les déploiements bleu/vert de microservices vers plusieurs comptes et régions à l'aide des services de code AWS et des clés multirégionales AWS KMS
- Gérez les applications de conteneur sur site en configurant Amazon ECS Anywhere avec le kit AWS CDK
- Migrer d'Oracle GlassFish vers AWS Elastic Beanstalk
- Migrer d'Oracle WebLogic vers Apache Tomcat (ToMee) sur Amazon ECS
- Configurez un espace de données minimum viable pour partager les données entre les organisations
- Modernisez les applications ASP.NET Web Forms sur AWS
- Surveillez les référentiels Amazon ECR pour détecter les autorisations génériques à l'aide d'AWS et d'AWS Config CloudFormation
- Surveillez l'activité des applications à l'aide de CloudWatch Logs Insights
- Configurez un pipeline CI/CD pour les charges de travail hybrides sur Amazon ECS Anywhere à l'aide d'AWS CDK et GitLab

- Configuration d'un référentiel de graphiques Helm v3 dans Amazon S3
- Configurer le end-to-end chiffrement des applications sur Amazon EKS à l'aide du gestionnaire de certificats et de Let's Encrypt
- Simplifiez le déploiement d'applications multi-locataires Amazon EKS à l'aide de Flux
- Rationalisez les flux de travail d'apprentissage automatique, du développement local aux expériences évolutives en utilisant l' SageMaker IA et Hydra
- Structurer un projet Python dans une architecture hexagonale à l'aide d'AWS Lambda
- AWS Infrastructure de test à l'aide LocalStack de tests Terraform
- Formez et déployez un modèle de machine learning personnalisé supporté par GPU sur Amazon SageMaker
- Coordonnez la dépendance des ressources et l'exécution des tâches à l'aide de la structure AWS Fargate WaitCondition hook
- Utilisez les agents Amazon Bedrock pour automatiser la création de contrôles d'accès dans Amazon EKS via des instructions textuelles

sans serveur

Rubriques

- Créez une application mobile React Native sans serveur à l'aide d'AWS Amplify
- Gestion des locataires sur plusieurs produits SaaS sur un seul plan de contrôle
- Création d'une EventBridge connexion Amazon entre comptes dans une organisation
- Fournissez des enregistrements DynamoDB à Amazon S3 à l'aide de Kinesis Data Streams et Firehose avec AWS CDK
- Implémentez la gestion des versions d'API basée sur les chemins en utilisant des domaines personnalisés dans Amazon API Gateway
- Importez la bibliothèque psycopg2 pour interagir avec votre base AWS Lambda de données PostgreSQL
- Intégrez Amazon API Gateway à Amazon SQS pour gérer le REST asynchrone APIs
- Traitez les événements de manière asynchrone avec Amazon API Gateway et AWS Lambda
- Traitez les événements de manière asynchrone avec Amazon API Gateway et Amazon DynamoDB Streams
- Traitez les événements de manière asynchrone avec Amazon API Gateway, Amazon SQS et AWS Fargate
- Exécutez les tâches d'automatisation d'AWS Systems Manager de manière synchrone depuis AWS Step Functions
- Exécuter des lectures parallèles d'objets S3 en utilisant Python dans une AWS Lambda fonction
- Envoyez des données de télémétrie de AWS Lambda vers OpenSearch pour des analyses et des visualisations en temps réel
- Configuration d'un routeur cellulaire sans serveur pour une architecture basée sur les cellules
- Configurer un accès privé à un compartiment Amazon S3 via un point de terminaison VPC
- Résoudre les problèmes liés aux états en AWS Step Functions utilisant Amazon Bedrock
- Enchaînez les services AWS en utilisant une approche sans serveur
- Plus de modèles

Créez une application mobile React Native sans serveur à l'aide d'AWS Amplify

Créée par Deekshitulu Pentakota (AWS)

Récapitulatif

Ce modèle montre comment créer un backend sans serveur pour une application mobile React Native à l'aide d'AWS Amplify et des services AWS suivants :

- AWS AppSync
- Amazon Cognito
- Amazon DynamoDB

Après avoir configuré et déployé le backend de l'application à l'aide d'Amplify, Amazon Cognito authentifie les utilisateurs de l'application et les autorise à accéder à l'application. AWS interagit AppSync ensuite avec l'application frontale et avec une table DynamoDB principale pour créer et récupérer des données.

> **Note**
>
> Ce modèle utilise une simple application « ToDoList » comme exemple, mais vous pouvez utiliser une procédure similaire pour créer n'importe quelle application mobile React Native.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande Amplify (Amplify CLI), installée et configurée
- XCode (n'importe quelle version)
- Microsoft Visual Studio (n'importe quelle version, n'importe quel éditeur de code, n'importe quel éditeur de texte)
- Connaissance d'Amplify
- Connaissance d'Amazon Cognito

- Connaissance d'AWS AppSync
- Connaissance de DynamoDB
- Connaissance de Node.js
- Familiarité avec npm
- Connaissance de React et React Native
- Familiarité avec JavaScript et (ECMAScript 6) ES6
- Connaissance de GraphQL

Architecture

Le schéma suivant montre un exemple d'architecture permettant d'exécuter le backend d'une application mobile React Native dans le cloud AWS :

Le schéma montre l'architecture suivante :

1. Amazon Cognito authentifie les utilisateurs de l'application et les autorise à accéder à l'application.
2. Pour créer et récupérer des données, AWS AppSync utilise une API GraphQL pour interagir avec l'application frontale et une table DynamoDB principale.

Outils

Services AWS

- AWS Amplify est un ensemble d'outils et de fonctionnalités spécialement conçus pour aider les développeurs web et mobiles frontaux à créer rapidement des applications complètes sur AWS.
- AWS AppSync fournit une interface GraphQL évolutive qui aide les développeurs d'applications à combiner des données provenant de plusieurs sources, notamment Amazon DynamoDB, AWS Lambda et HTTP. APIs
- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour les applications Web et mobiles.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.

Code

Le code de l'exemple d'application utilisé dans ce modèle est disponible dans le ios-todo-app référentiel GitHub aws-amplify-react-native-. Pour utiliser les fichiers d'exemple, suivez les instructions de la section Epics de ce modèle.

Épopées

Créez et exécutez votre application React Native

Tâche	Description	Compétences requises
Configurez un environnement de développement React Native.	Pour obtenir des instructions, consultez la section Configuration de l'environnement de développement dans la documentation de React Native.	Développeur d’applications

Créez et exécutez l'application mobile ToDoList React Native dans le simulateur iOS.	1. Créez un nouveau répertoire de projets d'application mobile React Native dans votre environnement local en exécutant la commande suivante dans une nouvelle fenêtre de terminal :
	`npx react-native init ToDoListAmplify`
	2. Accédez au répertoire racine du projet en exécutant la commande suivante :
	`cd ToDoListAmplify`
	3. Exécutez l'application en exécutant la commande suivante :
		Développeur d’applications

Tâche	Description	Compétences requises
	`npx react-native run-ios`	

Initialisation d'un nouvel environnement principal pour l'application

Tâche	Description	Compétences requises

Créez les services principaux nécessaires pour prendre en charge l'application dans Amplify.	1. Dans votre environnement local, exécutez la commande suivante depuis le répertoire racine du projet (ToDoListAmplify) :
	`amplify init`
	2. Un message vous demandant de fournir des informations sur l'application s'affiche. Entrez les informations requises en fonction de votre cas d'utilisation. Ensuite, appuyez sur Entrée.
	
	Pour la configuration de ToDoList l'application utilisée dans ce modèle, appliquez l'exemple de configuration suivant.
	
	Exemple de paramètres de configuration de l'application React Native Amplify
	`? Name: ToDoListAmplify`
		Développeur d’applications

Tâche	Description	Compétences requises
	``` ? Environment: dev ? Default editor: Visual Studio Code ? App type: javascript ? Javascript framework : react-native ? Source Directory Path: src ? Distribution Directory Path: / ? Build Command: npm run-script build ? Start Command: npm run-script start ? Select the authentic ation method you want to use: AWS profile ? Please choose the profile you want to use: default ```	
	Pour plus d'informations, consultez la section Créer un nouveau backend Amplify dans la documentation Amplify Dev Center.	

Tâche	Description	Compétences requises
	Note La `amplify init` commande fournit les ressources suivantes à l'aide d'AWS CloudFormation : • Rôles AWS Identity and Access Management (IAM) pour les utilisateurs authentifiés et non authentifiés (rôle Auth et rôle Unauth) • Un bucket Amazon Simple Storage Service (Amazon S3) à déployer (pour l'exemple d'application de ce modèle, Amplify-meta.json) • Un environnement principal dans Amplify Hosting	

Ajoutez l'authentification Amazon Cognito à votre application Amplify React Native

Tâche	Description	Compétences requises
Créez un service d'authentification Amazon Cognito.	1. Dans votre environnement local, exécutez la commande suivante depuis le répertoire racine du projet (ToDoListAmplify) :	Développeur d’applications

Tâche	Description	Compétences requises

	`amplify add auth`
	2. Un message vous demandant de fournir des informations sur les paramètres de configuration du service d'authentification s'affiche. Entrez les informations requises en fonction de votre cas d'utilisation. Ensuite, appuyez sur Entrée.
	
	Pour la configuration de ToDoList l'application utilisée dans ce modèle, appliquez l'exemple de configuration suivant.
	
	Exemples de paramètres de configuration du service d'authentification
	
	`? Do you want to use the default authentication and security configuration? \`
	`Default configuration`
	
	`? How do you want users to be able to sign in? \`
	`Username`
	
	`? Do you want to configure advanced settings? \`	

Tâche	Description	Compétences requises
	`No, I am done` **Note** La `amplify add auth` commande crée les dossiers, fichiers et fichiers de dépendance nécessaires dans un dossier local (amplify) situé dans le répertoire racine du projet. Pour la configuration de ToDoList l'application utilisée dans ce modèle, le fichier aws-exports.js est créé à cette fin.	

Tâche	Description	Compétences requises

Déployez le service Amazon Cognito sur le cloud AWS.	1. À partir du répertoire racine du projet, exécutez la commande Amplify CLI suivante :
	`amplify push`
	2. Un message vous demandant de confirmer le déploiement s'affiche . Entrez Oui. Ensuite, appuyez sur Entrée.
	Note
	Pour voir les services déployés dans votre projet, accédez à la console Amplify en exécutant la commande suivante :
	`amplify console`
		Développeur d’applications

Tâche	Description	Compétences requises

Installez les bibliothèques Amplify requises pour React Native et les CocoaPods dépendances pour iOS.	1. Installez les bibliothèques clientes open source Amplify requises en exécutant la commande suivante depuis le répertoire racine du projet :
	`npm install aws-amplify aws-amplify-react-native \ amazon-cognito-identity-js @react-native-community/netinfo \ @react-native-async-storage/async-storage`
	2. Installez les CocoaPods dépendances requises pour iOS en exécutant la commande suivante :
	`npx pod-install`
		Développeur d’applications

Tâche	Description	Compétences requises

Importez et configurez le service Amplify.	Dans le fichier du point d'entrée de l'application (par exemple, App.js), importez et chargez le fichier de configuration du service Amplify en saisissant les lignes de code suivantes :
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	Note
	Si vous recevez un message d'erreur après avoir importé le service Amplify dans le fichier de point d'entrée de l'application, arrêtez l'application. Ensuite, ouvrez XCode et sélectionnez le ToDoListAmplifyfichier .xcworkspace dans le dossier iOS du projet, puis exécutez l'application.
		Développeur d'applications

Tâche	Description	Compétences requises
Mettez à jour le fichier de point d'entrée de votre application pour utiliser le composant WithAuthenticator Higher-Order (HOC).	**Note** Le `withAuthenticator` HOC fournit des flux de travail de connexion, d'inscription et de mot de passe oublié dans votre application en utilisant seulement quelques lignes de code. Pour plus d'informations, voir Option 1 : Utiliser des composants d'interface utilisateur prédéfinis dans le centre de développement Amplify. Également, des composants d'ordre supérieur dans la documentation de React. 1. Dans le fichier du point d'entrée de l'application (par exemple, App.js), importez le `withAuthenticator` HOC en saisissant les lignes de code suivantes : `import { withAuthenticator } from`	Développeur d'applications

Tâche	Description	Compétences requises

	`'aws-amplify-react-native'`
	2. Exportez le WithAuthenticator HOC en saisissant le code suivant :
	`export default withAuthenticator(App)`
	
	Exemple de code WithAuthenticator HOC
	
	`import Amplify from 'aws-amplify'`
	`import config from './src/aws-exports'`
	`Amplify.configure(config)`
	`import { withAuthenticator } from 'aws-amplify-react-native';`
	
	`const App = () => {`
	`  return null;`
	`};`
	
	`export default withAuthenticator(App);`
	
	Note
	Dans iOS Simulator, l'application affiche l'écran de connexion	

Tâche	Description	Compétences requises
	fourni par le service Amazon Cognito.	
Testez la configuration du service d'authentification.	Dans le simulateur iOS, procédez comme suit : 1. Créez un nouveau compte dans l'application en utilisant une adresse e-mail réelle. Un code de vérification est ensuite envoyé à l'adresse e-mail enregistrée. 2. Vérifiez le compte configuré à l'aide du code que vous recevez dans l'e-mail de vérification. 3. Entrez le nom d'utilisateur et le mot de passe que vous avez créés. Choisissez ensuite Se connecter. Un écran de bienvenue apparaît. **Note** Vous pouvez également ouvrir la console Amazon Cognito et vérifier si un nouvel utilisateur a été créé dans le pool d'identités ou non.	Développeur d’applications

Connectez une AppSync API AWS et une base de données DynamoDB à l'application

Tâche	Description	Compétences requises
Créez une AppSync API AWS et une base de données DynamoDB.	1. Ajoutez une AppSync API AWS à votre application et provisionnez automatiquement une base de données DynamoDB en exécutant la commande Amplify CLI suivante depuis le répertoire racine du projet : `amplify add api` 2. Une invite s'affiche vous demandant de fournir des informations sur les paramètres de configuration de l'API et de la base de données. Entrez les informations requises en fonction de votre cas d'utilisation. Ensuite, appuyez sur Entrée. La CLI Amplify ouvre le fichier de schéma GraphQL dans votre éditeur de texte. Pour la configuration de ToDoList l'application utilisée dans ce modèle, appliquez l'exemple de configuration suivant.	Développeur d’applications

Tâche	Description	Compétences requises

	Exemples de paramètres de configuration d'API et de base de données
	
	`? Please select from one of the below mentioned services: \`
	`GraphQL`
	
	`? Provide API name: todolistamplify`
	
	`? Choose the default authorization type for the API \`
	`Amazon Cognito User Pool`
	
	`Do you want to use the default authentication and security configuration`
	
	`? Default configuration How do you want users to be able to sign in? \`
	`Username`
	
	`Do you want to configure advanced settings? \`
	`No, I am done.`
	
	`? Do you want to configure advanced settings for the GraphQL API \`
	`No, I am done.`
	
	`? Do you have an annotated GraphQL schema? \`	

Tâche	Description	Compétences requises

	No
	
	? Choose a schema
	template: \
	Single object with
	fields (e.g., “Todo”
	with ID, name,
	description)
	
	? Do you want to edit
	the schema now? \
	Yes
	
	Exemple de schéma GraphQL
	
	type Todo @model {
	id: ID!
	name: String!
	description: String
	}	

Tâche	Description	Compétences requises
Déployez l' AppSync API AWS.	1. Dans le répertoire racine du projet, exécutez la commande Amplify CLI suivante : `amplify push` 2. Une invite s'affiche pour vous demander de fournir des informations supplémentaires sur les paramètres de configuration de l'API et de la base de données. Entrez les informations requises en fonction de votre cas d'utilisation. Ensuite, appuyez sur Entrée. Votre application peut désormais interagir avec l' AppSync API AWS. Pour la configuration de ToDoList l'application utilisée dans ce modèle, appliquez l'exemple de configuration suivant. Exemple de paramètres de configuration de AppSync l'API AWS **Note** La configuration suivante crée l'API GraphQL dans AWS	Développeur d’applications

Tâche	Description	Compétences requises
	AppSync et une table Todo dans Dynamo DB. ? Are you sure you want to continue? Yes ? Do you want to generate code for your newly created GraphQL API Yes ? Choose the code generation language target javascript ? Enter the file name pattern of graphql queries, mutations and subscriptions src/graphql/**/*.js ? Do you want to generate/update all possible GraphQL operations - \ queries, mutations and subscriptions Yes ? Enter maximum statement depth \ [increase from default if your schema is deeply nested] 2	

Tâche	Description	Compétences requises
Connectez le frontend de l'application à l' AppSync API AWS.	Pour utiliser l'exemple d' ToDoList application fourni dans ce modèle, copiez le code du fichier App.js dans le ios-todo-app GitHub référenti el aws-amplify-react-native-. Intégrez ensuite l'exemple de code dans votre environne ment local. L'exemple de code fourni dans le fichier App.js du référenti el effectue les opérations suivantes : • Affiche le formulaire de création d'un ToDo article avec les champs Titre et Description • Affiche la liste des tâches à effectuer (titre et descripti on) • Publie et récupère des données à l'aide de méthodes `aws-amplify`	Développeur d’applications

Ressources connexes

- AWS Amplify
- Amazon Cognito
- AWS AppSync
- Amazon DynamoDB
- React (documentation React)

Gestion des locataires sur plusieurs produits SaaS sur un seul plan de contrôle

Créée par Ramanna Avancha (AWS), Jenifer Pascal (AWS), Kishan Kavala (AWS) et Anusha Mandava (AWS)

Récapitulatif

Ce modèle montre comment gérer le cycle de vie des clients sur plusieurs produits SaaS (Software as a Service) sur un seul plan de contrôle dans le cloud AWS. L'architecture de référence fournie peut aider les entreprises à réduire la mise en œuvre de fonctionnalités redondantes et partagées dans leurs produits SaaS individuels et à améliorer l'efficacité de la gouvernance à grande échelle.

Les grandes entreprises peuvent proposer plusieurs produits SaaS dans différentes unités commerciales. Ces produits doivent souvent être fournis pour être utilisés par des locataires externes à différents niveaux d'abonnement. Sans solution mutualisée, les administrateurs informatiques doivent passer du temps à gérer des fonctionnalités indifférenciées entre plusieurs SaaS APIs, au lieu de se concentrer sur le développement des fonctionnalités de base du produit.

La solution de locataire commun proposée dans ce modèle peut aider à centraliser la gestion de nombreuses fonctionnalités des produits SaaS partagés d'une entreprise, notamment les suivantes :

- Sécurité
- Provisionnement pour les locataires
- Stockage des données des locataires
- Communications avec les locataires
- Gestion des produits
- Enregistrement et surveillance des métriques

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Connaissance d'Amazon Cognito ou d'un fournisseur d'identité (IdP) tiers
- Connaissance d'Amazon API Gateway

- Connaissance d'AWS Lambda
- Connaissance d'Amazon DynamoDB
- Connaissance d'AWS Identity and Access Management (IAM)
- Connaissance d'AWS Step Functions
- Connaissance d'AWS CloudTrail et d'Amazon CloudWatch
- Connaissance des bibliothèques et du code Python
- Connaissance du SaaS APIs, notamment des différents types d'utilisateurs (organisations, locataires, administrateurs et utilisateurs d'applications), des modèles d'abonnement et des modèles d'isolation des locataires
- Connaissance des exigences SaaS multi-produits et des abonnements multi-locataires de votre entreprise

Limites

- Les intégrations entre la solution mutualisée et les produits SaaS individuels ne sont pas couvertes par ce modèle.
- Ce modèle déploie le service Amazon Cognito uniquement dans une seule région AWS.

Architecture

Pile technologique cible

- Amazon API Gateway
- Amazon Cognito
- AWS CloudTrail
- Amazon CloudWatch
- Amazon DynamoDB
- IAM
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon Simple Notification Service (Amazon SNS)
- Fonctions d'AWS Step

Architecture cible

Le schéma suivant montre un exemple de flux de travail pour gérer le cycle de vie des locataires sur plusieurs produits SaaS sur un seul plan de contrôle dans le cloud AWS.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur AWS lance le provisionnement des locataires, le provisionnement des produits ou des actions liées à l'administration en appelant un point de terminaison API Gateway.
2. L'utilisateur est authentifié par un jeton d'accès extrait d'un groupe d'utilisateurs Amazon Cognito ou d'un autre IdP.
3. Les tâches d'approvisionnement ou d'administration individuelles sont exécutées par des fonctions Lambda intégrées aux points de terminaison de l'API API Gateway.
4. L'administration APIs de la solution commune (pour les locataires, les produits et les utilisateurs) rassemble tous les paramètres d'entrée, en-têtes et jetons requis. L'administration APIs invoque ensuite les fonctions Lambda associées.
5. Les autorisations IAM pour les fonctions d'administration APIs et Lambda sont validées par le service IAM.
6. Les fonctions Lambda stockent et extraient les données des catalogues (pour les locataires, les produits et les utilisateurs) dans DynamoDB et Amazon S3.
7. Une fois les autorisations validées, un flux de travail AWS Step Functions est invoqué pour effectuer une tâche spécifique. L'exemple du diagramme montre un flux de travail de provisionnement des locataires.
8. Les tâches individuelles du flux de travail AWS Step Functions sont exécutées dans un flux de travail prédéterminé (machine à états).
9. Toutes les données essentielles nécessaires à l'exécution de la fonction Lambda associée à chaque tâche de flux de travail sont extraites de DynamoDB ou d'Amazon S3. D'autres ressources AWS devront peut-être être mises en service à l'aide d'un CloudFormation modèle AWS.
10. Le cas échéant, le flux de travail envoie une demande de mise à disposition de ressources AWS supplémentaires pour un produit SaaS spécifique sur le compte AWS de ce produit.
11. Lorsque la demande aboutit ou échoue, le flux de travail publie la mise à jour du statut sous forme de message sur une rubrique Amazon SNS.
12. Amazon SNS est abonné à la rubrique Amazon SNS du flux de travail Step Functions.
13. Amazon SNS renvoie ensuite la mise à jour de l'état du flux de travail à l'utilisateur AWS.

14 Les journaux des actions de chaque service AWS, y compris une piste d'audit des appels d'API, sont envoyés à CloudWatch. Des règles et des alarmes spécifiques peuvent être configurées CloudWatch pour chaque cas d'utilisation.

15 Les journaux sont archivés dans des compartiments Amazon S3 à des fins d'audit.

Automatisation et mise à l'échelle

Ce modèle utilise un CloudFormation modèle pour automatiser le déploiement de la solution mutualisée. Le modèle peut également vous aider à augmenter ou à réduire rapidement les ressources associées.

Pour plus d'informations, consultez la section Utilisation des CloudFormation modèles AWS dans le guide de CloudFormation l'utilisateur AWS.

Outils

Services AWS

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour les applications Web et mobiles.
- AWS vous CloudTrail aide à auditer la gouvernance, la conformité et le risque opérationnel de votre compte AWS.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à approvisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise.

Bonnes pratiques

Dans ce modèle, la solution utilise un plan de contrôle unique pour gérer l'intégration de plusieurs locataires et pour fournir un accès à plusieurs produits SaaS. Le plan de contrôle permet aux utilisateurs administratifs de gérer quatre autres plans spécifiques aux fonctionnalités :

- Avion de sécurité
- Plan de flux de travail
- Plan de communication
- Plan de journalisation et de surveillance

Épopées

Configuration du plan de sécurité

Tâche	Description	Compétences requises
Définissez les exigences relatives à votre plateforme SaaS à locataires multiples.	Établissez des exigences détaillées pour les éléments suivants : • Locataires • Users • Rôles • Produits SaaS • Abonnements • Echanges de profils	Architecte cloud, administrateur système AWS
Configurez le service Amazon Cognito.	Suivez les instructions de la section Getting started with	Architecte du cloud

Tâche	Description	Compétences requises
	Amazon Cognito Developer Guide du développeur Amazon Cognito.	
Configurez les politiques IAM requises.	Créez les politiques IAM requises pour votre cas d'utilisation. Mappez ensuite les politiques aux rôles IAM dans Amazon Cognito. Pour plus d'informations, consultez la section Gestion de l'accès à l'aide de politiques et de contrôle d'accès basé sur les rôles dans le manuel Amazon Cognito Developer Guide.	Administrateur cloud, architecte cloud, sécurité AWS IAM
Configurez les autorisations d'API requises.	Configurez les autorisations d'accès à API Gateway à l'aide des rôles et politiques IAM et des autorisateurs Lambda. Pour obtenir des instructions, consultez les sections suivantes du manuel Amazon API Gateway Developer Guide : • Contrôler l'accès à une API avec des autorisations IAM • Utiliser les autorisateurs Lambda d'API Gateway	Administrateur cloud, architecte cloud

Configuration du plan de données

Tâche	Description	Compétences requises
Créez les catalogues de données requis.	1. Créez des tables DynamoDB pour stocker les données des catalogues utilisateur. Assurez-vous d'inclure les attributs et les rôles des utilisateurs. Assurez-vous également de modéliser les données dans les tables du catalogue afin de conserver les attributs obligatoires et facultatifs pour chaque utilisateur et chaque rôle. 2. Créez des tables DynamoDB pour stocker les données des catalogues de produits. Assurez-vous de modéliser les cas d'utilisation spécifiques de vos produits SaaS. 3. Créez des tables DynamoDB pour stocker les données des catalogues clients. Assurez-vous de configurer des modèles d'abonnement pour les locataires, les produits et les licences pour les abonnements multi-SaaS et les tags.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Configuration de DynamoDB dans le manuel du développeur Amazon DynamoDB.	

Configuration du plan de contrôle

Tâche	Description	Compétences requises
Créez des fonctions Lambda et une API Gateway APIs pour exécuter les tâches du plan de contrôle requises.	Créez des fonctions Lambda et une API Gateway distinctes APIs pour ajouter, supprimer et gérer les éléments suivants : • Users • Locataires • Produits Pour plus d'informations, consultez la section Utilisation d'AWS Lambda avec Amazon API Gateway dans le manuel du développeur AWS Lambda.	Développeur d’applications

Configuration du plan de flux de travail

Tâche	Description	Compétences requises
Identifiez les tâches que les flux de travail AWS Step Functions doivent exécuter.	Identifiez et documentez les exigences détaillées du flux	Propriétaire de l'application

Tâche	Description	Compétences requises
	de travail AWS Step Functions pour les éléments suivants : • Users • Locataires • Produits **⚠ Important** Assurez-vous que les principales parties prenantes approuvent les exigences.	

Tâche	Description	Compétences requises
Créez les flux de travail AWS Step Functions requis.	1. Créez les flux de travail requis pour les utilisateurs, les locataires et les produits dans AWS Step Functions . Pour plus d'informations, consultez le guide du développeur AWS Step Functions. 2. Identifiez les mécanismes de gestion des nouvelles tentatives et des erreurs. Pour plus d'informations, consultez la section Gestion des erreurs, des nouvelles tentatives et ajout d'alertes aux machines Step Function State sur le blog AWS. 3. Implémentez les étapes du flux de travail à l'aide des fonctions Lambda. Pour obtenir des instructi ons, consultez la section Création d'une machine d'état Step Functions utilisant Lambda dans le guide du développeur AWS Step Functions. 4. Intégrez tous les services externes à AWS Step Functions selon vos besoins. 5. Conservez le statut de chaque flux de travail dans	Développeur d'applications, responsable de la création

Tâche	Description	Compétences requises
	une table DynamoDB et communiquez le statut de chaque flux de travail à l'aide d'Amazon SNS.	

Configuration du plan de communication

Tâche	Description	Compétences requises
Créez des rubriques Amazon SNS.	Créez des rubriques Amazon SNS pour recevoir des notifications sur les points suivants : • Statuts du flux de travail • Erreurs • Nouvelle tentative Pour plus d'informations, consultez la rubrique Création d'un réseau SNS dans le manuel Amazon SNS Developer Guide.	Propriétaire de l'application, architecte cloud
Abonnez des points de terminaison à chaque rubrique Amazon SNS.	Pour recevoir des messages publiés sur une rubrique Amazon SNS, vous devez abonner un point de terminaison à chaque rubrique. Pour plus d'informations, consultez la section Abonnement à une rubrique	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	Amazon SNS dans le manuel du développeur Amazon SNS.	

Configuration du plan de journalisation et de surveillance

Tâche	Description	Compétences requises
Activez la journalisation pour chaque composant de la solution mutualisée.	Activez la journalisation au niveau des composants pour chaque ressource de la solution mutualisée que vous avez créée. Pour obtenir des instructions, veuillez consulter les sections suivantes : • Comment activer les CloudWatch journaux pour résoudre les problèmes liés à mon API REST ou à mon API API WebSocket API Gateway ? (Centre de connaissances AWS) • Journalisation à l'aide de CloudWatch journaux (AWS Step Functions Developer Guide) • Journalisation des fonctions AWS Lambda en Python (Guide du développeur AWS Lambda) • Journalisation et surveillance dans Amazon Cognito	Développeur d'applications, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
	(Guide du développeur Amazon Cognito) • Surveillance avec Amazon CloudWatch (Guide du développeur Amazon DynamoDB) **Note** Vous pouvez consolider les journaux de chaque ressource dans un compte de journalisation centralisé en utilisant des politiques IAM. Pour plus d'informations, consultez la section Journalisation centralisée et mesures de sécurité pour plusieurs comptes.	

Fournir et déployer la solution Common Tenant

Tâche	Description	Compétences requises
Créez des CloudFormation modèles.	Automatisez le déploiement et la maintenance de la solution commune complète et de tous ses composants à l'aide CloudFormation de modèles.	Développeur d'applications, DevOps ingénieur, CloudFormation développeur

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez le guide de CloudFormation l'utilisateur AWS.	

Ressources connexes

- Contrôlez l'accès à une API REST en utilisant les groupes d'utilisateurs Amazon Cognito comme autorisateur (Amazon API Gateway Developer Guide)
- Utiliser les autorisateurs Lambda d'API Gateway (Amazon API Gateway Developer Guide)
- Groupes d'utilisateurs Amazon Cognito (Guide du développeur Amazon Cognito)
- CloudWatch Console entre comptes et entre régions (Amazon CloudWatch User Guide)

Création d'une EventBridge connexion Amazon entre comptes dans une organisation

Créée par Sam Wilson (AWS) et Robert Stone (AWS)

Récapitulatif

Les grands systèmes distribués utilisent Amazon EventBridge pour communiquer les changements d'état entre les différents comptes Amazon Web Services (AWS) d'une AWS Organizations organisation. Cependant, EventBridge il est généralement en mesure de cibler uniquement les terminaux ou les consommateurs. Compte AWS L'exception concerne un bus d'événements sur un autre compte. Ce bus d'événements est une cible valide. Pour utiliser les événements d'un bus d'événements dans un autre compte, les événements doivent être transférés du bus d'événements du compte source vers le bus d'événements du compte de destination. Pour éviter les difficultés liées à la gestion d'événements critiques entre applications au sein de différentes applications Comptes AWS, utilisez l'approche recommandée présentée dans ce modèle.

Ce modèle illustre comment implémenter une architecture axée sur les événements impliquant plusieurs acteurs EventBridge Comptes AWS au sein d'une AWS Organizations organisation. Le modèle utilise AWS Cloud Development Kit (AWS CDK) Toolkit et AWS CloudFormation.

EventBridge propose un bus d'événements sans serveur qui vous aide à recevoir, filtrer, transformer, acheminer et diffuser des événements. Composant essentiel des architectures axées sur les événements, il EventBridge permet de séparer les producteurs de messages des consommateurs de ces messages. Dans un seul compte, c'est simple. Une structure à comptes multiples nécessite des considérations supplémentaires pour que les événements du bus d'événements d'un compte soient consommés dans d'autres comptes de la même organisation.

Pour plus d'informations sur les considérations spécifiques aux comptes pour les producteurs et les consommateurs, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Une AWS Organizations organisation avec au moins deux associés Comptes AWS
- Un rôle AWS Identity and Access Management (IAM) dans les deux cas Comptes AWS qui vous permet de provisionner une infrastructure dans les deux en Comptes AWS utilisant AWS CloudFormation

- Git installé localement
- AWS Command Line Interface (AWS CLI) installé localement
- AWS CDK installé localement et amorcé dans les deux Comptes AWS

Versions du produit

Ce modèle a été créé et testé à l'aide des outils et versions suivants :

- AWS CDK Boîte à outils 2.126.0
- Node.js 18,19,0
- npm 10.2.3
- Python 3.12

Ce modèle devrait fonctionner avec n'importe quelle version de AWS CDK v2 ou npm. Les versions 13.0.0 à 13.6.0 de Node.js ne sont pas compatibles avec. AWS CDK

Architecture

Architecture cible

Le schéma suivant montre le flux de travail architectural permettant de transférer un événement depuis un compte et de le consommer sur un autre compte.

Le flux de travail comprend les étapes suivantes :

1. La AWS Lambda fonction Producteur du compte Source place un événement sur le bus d' EventBridge événements du compte.
2. La EventBridge règle multi-comptes achemine l'événement vers un bus d' EventBridge événements dans le compte Destination.
3. Le bus EventBridge d'événements du compte Destination possède une règle Lambda cible qui invoque la fonction Consumer Lambda.

Une bonne pratique consiste à utiliser une file d'attente de lettres mortes (DLQ) pour gérer les invocations échouées de la fonction Consumer Lambda. Cependant, le DLQ a été omis de cette solution pour des raisons de clarté. Pour en savoir plus sur la façon d'implémenter une DLQ dans

vos flux de travail et d'améliorer la capacité de vos flux de travail à se rétablir en cas de défaillance, consultez le billet de blog Implementation AWS Lambda error handling patterns.

Automatisation et mise à l'échelle

AWS CDK provisionne automatiquement l'architecture requise. EventBridge peut atteindre des milliers d'enregistrements par seconde en fonction du Région AWS. Pour plus d'informations, consultez la documentation relative EventBridge aux quotas Amazon.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code. Ce modèle utilise le AWS CDK Toolkit, un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre AWS CDK application.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, AWS Lambda des fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

Autres outils

- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.
- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub cross-account-eventbridge-in-organization.

Bonnes pratiques

Pour connaître les meilleures pratiques en matière d' EventBridgeutilisation, consultez les ressources suivantes :

- Bonnes pratiques relatives aux modèles EventBridge d'événements Amazon
- Bonnes pratiques lors de la définition de règles dans Amazon EventBridge

Épopées

Préparez votre environnement AWS CDK de déploiement local

Tâche	Description	Compétences requises
Configurez les informations d'identification locales pour le compte source et le compte de destination.	Consultez la section Configuration d'une nouvelle configuration et de nouvelles informations d'identification, et utilisez la méthode d'authentification et d'identification la plus adaptée à votre environnement. ⚠ Important Assurez-vous de configurer l'authentification AWS CLI du compte source et du compte de destination. Ces instructions supposent que vous avez configuré deux profils AWS localemen	Développeur d’applications

Tâche	Description	Compétences requises
	t : `sourceAccount` et`destinationAccount` .	

Bootstrap les deux Comptes AWS.	Pour démarrer les comptes, exécutez les commandes suivantes :
	`cdk bootstrap --profile sourceAccount`
	`cdk bootstrap --profile destinationAccount`
		Développeur d'applications

Clonez le code du modèle.	Pour cloner le dépôt, exécutez la commande suivante :
	`git clone git@github.com:aws-samples/aws-cdk-examples.git`
	Ensuite, remplacez le répertoire par le dossier du projet nouvellement cloné :
	`cd aws-cdk-examples/python/cross-account-eventbridge-in-organization`
		Développeur d'applications

ProducerStack Déployer sur le compte source

Tâche	Description	Compétences requises
Modifiez `cdk.json` avec vos informations AWS Organizations et celles de votre compte.	Dans le dossier racine du projet, apportez les modifications suivantes à `cdk.json` :	Développeur d'applications

Tâche	Description	Compétences requises
	• `organization_id` – L'identifiant Organizations des comptes impliqués dans votre déploiement • `event_bus _name` – `CrossAcco unt` , ou vous pouvez le renommer • `rules[].targets[]. arn` – L' Compte AWS identifiant du compte consommateur (compte de destination)	
Déployez les ProducerStack ressources.	Exécutez la commande suivante depuis le répertoire racine du projet : `cdk deploy ProducerS tack --profile sourceAccount` Lorsque vous y êtes invité, acceptez les nouveaux rôles IAM et les autres autorisations liées à la sécurité créés via. AWS CloudFormation	Développeur d'applications

Tâche	Description	Compétences requises
Vérifiez que les ProducerStack ressources sont déployées.	Pour vérifier les ressources, procédez comme suit : 1. Sur le compte AWS Management Console for the Source, sélectionnez CloudFormation. 2. Dans la liste des piles, choisissez ProducerStack. 3. Dans l'onglet Stack Info, vérifiez que l'état de la pile est`CREATE_COMPLETE` . Dans l'onglet Ressources, passez éventuellement en revue les ressources configurées.	Développeur d’applications

ConsumerStack Déployer sur le compte de destination

Tâche	Description	Compétences requises
Déployez les ConsumerStack ressources.	Exécutez la commande suivante depuis le répertoire racine du projet : `cdk deploy ConsumerStack --profile destinationAccount` Lorsque vous y êtes invité, acceptez les nouveaux rôles IAM et les autres autorisations liées à la sécurité créés via. AWS CloudFormation	Développeur d’applications

Tâche	Description	Compétences requises
Vérifiez que les ConsumerStack ressources sont déployées	1. Sur la console du compte Destination, choisissez CloudFormation. 2. Dans la liste des piles, choisissez ConsumerStack. 3. Dans l'onglet Stack Info, vérifiez que l'état de la pile est`CREATE_COMPLETE` . Dans l'onglet Ressources, passez éventuellement en revue les ressources configurées.	Développeur d’applications

Produisez et consommez des événements

Tâche	Description	Compétences requises
Appelez la fonction Producer Lambda.	1. Sur la console du compte Source, choisissez Lambda. 2. Dans la liste des fonctions, choisissez ProducerStack-ProducerLambda XXXX (XXXX représente une séquence de caractères générée automatiquement par AWS CDK). 3. Choisissez l’onglet Test. 4. Dans la section Test event, sélectionnez Test. Le contenu de la zone de texte Event JSON peut être n'importe quel JSON	Développeur d’applications

Tâche	Description	Compétences requises
	valide fourni à la fonction Lambda en tant que charge utile. Dans ce cas, le JSON fourni par défaut est suffisant. 5. Vérifiez que le message Executing function : successful apparaît dans une bannière verte au-dessus de la section Test event.	

Tâche	Description	Compétences requises
Vérifiez que l'événement a bien été reçu.	1. Sur la console du compte Destination, choisissez Lambda. 2. Dans la liste des fonctions, choisissez ConsumerStack- ConsumerLambda XXXX (XXXX représente une séquence de caractères générée automatiquement par AWS CDK). 3. Choisissez l'onglet Surveiller. 4. Dans la section Moniteur, choisissez Afficher CloudWatch les journaux. 5. Dans le nouvel onglet, choisissez le nom du flux de journal le plus récent. 6. Vérifiez qu'une instruction de journal telle que la suivante apparaît : `[DEBUG] 2024-04-08T19:08:10.091Z 9c16844a-f9de-444d-b621-86afe64d4cc8 Event: {'version':'0', 'id':'0b9faa96-973f-8be2-ecf8-75e4f328b980', 'detail-type':'TestType', 'source':'Producer', 'account'`	Développeur d'applications

Tâche	Description	Compétences requises
	`:'XXXXXXXXXXXX', 'time':'2024-04-08 T19:08:09Z', 'region':'us-east-1', 'resources': [], 'detail': {'key1':'value1', 'key2':'value2', 'key3':'value3'}}`	

Nettoyage

Tâche	Description	Compétences requises
Détruisez les ConsumerStack ressources.	Si vous utilisez ce modèle comme test, nettoyez les ressources déployées pour éviter d'encourir des coûts supplémentaires. Exécutez la commande suivante depuis le répertoire racine du projet : `cdk destroy ConsumerStack --profile destinationAccount` Vous serez invité à confirmer la suppression de la pile.	Développeur d’applications
Détruisez les ProducerStack ressources.	Exécutez la commande suivante depuis le répertoire racine du projet :	Développeur d’applications

Tâche	Description	Compétences requises
	`cdk destroy ProducerStack --profile sourceAccount` Vous serez invité à confirmer la suppression de la pile.	

Résolution des problèmes

Problème	Solution
Aucun événement n'a été reçu sur le compte Destination.	1. Vérifiez que l'identifiant Organizations fourni est correct. 2. Vérifiez que le compte Source fait partie de l'organisation fournie. 3. Vérifiez que les règles du bus d'événements du compte source correspondent aux informations correctes du compte destination.
L'appel d'une fonction Lambda depuis la console renvoie l'erreur suivante : `User: arn:aws:iam::123456789012:user/XXXXX is not authorized to perform: lambda:Invoke`	Contactez votre Compte AWS administrateur pour obtenir les autorisations `lambda:Invoke` d'action appropriées sur la fonction `ProducerStack-ProducerLambdaXXXX` Lambda.

Ressources connexes

Références

- AWS Organizations Guide de l'utilisateur
- Modèles d' EventBridge événements Amazon
- Règles sur Amazon EventBridge

Tutoriels et vidéos

- Tutoriel : Création et configuration d'une organisation
- AWS re:Invent 2023 - Modèles avancés axés sur les événements avec Amazon (01-R) EventBridge COM3

Informations supplémentaires

Règle du producteur

Dans le compte Source, un bus d' EventBridge événements est créé pour accepter les messages des producteurs (comme indiqué dans la section Architecture). Une règle associée aux autorisations IAM est créée sur ce bus d'événements. Les règles ciblent le bus d' EventBridge événements dans le compte Destination selon la `cdk.json` structure suivante :

```
"rules": [
  {
    "id": "CrossAccount",
    "sources": ["Producer"],
    "detail_types": ["TestType"],
    "targets": [
      {
        "id": "ConsumerEventBus",
        "arn": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount"
      }
    ]
  }
]
```

Pour chaque bus d'événements consommant, le modèle d'événement et le bus d'événements cible doivent être inclus.

Schéma d'événement

Les modèles d'événements filtrent les événements auxquels cette règle s'applique. Aux fins de cet exemple, les sources d'événements et l'enregistrement `detail_types` identifient les événements à transmettre du bus d'événements du compte source au bus d'événements du compte de destination.

Bus de l'événement cible

Cette règle cible un bus d'événements qui existe dans un autre compte. Le nom complet `arn` (Amazon Resource Name) est nécessaire pour identifier de manière unique le bus d'événements cible, et `id` il s'agit de l'ID logique utilisé par AWS CloudFormation. Il n'est pas nécessaire que le bus d'événements cible existe réellement au moment de la création de la règle cible.

Considérations spécifiques au compte de destination

Dans le compte Destination, un bus d' EventBridge événements est créé pour recevoir les messages du bus d'événements du compte source. Pour autoriser la publication d'événements depuis le compte Source, vous devez créer une politique basée sur les ressources :

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowOrgToPutEvents",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "events:PutEvents",
    "Resource": "arn:aws:events:us-east-2:012345678901:event-bus/CrossAccount",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "o-XXXXXXXXX"
      }
    }
  }]
}
```

Il est particulièrement important d'accorder cette `events:PutEvents` autorisation, qui permet à tout autre compte de la même organisation de publier des événements sur ce bus d'événements. Le paramétrage `aws:PrincipalOrgId` en tant qu'ID d'organisation accorde les autorisations nécessaires.

Schéma d'événement

Vous pouvez modifier le modèle d'événement inclus en fonction de votre cas d'utilisation :

```
rule = events.Rule(
    self,
    self.id + 'Rule' + rule_definition['id'],
    event_bus=event_bus,
    event_pattern=events.EventPattern(
        source=rule_definition['sources'],
```

```
        detail_type=rule_definition['detail_types'],
    )
)
```

Pour réduire le traitement inutile, le modèle d'événements doit spécifier que seuls les événements devant être traités par le compte Destination sont transmis au bus d'événements du compte Destination.

Politique basée sur les ressources

Cet exemple utilise l'ID de l'organisation pour contrôler les comptes autorisés à placer des événements sur le bus d'événements du compte Destination. Envisagez d'utiliser une politique plus restrictive, telle que la spécification du compte source.

EventBridge quotas

Tenez compte des quotas suivants :

- Le quota par défaut est de 300 règles par bus d'événements. Cela peut être étendu si nécessaire, mais il doit s'adapter à la plupart des cas d'utilisation.
- Le maximum autorisé est de cinq cibles par règle. Nous recommandons aux architectes d'applications d'utiliser une règle distincte pour chaque compte de destination afin de permettre un contrôle précis du modèle d'événements.

Fournissez des enregistrements DynamoDB à Amazon S3 à l'aide de Kinesis Data Streams et Firehose avec AWS CDK

Créée par Shashank Shrivastava (AWS) et Daniel Matuki da Cunha (AWS)

Récapitulatif

Ce modèle fournit un exemple de code et une application permettant de transmettre des enregistrements d'Amazon DynamoDB à Amazon Simple Storage Service (Amazon S3) à l'aide d'Amazon Kinesis Data Streams et d'Amazon Data Firehose. L'approche du modèle utilise des constructions AWS Cloud Development Kit (AWS CDK) L3 et inclut un exemple de la manière d'effectuer une transformation des données AWS Lambda avant que les données ne soient livrées au compartiment S3 cible sur le cloud Amazon Web Services (AWS).

Kinesis Data Streams enregistre les modifications apportées au niveau des éléments dans les tables DynamoDB et les réplique dans le flux de données Kinesis requis. Vos applications peuvent accéder au flux de données Kinesis et afficher les modifications au niveau élément en quasi-temps réel. Kinesis Data Streams donne également accès à d'autres services Amazon Kinesis, tels que Firehose et Amazon Managed Service pour Apache Flink. Cela signifie que vous pouvez créer des applications qui fournissent des tableaux de bord en temps réel, génèrent des alertes, mettent en œuvre des prix et des publicités dynamiques et effectuent des analyses de données sophistiquées.

Vous pouvez utiliser ce modèle pour vos cas d'utilisation en matière d'intégration de données. Par exemple, les véhicules de transport ou les équipements industriels peuvent envoyer de gros volumes de données vers une table DynamoDB. Ces données peuvent ensuite être transformées et stockées dans un lac de données hébergé dans Amazon S3. Vous pouvez ensuite interroger et traiter les données et prévoir tout défaut potentiel en utilisant des services sans serveur tels qu'Amazon Athena, Amazon Redshift Spectrum, Amazon Rekognition et. AWS Glue

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Command Line Interface (AWS CLI), installé et configuré. Pour plus d'informations, consultez la section Mise en route avec le AWS CLI dans la AWS CLI documentation.
- Node.js (18.x+) et npm, installés et configurés. Pour plus d'informations, consultez la section Téléchargement et installation de Node.js et de npm dans la `npm` documentation.

- aws-cdk (2.x+), installé et configuré. Pour plus d'informations, consultez la section Mise en route avec le AWS CDK dans la AWS CDK documentation.
- Le référentiel GitHub aws-dynamodb-kinesisfirehose-s3-ingestion, cloné et configuré sur votre machine locale.
- Exemples de données existants pour la table DynamoDB. Les données doivent utiliser le format suivant : `{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}`

Architecture

Le schéma suivant montre un exemple de flux de travail permettant de transférer des enregistrements de DynamoDB vers Amazon S3 à l'aide de Kinesis Data Streams et Firehose.

Le schéma suivant illustre le flux de travail suivant :

1. Les données sont ingérées à l'aide d'Amazon API Gateway en tant que proxy pour DynamoDB. Vous pouvez également utiliser n'importe quelle autre source pour ingérer des données dans DynamoDB.
2. Les modifications au niveau des articles sont générées en temps quasi réel dans Kinesis Data Streams pour être transmises à Amazon S3.
3. Kinesis Data Streams envoie les enregistrements à Firehose pour transformation et livraison.
4. Une fonction Lambda convertit les enregistrements d'un format d'enregistrement DynamoDB au format JSON, qui contient uniquement les noms et valeurs des attributs des éléments d'enregistrement.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure cloud AWS sous forme de code.
- AWS CDK Toolkit est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre AWS CDK application.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub aws-dynamodb-kinesisfirehose-s3-ingestion.

Épopées

Configuration et configuration de l'exemple de code

Tâche	Description	Compétences requises

Installez les dépendances.	Sur votre machine locale, installez les dépendances à partir des `package.json` fichiers des `sample-application` répertoires `pattern/aws-dynamodb-kinesisstreams-s3` et en exécutant les commandes suivantes :
	`cd <project_root>/pattern/aws-dynamodb-kinesisstreams-s3`
	`npm install && npm run build`
	`cd <project_root>/sample-application/`
	`npm install && npm run build`
		Développeur d'applications, AWS général

Tâche	Description	Compétences requises
Générez le CloudFormation modèle.	1. Exécutez la commande `cd <project_root>/sample-application/ .` 2. Exécutez la `cdk synth` commande pour générer le CloudFormation modèle. 3. La `AwsDynamodbKinesisfirehoseS3IngestionStack.template.json` sortie est stockée dans le `cdk.out` répertoire. 4. Utilisez AWS CDK ou AWS Management Console pour traiter le modèle dans CloudFormation.	Développeur d'applications, AWS général, AWS DevOps

Déployez les ressources

Tâche	Description	Compétences requises
Vérifiez et déployez les ressources.	1. Exécutez la `cdk diff` commande pour identifier les types de ressources créés par la AWS CDK construction. 2. Exécutez la `cdk deploy` commande pour déployer les ressources.	Développeur d'applications, AWS général, AWS DevOps

Ingérez des données dans la table DynamoDB pour tester la solution

Tâche	Description	Compétences requises

Ingérez vos exemples de données dans la table DynamoDB.	Envoyez une demande à votre table DynamoDB en exécutant la commande suivante dans : AWS CLI
	
	`aws dynamodb put-item --table-name <your_table_name> --item '{"<table_partition_key>": {"S": "<partition_key_ID>"},"MessageData":{"S": "<data>"}}'`
	
	exemple :
	
	`aws dynamodb put-item --table-name SourceData_table --item '{"SourceDataId": {"S": "123"},"MessageData":{"S": "Hello World"}}'`
	
	Par défaut, le `put-item` ne renvoie aucune valeur en sortie si l'opération réussit. Si l'opération échoue, elle renvoie une erreur. Les données sont stockées dans DynamoDB puis envoyées
		Développeur d’applications

Tâche	Description	Compétences requises
	à Kinesis Data Streams et Firehose. **Note** Vous utilisez différent es approches pour ajouter des données dans une table DynamoDB. Pour plus d'informations, consultez la section Charger des données dans des tables dans la documentation DynamoDB.	
Vérifiez qu'un nouvel objet est créé dans le compartiment S3.	Connectez-vous au compartim ent S3 AWS Management Console et surveillez-le pour vérifier qu'un nouvel objet a été créé avec les données que vous avez envoyées. Pour plus d'informations, consultez GetObjectla documentation Amazon S3.	Développeur d'applications, AWS général

Nettoyage des ressources

Tâche	Description	Compétences requises
Nettoyez les ressources.	Exécutez la `cdk destroy` commande pour supprimer	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	toutes les ressources utilisées par ce modèle.	

Ressources connexes

- s-3 static-site-stack .ts (GitHub dépôt)
- aws-apigateway-dynamodb module (GitHub référentiel)
- aws-kinesisstreams-kinesisfirehose-sModule 3 (GitHub référentiel)
- Modifier la capture des données pour DynamoDB Streams (documentation DynamoDB)
- Utilisation de Kinesis Data Streams pour capturer les modifications apportées à DynamoDB (documentation DynamoDB)

Implémentez la gestion des versions d'API basée sur les chemins en utilisant des domaines personnalisés dans Amazon API Gateway

Créée par Corey Schnedl (AWS), Anbazhagan Ponnuswamy (AWS), Marcelo Barbosa (AWS), Gaurav Samudra (AWS), Mario Lopez Martinez (AWS) et Abhilash Vinod (AWS)

Récapitulatif

Ce modèle montre comment vous pouvez utiliser la fonctionnalité de mappage d'API des domaines personnalisés pour implémenter une solution de gestion des versions d'API basée sur les chemins pour Amazon API Gateway.

Amazon API Gateway est un service entièrement géré que vous pouvez utiliser pour créer, publier, gérer, surveiller et sécuriser APIs à n'importe quelle échelle. En utilisant la fonctionnalité de domaine personnalisé du service, vous pouvez créer des noms de domaine personnalisés plus simples et plus intuitifs URLs que vous pouvez fournir aux utilisateurs de vos API. Vous pouvez utiliser les mappages d'API pour connecter les étapes d'API à un nom de domaine personnalisé. Après avoir créé un nom de domaine et configuré les enregistrements DNS, vous utilisez les mappages d'API pour envoyer du trafic vers vous APIs via votre nom de domaine personnalisé.

Une fois qu'une API est mise à la disposition du public, les consommateurs l'utilisent. À mesure qu'une API publique évolue, son contrat de service évolue également pour refléter les nouvelles fonctionnalités et capacités. Cependant, il n'est pas judicieux de modifier ou de supprimer des fonctionnalités existantes. Toute modification importante peut avoir un impact sur les applications du client et les interrompre lors de l'exécution. Le versionnement des API est important pour éviter de rompre la rétrocompatibilité et de rompre un contrat.

Vous avez besoin d'une stratégie claire pour le versionnement des API afin d'aider les consommateurs à les adopter. La gestion APIs des versions basée sur les chemins URLs est l'approche la plus simple et la plus couramment utilisée. Dans ce type de versionnement, les versions sont explicitement définies dans le cadre de l'API URIs. L'exemple suivant URLs montre comment un consommateur peut utiliser l'URI pour spécifier une version d'API pour sa demande :

```
https://api.example.com/api/v1/orders

https://api.example.com/api/v2/orders

https://api.example.com/api/vX/orders
```

Ce modèle utilise le AWS Cloud Development Kit (AWS CDK) pour créer, déployer et tester un exemple d'implémentation d'une solution de version évolutive basée sur les chemins pour votre API. AWS CDK est un framework de développement de logiciels open source permettant de modéliser et de provisionner les ressources de vos applications cloud à l'aide de langages de programmation familiers.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- La propriété d'un domaine est requise pour utiliser le référentiel d'exemples de ce modèle et pour utiliser les fonctionnalités de domaine personnalisées d'Amazon API Gateway. Vous pouvez utiliser Amazon Route 53 pour créer et gérer les domaines de votre organisation. Pour plus d'informations sur l'enregistrement ou le transfert d'un domaine avec Route 53, consultez la section Enregistrement de nouveaux domaines dans la documentation Route 53.
- Avant de configurer un nom de domaine personnalisé pour une API, vous devez disposer d'un certificat SSL/TLS. AWS Certificate Manager
- Vous devez créer ou mettre à jour l’enregistrement de ressource de votre fournisseur DNS pour le mapper au point de terminaison de votre API. Sans un tel mappage, les demandes d'API liées au nom de domaine personnalisé ne peuvent pas atteindre API Gateway.

Limites

- Les noms de domaine personnalisés ne sont pas pris en charge pour les domaines privés APIs.
- Un nom de domaine personnalisé doit être unique au sein d'un Région AWS ensemble Comptes AWS.
- Pour configurer des mappages d’API à plusieurs niveaux, vous devez utiliser un nom de domaine personnalisé régional et la politique de sécurité TLS 1.2.
- Dans un mappage d'API, le nom de domaine personnalisé et le nom de domaine mappé APIs doivent être identiques Compte AWS.
- Les mappages d'API ne doivent contenir que des lettres, des chiffres et les caractères suivants : `$-_.+!*'()/`
- La longueur maximale du chemin d’un mappage d’API est de 300 caractères.
- Vous pouvez disposer de 200 mappages d’API à plusieurs niveaux pour chaque nom de domaine.

- Vous ne pouvez APIs mapper HTTP à un nom de domaine personnalisé régional qu'avec la politique de sécurité TLS 1.2.
- Vous ne pouvez pas WebSocket APIs mapper vers le même nom de domaine personnalisé qu'une API HTTP ou une API REST.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Cet exemple d'implémentation est utilisé AWS CDK dans la TypeScript version 2.149.0.

Architecture

Le schéma suivant montre le flux de travail de l'architecture.

Le diagramme illustre les éléments suivants :

1. L'utilisateur de l'API envoie une demande à Amazon API Gateway avec un nom de domaine personnalisé.
2. API Gateway achemine dynamiquement la demande de l'utilisateur vers une instance et une étape appropriées d'API Gateway, en fonction du chemin indiqué dans l'URL de la demande. Le tableau suivant montre un exemple de la manière dont les différents chemins basés sur des URL peuvent être routés vers des étapes spécifiques pour différentes instances d'API Gateway.

« Hello, World! »	Étape	Chemin	Point final par défaut
Calcul APIv1	api	apiv1	Activées
Calcul APIv2	api	apiv2	Activées
Calcul APIv X	api	API Vx	Activées

3. L'instance API Gateway de destination traite la demande et renvoie le résultat à l'utilisateur.

Automatisation et mise à l'échelle

Nous vous recommandons d'utiliser des AWS CloudFormation piles distinctes pour chaque version de votre API. Avec cette approche, vous pouvez obtenir une isolation complète entre le backend vers APIs lequel la fonction de mappage d'API de domaine personnalisée peut être acheminée. L'avantage de cette approche est que différentes versions de votre API peuvent être déployées ou supprimées indépendamment sans risque de modification d'une autre API. Cette approche augmente la résilience grâce à l'isolation des CloudFormation piles. En outre, il vous fournit différentes options de back-end pour votre API AWS Lambda AWS Fargate, telles que les points de terminaison HTTP et les actions de. Services AWS

Vous pouvez utiliser des stratégies de branchement Git, telles que Gitflow, en combinaison avec des CloudFormation piles isolées pour gérer le code source déployé sur différentes versions de l'API. En utilisant cette option, vous pouvez gérer différentes versions de votre API sans avoir à dupliquer le code source pour les nouvelles versions. Avec Gitflow, vous pouvez ajouter des balises aux commits dans votre dépôt git au fur et à mesure que les versions sont effectuées. Par conséquent, vous disposez d'un instantané complet du code source associé à une version spécifique. Lorsque des mises à jour doivent être effectuées, vous pouvez extraire le code d'une version spécifique, effectuer des mises à jour, puis déployer le code source mis à jour sur la CloudFormation pile correspondant à la version majeure correspondante. Cette approche réduit le risque de rupture d'une autre version d'API, car chaque version de l'API possède un code source isolé et est déployée sur des CloudFormation piles distinctes.

Outils

Services AWS

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS Certificate Manager (ACM) vous aide à créer, à stocker et à renouveler les certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et vos applications. AWS
- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel open source permettant de définir votre infrastructure cloud dans le code et de la provisionner via ce dernier. AWS CloudFormation L'exemple d'implémentation de ce modèle utilise le AWS CDK in TypeScript. L'utilisation du AWS CDK in TypeScript utilise des outils familiers, notamment le TypeScript compilateur Microsoft (`tsc`), Node.js et le gestionnaire de packages de nœuds (`npm`). Si vous préférez, vous pouvez utiliser Yarn, bien que les exemples de ce modèle l'utilisentnpm.

Les modules qui composent la bibliothèque AWS Construct sont distribués via le `npm` référentiel npmjs.org.

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.
- AWS WAFest un pare-feu d'applications Web qui vous aide à surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources protégées de votre application Web.

Autres outils

- Bruno est un client de test d'API open source et convivial pour Git.
- cdk-nag est un utilitaire open source qui vérifie les meilleures pratiques des AWS CDK applications à l'aide de packs de règles.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub path-based-versioning-with-api-gateway.

Bonnes pratiques

- Utilisez un pipeline robuste d'intégration continue et de livraison continue (CI/CD) pour automatiser les tests et le déploiement de vos CloudFormation piles conçues avec le. AWS CDK Pour plus d'informations relatives à cette recommandation, consultez le guide AWS DevOps Well-Architected.
- AWS WAF est un pare-feu géré qui s'intègre facilement à des services tels qu'Amazon API Gateway. Bien qu'il AWS WAF ne s'agisse pas d'un composant nécessaire au bon fonctionnement de ce modèle de version, nous vous recommandons de l'inclure dans API Gateway en tant que bonne pratique AWS WAF de sécurité.
- Encouragez les utilisateurs d'API à passer régulièrement à la dernière version de votre API afin que les anciennes versions de votre API puissent être déconseillées et supprimées efficacement.
- Avant d'utiliser cette approche dans un environnement de production, implémentez un pare-feu et une stratégie d'autorisation pour votre API.

- Implémentez l'accès à la gestion de vos AWS ressources Compte AWS en utilisant le modèle d'accès avec le moindre privilège.
- Pour appliquer les meilleures pratiques et les recommandations de sécurité aux applications créées avec le AWS CDK, nous vous recommandons d'utiliser l'utilitaire cdk-nag.

Épopées

Préparez votre environnement local

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le référentiel d'applications d'exemple, exécutez la commande suivante : `git clone https://github.com/aws-samples/path-based-versioning-with-api-gateway`	Développeur d’applications
Accédez au référentiel cloné.	Pour accéder à l'emplacement du dossier du référentiel cloné, exécutez la commande suivante : `cd api-gateway-custom-domain-versioning`	Développeur d’applications
Installez les dépendances obligatoires.	Pour installer les dépendances requises, exécutez la commande suivante : `npm install`	Développeur d’applications

Déployer la pile CloudFormation de routage

Tâche	Description	Compétences requises
Lancez le déploiement de la pile de routage.	Pour lancer le déploiement de la pile de CloudFormation routage `CustomDomainRouterStack`, exécutez la commande suivante, en la `example.com` remplaçant par le nom du domaine que vous possédez : `npx cdk deploy CustomDomainRouterStack --parameters PrerequisiteDomainName=example.com` **Note** Le déploiement de la pile ne réussira pas tant que la tâche de validation DNS du domaine suivante n'aura pas été exécutée avec succès.	Développeur d’applications

Vérifier la propriété du domaine

Tâche	Description	Compétences requises
Vérifiez la propriété de votre domaine.	Le certificat restera dans le statut En attente de validation jusqu'à ce que vous prouviez que vous êtes propriétaire du domaine associé. Pour prouver que vous en êtes le propriétaire, ajoutez des enregistrements CNAME à la zone hébergée associée au domaine. Pour plus d'informations, consultez la section Validation DNS dans la AWS Certificate Manager documentation. L'ajout des enregistrements appropriés permet au `CustomDomainRouterStack` déploiement de réussir.	Développeur d'applications, administrateur système AWS, administrateur réseau
Créez un enregistrement d'alias pour pointer vers votre domaine personnalisé API Gateway.	Une fois le certificat émis et validé avec succès, créez un enregistrement DNS qui pointe vers l'URL de votre domaine personnalisé Amazon API Gateway. L'URL du domaine personnalisé est générée de manière unique par le provisionnement du domaine personnalisé et est spécifiée en tant que	Développeur d'applications, administrateur système AWS, administrateur réseau

Tâche	Description	Compétences requises
	paramètre CloudFormation de sortie. Voici un exemple de record : Politique de routage : routage simple Nom de l'enregistrement : `demo.api-gateway-custom-domain-versioning.example.com` Alias : Oui Type d'enregistrement : enregistrement DNS de type « A » qui pointe vers une AWS ressource Value (Valeur) : `d-xxxxxxxxxx.execute-api.xx-xxxx-x.amazonaws.com` TTL (secondes) : 300	

Déployez CloudFormation des stacks et appelez l'API

Tâche	Description	Compétences requises
Déployez la `ApiStackV1` pile.	Pour déployer la `ApiStackV1` pile, utilisez la commande suivante : `npm run deploy-v1`	Développeur d’applications

Tâche	Description	Compétences requises
	Le code CDK suivant ajoute un mappage d'API : `var apiMapping = new CfnApiMapping(this, "ApiMapping", { apiId: this.lambdaRestApi.restApiId, domainName: props.customDomainName.domainName, stage: "api", apiMappingKey: "api/v1", });`	
Déployez la `ApiStackV2` pile.	Pour déployer la `ApiStackV2` pile, utilisez la commande suivante : `npm run deploy-v2`	Développeur d’applications
Appelez l'API.	Pour appeler l'API et tester les points de terminaison de l'API à l'aide de Bruno, consultez les instructions de la section Informations supplémentaires.	Développeur d’applications

Nettoyage des ressources

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour détruire les ressources associées à cet exemple d'application, utilisez la commande suivante :	Développeur d’applications

Tâche	Description	Compétences requises
	`npx cdk destroy --all` **Note** Assurez-vous de nettoyer tous les enregistrements DNS Route 53 ajoutés manuellement pour le processus de vérification de la propriété du domaine.	

Résolution des problèmes

Problème	Solution
Le déploiement `CustomDomainRouterStack` expire car le certificat ne peut pas être validé.	Assurez-vous d'avoir ajouté les enregistrements CNAME de validation DNS appropriés, comme décrit dans la tâche précédente. Votre nouveau certificat peut continuer à afficher le statut En attente de validation jusqu'à 30 minutes après l'ajout des enregistrements de validation DNS. Pour plus d'informations, consultez la section Validation DNS dans la AWS Certificate Manager documentation.

Ressources connexes

- Implémentation du versionnement d'API Gateway basé sur les en-têtes avec Amazon CloudFront — Ce billet de AWS Compute Blog propose une stratégie de gestion des versions basée sur

les en-têtes comme alternative à la stratégie de version basée sur les chemins décrite dans ce modèle.

- AWS CDK Atelier — Cet atelier d'introduction se concentre sur la création et le déploiement d'applications AWS à l'aide du AWS Cloud Development Kit (AWS CDK). Cet atelier prend en charge Go, Python et TypeScript.

Informations supplémentaires

Tester votre API avec Bruno

Nous vous recommandons d'utiliser Bruno, un outil de test d'API open source, pour vérifier que le routage basé sur le chemin fonctionne correctement pour l'exemple d'application. Ce modèle fournit une collecte d'échantillons pour faciliter le test de votre exemple d'API.

Pour appeler et tester votre API, procédez comme suit :

1. Installez Bruno.
2. Ouvrez Bruno.
3. Dans le référentiel de code de ce modèle, sélectionnez Bruno/sample-API- Gateway-Custom-Domain-Versioning et ouvrez la collection.
4. Pour voir le menu déroulant Environnements en haut à droite de l'interface utilisateur (UI), sélectionnez une demande dans la collection.
5. Dans le menu déroulant Environnements, sélectionnez Configurer.
6. Remplacez la `REPLACE_ME_WITH_YOUR_DOMAIN` valeur par votre domaine personnalisé.
7. Choisissez Enregistrer, puis fermez la section Configuration.
8. Pour l'environnement Sandbox, vérifiez que l'option Active est sélectionnée.
9. Appelez votre API en utilisant le bouton -> pour la demande sélectionnée.
10. Prenez note de la façon dont la validation (transmission de valeurs non numériques) est gérée dans V1 par rapport à V2.

Pour voir des captures d'écran d'un exemple d'appel d'API et une comparaison des validations V1 et V2, voir Tester votre exemple d'API dans le `README.md` fichier du référentiel de code de ce modèle.

Importez la bibliothèque psycopg2 pour interagir avec votre base AWS Lambda de données PostgreSQL

Créée par Louis Hourcade (AWS)

Récapitulatif

Psycopg est un adaptateur de base de données PostgressQL pour Python. Les développeurs utilisent la `psycopg2` bibliothèque pour écrire des applications Python qui interagissent avec les bases de données PostgreSQL.

Sur Amazon Web Services (AWS), les développeurs exécutent également du code pour des applications ou des services de backend. AWS Lambda Lambda est un service de calcul sans serveur piloté par les événements qui exécute du code sans qu'il soit nécessaire de provisionner ou de gérer des serveurs.

Par défaut, lorsque vous créez une nouvelle fonction qui utilise un environnement d'exécution Python (version 3.9, 3.8 ou 3.7), l'environnement d'exécution Lambda est créé à partir d'une image de base pour Lambda fournie par. AWS Les bibliothèques, telles que `pandas` ou`psycopg2`, ne sont pas incluses dans l'image de base. Pour utiliser une bibliothèque, vous devez la regrouper dans un package personnalisé et l'associer à Lambda.

Il existe plusieurs méthodes pour regrouper et associer une bibliothèque, notamment les suivantes :

- Déployez votre fonction Lambda à partir d'une archive de fichier .zip.
- Déployez votre fonction Lambda à partir d'une image de conteneur personnalisée.
- Créez une couche Lambda et attachez-la à votre fonction Lambda.

Ce modèle illustre les deux premières options.

Avec un package de déploiement .zip, l'ajout de la `pandas` bibliothèque à votre fonction Lambda est relativement simple. Créez un dossier sur votre machine Linux, ajoutez le script Lambda ainsi que la `pandas` bibliothèque et les dépendances de la bibliothèque au dossier, compressez le dossier et fournissez-le comme source pour votre fonction Lambda.

Bien que l'utilisation d'un package de déploiement .zip soit une pratique courante, cette approche ne fonctionne pas pour la `psycopg2` bibliothèque. Ce modèle montre d'abord l'erreur que vous obtenez si vous utilisez un package de déploiement .zip pour ajouter la `psycopg2` bibliothèque à

votre fonction Lambda. Le modèle montre ensuite comment déployer Lambda à partir d'un Dockerfile et modifier l'image Lambda pour faire fonctionner la bibliothèque. `psycopg2`

Pour plus d'informations sur les trois ressources déployées par le modèle, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS disposant des autorisations suffisantes pour déployer les AWS ressources utilisées par ce modèle
- AWS Cloud Development Kit (AWS CDK) installé globalement en exécutant `npm install -g aws-cdk`
- Un client Git
- Python
- Docker

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Versions du produit

- Version d'exécution d'AWS Lambda : Python 3.8 (le modèle peut être adapté pour d'autres versions de Python.)
- Version 2.9.3 de Psycopg2
- Version 1.5.2 des Pandas

Architecture

Présentation de la solution

Pour illustrer les défis auxquels vous pourriez être confronté lors de l'utilisation de la `psycopg2` bibliothèque dans Lambda, le modèle déploie deux fonctions Lambda :

- Une fonction Lambda avec le runtime Python 3.8 créée à partir d'un fichier .zip. Les `pandas` bibliothèques `psycopg2` et sont installées dans ce package de déploiement .zip à l'aide de pip.
- Une fonction Lambda avec le runtime Python 3.8 créée à partir d'un Dockerfile. Le Dockerfile installe les `pandas` bibliothèques `psycopg2` et dans l'image du conteneur Lambda.

La première fonction Lambda installe la `pandas` bibliothèque et ses dépendances dans un fichier .zip, et Lambda peut utiliser cette bibliothèque.

La deuxième fonction Lambda montre qu'en créant une image de conteneur pour votre fonction Lambda, vous pouvez exécuter les `pandas` bibliothèques `psycopg2` et dans Lambda.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure cloud AWS sous forme de code.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- pandas est un outil open source basé sur Python pour l'analyse et la manipulation de données.
- Psycopg est un adaptateur de base de données PostgreSQL pour le langage Python conçu pour les applications multithread. Ce modèle utilise Psycopg 2.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt import-psycopg2 - - sur. in-lambda-to-interact with-postgres-database GitHub

Bonnes pratiques

Ce modèle fournit un exemple pratique d'utilisation AWS CDK pour créer une fonction Lambda à partir d'un Dockerfile. Si vous réutilisez ce code dans votre application, assurez-vous que les ressources déployées répondent à toutes les exigences de sécurité. Utilisez des outils tels que Checkov, qui analyse les configurations de l'infrastructure cloud pour détecter les erreurs de configuration avant le déploiement de l'infrastructure.

Épopées

Cloner le référentiel et configurer le déploiement

Tâche	Description	Compétences requises

Pour cloner le référentiel.	Pour cloner le GitHub dépôt sur votre machine locale, exécutez les commandes suivantes :
	`git clone https://github.com/aws-samples/import-psycopg2-in-lambda-to-interact-with-postgres-database.git`
	`cd AWS-lambda-psycopg2`
		AWS général

Configurez votre déploiement.	Modifiez le `app.py` fichier contenant les informations relatives à Compte AWS :
	`aws_acccount = "AWS_ACCOUNT_ID"`
	`region = "AWS_REGION"`
	`# Select the CPU architecture you are using to build the image (ARM or X86)`
	`architecture = "ARM"`
		AWS général

Démarrez votre compte AWS et déployez l'application

Tâche	Description	Compétences requises
Bootstrap votre. Compte AWS	Si vous n'avez pas encore amorcé votre environnement AWS, exécutez les commandes suivantes avec les AWS informations d'identification de votre AWS compte : `cdk bootstrap aws://<tooling-account-id>/<aws-region>`	AWS général
Déployez le code.	Pour déployer l' AWS CDK application, exécutez la commande suivante : `cdk deploy AWSLambdaPyscopg2`	AWS général

Testez les fonctions Lambda depuis l'AWS Management Console

Tâche	Description	Compétences requises
Testez la fonction Lambda créée à partir du fichier .zip.	Pour tester la fonction Lambda créée à partir du fichier .zip, procédez comme suit : 1. Connectez-vous à la console et ouvrez la console Lambda à l'adresse. https://console.aws.amazon.com/lambda/	AWS général

Tâche	Description	Compétences requises
	2. Sélectionnez la fonction `lambda-from-zip` Lambda. 3. Créez un événement de test pour appeler la fonction. 4. Lorsqu'elle est invoquée, la fonction doit générer une erreur incluant le message suivant : `"errorMessage": Unable to import module 'lambda_code': libpq.so.5: cannot open shared object, "stackTrace": [] "errorType": Runtime.ImportModuleError",` 5. Ouvrez la CloudWatch console Amazon à l'adresse https://console.aws.amazon.com/cloudwatch/. Les CloudWatch journaux indiquent que la `pandas` bibliothèque a été importée avec succès mais que l'importation de la `psycopg2` bibliothèque a échoué. Comme Lambda ne trouve pas les bibliothèques	

Tâche	Description	Compétences requises
	PostgreSQL requises dans l'image par défaut, il ne peut pas utiliser la bibliothèque. `psycopg2`	

Tâche	Description	Compétences requises

Testez la fonction Lambda créée à partir du Dockerfile.	Pour utiliser la `psycopg2` bibliothèque dans votre fonction Lambda, vous devez modifier l'image Lambda Amazon Machine (AMI).
	
	Pour tester la fonction Lambda créée à partir du Dockerfile, procédez comme suit :
	
	1. Connectez-vous à la console et ouvrez la console Lambda.
	2. Sélectionnez la fonction `lambda-from-docker` Lambda.
	3. Créez un événement de test pour appeler la fonction.
	4. Lorsqu'elle est invoquée, la fonction doit s'exécuter correctement.
	
	Le code suivant montre le Dockerfile créé par le AWS CDK modèle :
	
	`# Start from lambda Python3.8 image`
	`FROM public.ecr.aws/lambda/python:3.8`
	
	`# Copy the lambda code, together with its requirements`
		AWS général

Tâche	Description	Compétences requises

	``
	COPY lambda/requirement
	s.txt ${LAMBDA_
	TASK_ROOT}
	COPY lambda/lambda_code
	.py ${LAMBDA_TASK_ROOT
	}
	
	# Install postgresql-
	devel in your image
	RUN yum install -y gcc
	 postgresql-devel
	
	# install the requireme
	nts for the Lambda code
	RUN pip3 install -r
	 requirements.txt
	 --target "${LAMBDA
	_TASK_ROOT}"
	
	# Command can be
	 overwritten by
	 providing a different
	 command in the template
	 directly.
	CMD ["lambda_code.hand
	ler"]
	``	

	Le Dockerfile prend l'image AWS Lambda fournie pour le runtime Python 3.8 et installe postgresql-devel, qui contient les bibliothèques nécessaires pour compiler des applications qui interagissent directement avec le serveur de gestion PostgreSQL. Le Dockerfile installe également les `psycopg2` bibliothèques `pandas` et, qui sont indiquées	

Tâche	Description	Compétences requises
	dans le fichier. `requirements.txt`	

Ressources connexes

- AWS CDK documentation
- AWS Lambda documentation

Informations supplémentaires

Dans ce modèle, le AWS CDK modèle fournit une AWS pile de trois ressources :

- Rôle AWS Identity and Access Management (IAM) pour les fonctions Lambda.
- Une fonction Lambda avec un environnement d'exécution Python 3.8. La fonction est déployée à partir du package `Constructs/lambda/lambda_deploy.zip` de déploiement.
- Une fonction Lambda avec un environnement d'exécution Python 3.8. La fonction est déployée à partir du Dockerfile situé sous le dossier `Constructs`

Le script des deux fonctions Lambda vérifie si les `psycopg2` bibliothèques `pandas` et sont correctement importées :

```
import pandas
print("pandas successfully imported")

import psycopg2
print("psycopg2 successfully imported")

def handler(event, context):
    """Function that checks whether psycopg2  and pandas are successfully imported or
 not"""
    return {"Status": "psycopg2 and pandas successfully imported"}
```

Le package `lambda_deploy.zip` de déploiement est créé avec le script `Constructs/lambda/build.sh` bash. Ce script crée un dossier, copie le script Lambda, installe les `psycopg2`

bibliothèques `pandas` et et génère le fichier .zip. Pour générer vous-même le fichier .zip, exécutez ce script bash et redéployez la pile. AWS CDK

Le Dockerfile commence par l'image de base AWS fournie pour Lambda avec un environnement d'exécution Python 3.8. Le Dockerfile installe les `psycopg2` bibliothèques `pandas` et au-dessus de l'image par défaut.

Intégrez Amazon API Gateway à Amazon SQS pour gérer le REST asynchrone APIs

Créée par Natalia Colantonio Favero (AWS) et Gustavo Martim (AWS)

Récapitulatif

Lorsque vous déployez REST APIs, vous devez parfois exposer une file de messages que les applications clientes peuvent publier. Par exemple, vous pouvez rencontrer des problèmes liés à la latence des tiers APIs et aux retards dans les réponses, ou vous pouvez vouloir éviter le temps de réponse des requêtes de base de données ou éviter de dimensionner le serveur en cas de grand nombre de requêtes simultanées APIs. Dans ces scénarios, les applications clientes qui publient dans la file d'attente doivent uniquement savoir que l'API a reçu les données, et non pas ce qui se passe après réception des données.

Ce modèle crée un point de terminaison d'API REST en utilisant Amazon API Gateway pour envoyer un message à Amazon Simple Queue Service (Amazon SQS). Cela crée une easy-to-implement intégration entre les deux services qui évite l'accès direct à la file d'attente SQS.

Conditions préalables et limitations

- Un AWS compte actif

Architecture

Le schéma illustre les étapes suivantes :

1. Demandez un point de terminaison d'API POST REST à l'aide d'un outil tel que Postman, d'une autre API ou d'autres technologies.
2. API Gateway publie un message, qui est reçu dans le corps de la demande, dans la file d'attente.
3. Amazon SQS reçoit le message et envoie une réponse à API Gateway avec un code de réussite ou d'échec.

Outils

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

Épopées

Création d'une file d'attente SQS

Tâche	Description	Compétences requises
Créez une file d'attente.	Pour créer une file d'attente SQS qui reçoit les messages de l'API REST : 1. Connectez-vous à votre Compte AWS. 2. Ouvrez la console Amazon SQS à l'adresse. https://console.aws.amazon.com/sqs/ 3. Choisissez Créez une file d'attente. 4. Sur la page Créer une file d'attente, choisissez la bonne Région AWS option dans la liste déroulante Région. 5. Pour Type, conservez le paramètre par défaut (Standard). 6. Entrez un nom pour votre file d'attente.	Développeur d’applications

Tâche	Description	Compétences requises
	7. Conservez les valeurs par défaut pour tous les autres paramètres. 8. Choisissez Créez une file d'attente.	

Fournir un accès à Amazon SQS

Tâche	Description	Compétences requises
Créez un rôle IAM.	Ce rôle IAM donne aux ressources d'API Gateway un accès complet à Amazon SQS. 1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/. 2. Dans le panneau de navigation, choisissez Rôles, puis Créer un rôle. 3. Pour Trusted entity (Entité de confiance), choisissez Service AWS. 4. Dans le cas d'utilisation, choisissez API Gateway dans la liste déroulante, puis choisissez Next, Next. 5. Dans Nom du rôle, entrez AWSGatewayRoleForSQS et une description facultative, puis choisissez Créer un rôle.	Développeur d'applications, administrateur AWS

Tâche	Description	Compétences requises
	6. Dans le volet Rôles, recherchez AWSGatewayRoleForSQS et cochez sa case. 7. Dans la section Politiques d'autorisations, choisissez Ajouter des autorisations, Attacher des politiques. 8. Recherchez Amazon SQSFull Access et sélectionnez-le. 9. Choisissez Add permissions (Ajouter des autorisations). 10. Dans la section Résumé de AWSGatewayRoleForSQS, copiez le numéro de ressource Amazon (ARN). Vous utiliserez cet identifiant ultérieurement.	

Création d'une API REST

Tâche	Description	Compétences requises
Créez une API REST.	Il s'agit de l'API REST à laquelle les requêtes HTTP sont envoyées. 1. Ouvrez la console API Gateway à l'adresse https://console.aws.amazon.com/apigateway/. 2. Dans la section API REST, choisissez Build.	Développeur d’applications

Tâche	Description	Compétences requises
	3. Pour le nom de l'API, entrez un nom et une description facultative pour votre API, conservez tous les autres paramètres par défaut, puis choisissez Create API.	

Tâche	Description	Compétences requises
Connectez API Gateway à Amazon SQS.	Cette étape permet au message de circuler depuis le corps de la requête HTTP vers Amazon SQS. 1. Sur la console API Gateway, choisissez l'API que vous avez créée. 2. Sur la page Ressources, dans la section Méthodes, choisissez Créer une méthode. 3. Pour Type de méthode, sélectionnez POST. 4. Dans Type d'intégration, sélectionnez Service AWS. 5. Pour Région AWS, choisissez la région dans laquelle vous avez créé votre file d'attente SQS. 6. Pour Service AWS, choisissez Simple Queue Service (SQS). 7. Pour la méthode HTTP, choisissez POST. 8. Pour Type d'action, choisissez Utiliser le remplacement du chemin. 9. <name of SQS queue>Pour Path override, entrez/<AWS account ID>. 10. Pour Rôle d'exécution, collez l'ARN du rôle que	Développeur d’applications

Tâche	Description	Compétences requises
	vous avez créé précédemment. 11. Choisissez Créer une méthode.	

Testez l'API REST

Tâche	Description	Compétences requises
Testez l'API REST.	Exécutez un test pour vérifier s'il n'y a pas de configuration manquante : 1. Sur la console API Gateway, choisissez l'API REST que vous avez créée. 2. Dans le volet Ressources, choisissez la méthode POST. 3. Choisissez l'onglet Test. (Utilisez la flèche droite si l'onglet n'est pas affiché.) 4. Pour le corps de la requête, collez le code JSON suivant : `{ "message": "lorem ipsum" }` 5. Sélectionnez Tester).	Développeur d'applications

Tâche	Description	Compétences requises
	Vous recevrez un message d'erreur similaire à ce qui suit : `<UnknownOperationException/>`	

Tâche	Description	Compétences requises
Modifiez l'intégration de l'API pour transmettre correctement la demande à Amazon SQS.	Complétez la configuration pour corriger l'erreur d'intégration : 1. Sur la console API Gateway, choisissez l'API que vous avez créée, puis sélectionnez POST. 2. La section Method Execution présente le mappage visuel entre API Gateway et Amazon SQS. Dans cette section, choisissez Demande d'intégration, puis Modifier. 3. Développez la section des en-têtes HTTP, puis choisissez le paramètre Ajouter un en-tête de demande. • Dans Nom, spécifiez le type de contenu. • Dans le champ Mappé depuis, saisissez « application/ » x-www-form-urlencoded. Assurez-vous d'inclure les guillemets simples. • Cochez la case Mise en cache. 4. Développez la section Modèles de mappage.	Développeur d’applications

Tâche	Description	Compétences requises
	• Sélectionnez Add mapping template. • Pour Type de contenu, entrez application/json. • Pour le corps du modèle, collez ce code : `Action=SendMessage&MessageBody=$input.body` • Choisissez Enregistrer.	

Tâche	Description	Compétences requises
Testez et validez le message dans Amazon SQS.	Exécutez un test pour confirmer qu'il s'est bien déroulé : 1. Sur la console API Gateway, choisissez l'API REST que vous avez créée. 2. Dans le volet Ressources, choisissez la méthode POST. 3. Choisissez l’onglet Test. (Utilisez la flèche droite si l'onglet n'est pas affiché.) 4. Pour le corps de la requête, collez le code JSON suivant : `{ "message": "lorem ipsum" }` 5. Sélectionnez Tester). 6. Ouvrez la console Amazon SQS. 7. Dans le volet de navigation, choisissez Queues, puis choisissez votre file d'attente. 8. Choisissez Envoyer et recevoir des messages. 9. Choisissez Rechercher des messages.	Développeur d’applications

Tâche	Description	Compétences requises
	10. Choisissez Message. Il doit afficher les informations suivantes : `Body { "message": "lorem ipsum" }`	

Tâche	Description	Compétences requises

Testez API Gateway avec un caractère spécial.	Exécutez un test qui inclut des caractères spéciaux (tels que &) qui ne sont pas acceptables dans un message :
	1. Sur la console API Gateway, choisissez votre API.
	2. Répétez le test de l'étape précédente en utilisant le code JSON suivant :
	`{ "message": "lorem ipsum &" }`
	3. Sélectionnez Tester).
	Vous recevrez un message d'erreur tel que le suivant :
	`{ "Error": { "Code": "AccessDenied", "Message": "Access to the resource https://sqs.us-east-2.amazonaws.com/976166761794/Apg2 is denied.", "Type": "Sender" }, "RequestId": "e83c9c67-bcf6-5e9a-91e9-c737094b17ab"`
		Développeur d'applications

Tâche	Description	Compétences requises
	<pre>}</pre> Cela est dû au fait que les caractères spéciaux ne sont pas pris en charge par défaut dans le corps du message. À l'étape suivante, vous allez configurer API Gateway pour qu'il prenne en charge les caractères spéciaux. Pour plus d'informations sur les conversions par type de contenu, consultez la documentation d'API Gateway.	

Tâche	Description	Compétences requises

Modifiez la configuration de l'API pour prendre en charge les caractères spéciaux.	Ajustez la configuration pour accepter les caractères spéciaux dans le message :
	1. Sur la console API Gateway, choisissez l'API que vous avez créée, puis sélectionnez POST.
	2. Choisissez Requête d'intégration, puis Modifier.
	3. Changez la gestion du contenu pour Convertir en texte.
	4. Dans la section Modèles de mappage :
	• Pour Type de contenu, entrez application/json.
	• Pour le corps du modèle, spécifiez :
	`Action=SendMessage&MessageBody=$util.urlEncode($input.body)`
	• Choisissez Enregistrer.
	5. Choisissez l'onglet Test.
	6. Pour le corps de la requête, entrez le code JSON précédent :
	`{ " message": "lorem ipsum &" }`
		Développeur d'applications

Tâche	Description	Compétences requises
	7. Sélectionnez Tester). 8. Ouvrez la console Amazon SQS. 9. Sélectionnez votre file d'attente, puis choisissez Envoyer et recevoir des messages, Rechercher des messages, Envoyer un message comme précédemment. Le nouveau message doit inclure le caractère spécial.	

Déployer l'API REST

Tâche	Description	Compétences requises
Déployez l'API.	Pour déployer l'API REST : 1. Ouvrez la console API Gateway. 2. Choisissez votre API. 3. Sélectionnez Deploy API (Déployer une API). Pour plus d'informations sur cette étape, consultez la documentation d'API Gateway.	Développeur d’applications
Testez avec un outil externe.	Effectuez un test avec un outil externe pour vérifier que le message a bien été reçu :	Développeur d’applications

Tâche	Description	Compétences requises
	1. Ouvrez un outil tel que Postman, Insomnia ou cURL. 2. Exécutez votre API. 3. Ouvrez la console Amazon SQS. 4. Sélectionnez votre file d'attente. 5. Chargez les messages pour voir le nouveau message.	

Nettoyage

Tâche	Description	Compétences requises
Supprimez l'API.	Sur la console API Gateway, choisissez l'API que vous avez créée, puis choisissez Delete.	Développeur d’applications
Supprimez le rôle IAM.	Sur la console IAM, dans le volet Rôles, sélectionnez AWSGatewayRoleForSQS, puis choisissez Supprimer.	Développeur d’applications
Supprimez la file d'attente SQS.	Sur la console Amazon SQS, dans le volet Queues, choisissez la file d'attente SQS que vous avez créée, puis choisissez Supprimer.	Développeur d’applications

Ressources connexes

- SQS- SendMessage (documentation API Gateway)

- Conversions de type de contenu dans API Gateway (documentation API Gateway)
- variables $util (documentation API Gateway)
- Comment intégrer une API REST API Gateway à Amazon SQS et résoudre les erreurs courantes ? (AWS Re:publier l'article)

Traitez les événements de manière asynchrone avec Amazon API Gateway et AWS Lambda

Créée par Andrea Meroni (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) et Michael Wallner (AWS)

Récapitulatif

Amazon API Gateway est un service entièrement géré que les développeurs peuvent utiliser pour créer, publier, gérer, surveiller et sécuriser APIs à n'importe quelle échelle. Il gère les tâches liées à l'acceptation et au traitement de centaines de milliers d'appels d'API simultanés.

Le délai d'intégration est un quota de service important pour API Gateway. Le délai d'attente est le délai maximal pendant lequel un service principal doit renvoyer une réponse avant que l'API REST ne renvoie une erreur. La limite stricte de 29 secondes est généralement acceptable pour les charges de travail synchrones. Toutefois, cette limite représente un défi pour les développeurs qui souhaitent utiliser API Gateway avec des charges de travail asynchrones.

Ce modèle montre un exemple d'architecture permettant de traiter les événements de manière asynchrone à l'aide d'API Gateway et. AWS Lambda L'architecture prend en charge l'exécution de tâches de traitement d'une durée maximale de 15 minutes et utilise une API REST de base comme interface.

Projen est utilisé pour configurer l'environnement de développement local et pour déployer l'exemple d'architecture sur une cible Compte AWS, en combinaison avec le AWS Cloud Development Kit (AWS CDK) Toolkit, Docker et Node.js. Projen configure automatiquement un environnement virtuel Python avec le pré-commit et les outils utilisés pour l'assurance qualité du code, l'analyse de sécurité et les tests unitaires. Pour plus d'informations, consultez la section Outils.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Les outils suivants sont installés sur votre poste de travail :
  - AWS Cloud Development Kit (AWS CDK) Boîte à outils version 2.85.0
  - Version 20.10.21 de Docker
  - Version 18.13.0 de Node.js
  - Version du projet 0.71.111

- Version 3.9.16 de Python

Limites

- Le temps d'exécution maximal d'une tâche est limité par le temps d'exécution maximal des fonctions Lambda (15 minutes).
- Le nombre maximum de demandes de travail simultanées est limité par la simultanéité réservée de la fonction Lambda.

Architecture

Le schéma suivant montre l'interaction de l'API jobs avec les fonctions Lambda de traitement des événements et de gestion des erreurs, les événements étant stockés dans une archive d'événements Amazon. EventBridge

Un flux de travail typique comprend les étapes suivantes :

1. Vous vous authentifiez auprès de AWS Identity and Access Management (IAM) et obtenez des informations d'identification de sécurité.
2. Vous envoyez une `POST` requête HTTP au point de terminaison de l'API des `/jobs` tâches, en spécifiant les paramètres de la tâche dans le corps de la demande.
3. L'API jobs, qui est une API REST API Gateway, vous renvoie une réponse HTTP contenant l'identifiant de la tâche.
4. L'API jobs appelle de manière asynchrone la fonction Lambda de traitement des événements.
5. La fonction de traitement des événements traite l'événement, puis place les résultats de la tâche dans la table Amazon DynamoDB de la tâche
6. Vous envoyez une `GET` requête HTTP au point de terminaison de l'API des `/jobs/{jobId}` tâches, avec l'identifiant de tâche de l'étape 3 sous la forme`{jobId}`.
7. L'API des tâches interroge la table `jobs` DynamoDB pour récupérer les résultats des tâches.
8. L'API des tâches renvoie une réponse HTTP contenant les résultats des tâches.
9. Si le traitement des événements échoue, la fonction de traitement des événements envoie l'événement à la fonction de gestion des erreurs.
10. La fonction de gestion des erreurs place les paramètres de la tâche dans la table DynamoDB`jobs`.

11. Vous pouvez récupérer les paramètres des tâches en envoyant une `GET` requête HTTP au point de terminaison de l'API `/jobs/{jobId}` des tâches.
12. Si la gestion des erreurs échoue, la fonction de gestion des erreurs envoie l'événement à une archive d' EventBridge événements.

    Vous pouvez rejouer les événements archivés en utilisant EventBridge.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres domaines. Comptes AWS
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Autres outils

- autopep8 formate automatiquement le code Python en fonction du guide de style de la Python Enhancement Proposal (PEP) 8.
- Bandit scanne le code Python pour détecter les problèmes de sécurité courants.
- Commitizen est un vérificateur et un générateur de commit Git. `CHANGELOG`
- cfn-lint est un linter AWS CloudFormation
- Checkov est un outil d'analyse de code statique qui vérifie l'infrastructure en tant que code (IaC) pour détecter les erreurs de configuration liées à la sécurité et à la conformité.
- jq est un outil en ligne de commande pour analyser le JSON.

- Postman est une plateforme d'API.
- pre-commit est un gestionnaire de hooks Git.
- Projen est un générateur de projets.
- pytest est un framework Python pour écrire de petits tests lisibles.

Référentiel de code

Cet exemple de code d'architecture se trouve dans le référentiel GitHub Asynchronous Event Processing with API Gateway and Lambda.

Bonnes pratiques

- Cet exemple d'architecture n'inclut pas la surveillance de l'infrastructure déployée. Si votre cas d'utilisation nécessite une surveillance, évaluez l'ajout de constructions de surveillance CDK ou d'une autre solution de surveillance.
- Cet exemple d'architecture utilise les autorisations IAM pour contrôler l'accès à l'API des tâches. Toute personne autorisée à assumer le `JobsAPIInvokeRole` sera en mesure d'invoquer l'API jobs. Le mécanisme de contrôle d'accès est donc binaire. Si votre cas d'utilisation nécessite un modèle d'autorisation plus complexe, évaluez-le à l'aide d'un autre mécanisme de contrôle d'accès.
- Lorsqu'un utilisateur envoie une `POST` requête HTTP au point de terminaison de l'API `/jobs` jobs, les données d'entrée sont validées à deux niveaux différents :
  - Amazon API Gateway est chargé de la validation de la première demande.
  - La fonction de traitement des événements exécute la deuxième demande.

    Aucune validation n'est effectuée lorsque l'utilisateur envoie une `GET` requête HTTP au point de terminaison de l'API `/jobs/{jobId}` des tâches. Si votre cas d'utilisation nécessite une validation des entrées supplémentaire et un niveau de sécurité accru, évaluez l'utilisation d'AWS WAF pour protéger votre API.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le dépôt localement, exécutez la commande suivante : `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-lambda-cdk.git`	DevOps ingénieur

Configurez le projet.	Remplacez le répertoire par la racine du référentiel et configurez l'environnement virtuel Python et tous les outils à l'aide de Projen :
	`cd asynchronous-event-processing-api-gateway-api-gateway-lambda-cdk`
	`npx projen`
		DevOps ingénieur

Installez des hooks de pré-validation.	Pour installer des hooks de pré-validation, procédez comme suit : 1. Activez l'environnement virtuel Python : `source .env/bin/activate`	DevOps ingénieur

Tâche	Description	Compétences requises

	2. Installez les hooks de pré-validation :
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`	

Déployez l'exemple d'architecture

Tâche	Description	Compétences requises
Bootstrap. AWS CDK	Pour démarrer votre AWS CDK compte Compte AWS, exécutez la commande suivante : `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Déployez l'exemple d'architecture.	Pour déployer l'exemple d'architecture dans votre Compte AWS, exécutez la commande suivante : `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Testez l'architecture

Tâche	Description	Compétences requises
Installez les prérequis de test.	Installez sur votre poste de travail the AWS Command Line Interface (AWS CLI), Postman et jq. L'utilisation de Postman pour tester cet exemple d'architecture est suggérée mais pas obligatoire. Si vous choisissez un autre outil de test d'API, assurez-vous qu'il prend en charge l'authentification AWS Signature version 4 et reportez-vous aux points de terminaison d'API exposés qui peuvent être inspectés en exportant l'API REST.	DevOps ingénieur
Supposons que`JobsAPIInvokeRole` .	Supposons que `JobsAPIInvokeRole` ce qui a été imprimé en tant que sortie de la commande de déploiement : `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS | jq`	AWS DevOps

Tâche	Description	Compétences requises
	``` ‘.Credentials’’.Ac cessKeyId’) export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq ‘.Credentials’’.Se cretAccessKey’) export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq ‘.Credentials’’.Se ssionToken’) ```	

Tâche	Description	Compétences requises
Configurez Postman.	1. Pour importer la collection Postman incluse dans le référentiel, suivez les instructions de la documentation Postman. 2. Définissez les `JobsAPI` variables avec les valeurs suivantes : • `accessKey` – La valeur de l'`Credentials.AccessKeyId` attribut issu de la `assume-role` commande • `baseUrl`– La valeur de la `JobsApiJobsAPIEndpoint` sortie de la commande de déploiement, sans la barre oblique • `region`– La valeur de l' Région AWS endroit où vous avez déployé l'exemple d'architecture • `seconds`– Valeur du paramètre d'entrée pour l'exemple de tâche. Il doit s'agir d'un entier positif • `secretKey` – La valeur de l'`Credentials.SecretAccessKey` attribut	AWS DevOps

Tâche	Description	Compétences requises
	issu de la `assume-role` commande • `sessionToken` – La valeur de l'`Credentials.SessionToken` attribut issu de la `assume-role` commande	
Testez l'exemple d'architecture.	Pour tester l'exemple d'architecture, envoyez des demandes à l'API jobs. Pour plus d'informations, consultez la documentation de Postman.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
La destruction puis le redéploiement de l'architecture d'exemple échouent car le groupe de CloudWatch journaux Amazon Logs existe `/aws/apigateway/JobsAPIAccessLogs` déjà.	1. Si nécessaire, exportez vos données de journal vers Amazon S3. 2. Supprimez le groupe de CloudWatch journaux Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Redéployez l'exemple d'architecture.

Ressources connexes

- Modèle de mappage API Gateway et référence à la variable de journalisation des accès
- Configurer l'invocation asynchrone de la fonction Lambda du backend

Traitez les événements de manière asynchrone avec Amazon API Gateway et Amazon DynamoDB Streams

Créée par Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) et Michael Wallner (AWS)

Récapitulatif

Amazon API Gateway est un service entièrement géré que les développeurs peuvent utiliser pour créer, publier, gérer, surveiller et sécuriser APIs à n'importe quelle échelle. Il gère les tâches liées à l'acceptation et au traitement de centaines de milliers d'appels d'API simultanés.

Le délai d'intégration est un quota de service important pour API Gateway. Le délai d'attente est le délai maximal pendant lequel un service principal doit renvoyer une réponse avant que l'API REST ne renvoie une erreur. La limite stricte de 29 secondes est généralement acceptable pour les charges de travail synchrones. Toutefois, cette limite représente un défi pour les développeurs qui souhaitent utiliser API Gateway avec des charges de travail asynchrones.

Ce modèle montre un exemple d'architecture permettant de traiter des événements de manière asynchrone à l'aide d'API Gateway, d'Amazon DynamoDB Streams et. AWS Lambda L'architecture prend en charge l'exécution de tâches de traitement parallèle avec les mêmes paramètres d'entrée et utilise une API REST de base comme interface. Dans cet exemple, l'utilisation de Lambda comme backend limite la durée des tâches à 15 minutes. Vous pouvez éviter cette limite en utilisant un autre service pour traiter les événements entrants (par exemple, AWS Fargate).

Projen est utilisé pour configurer l'environnement de développement local et pour déployer l'exemple d'architecture sur une cible Compte AWS, en combinaison avec le AWS Cloud Development Kit (AWS CDK) Toolkit, Docker et Node.js. Projen configure automatiquement un environnement virtuel Python avec le pré-commit et les outils utilisés pour l'assurance qualité du code, l'analyse de sécurité et les tests unitaires. Pour plus d'informations, consultez la section Outils.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Les outils suivants sont installés sur votre poste de travail :
  - AWS Cloud Development Kit (AWS CDK) Toolkit version 2.85.0 ou ultérieure
  - Docker version 20.10.21 ou ultérieure

- Node.js version 18 ou ultérieure
- Projen version 0.71.111 ou ultérieure
- Python version 3.9.16 ou ultérieure

Limites

- Le nombre maximum de lecteurs recommandé pour DynamoDB Streams est de deux afin d'éviter toute limitation.
- Le temps d'exécution maximal d'une tâche est limité par le temps d'exécution maximal des fonctions Lambda (15 minutes).
- Le nombre maximum de demandes de travail simultanées est limité par la simultanéité réservée des fonctions Lambda.

Architecture

Architecture

Le schéma suivant montre l'interaction de l'API jobs avec DynamoDB Streams et les fonctions Lambda de traitement des événements et de gestion des erreurs, avec les événements stockés dans une archive d'événements Amazon. EventBridge

Un flux de travail typique comprend les étapes suivantes :

1. Vous vous authentifiez auprès de AWS Identity and Access Management (IAM) et obtenez des informations d'identification de sécurité.
2. Vous envoyez une `POST` requête HTTP au point de terminaison de l'API des `/jobs` tâches, en spécifiant les paramètres de la tâche dans le corps de la demande.
3. L'API des tâches vous renvoie une réponse HTTP contenant l'identifiant de la tâche.
4. L'API des tâches place les paramètres des tâches dans la table `jobs_table` Amazon DynamoDB.
5. Le flux `jobs_table` DynamoDB de la table DynamoDB invoque les fonctions Lambda de traitement des événements.
6. Les fonctions Lambda de traitement des événements traitent l'événement puis placent les résultats de la tâche dans la table DynamoDB. `jobs_table` Pour garantir des résultats cohérents,

les fonctions de traitement des événements mettent en œuvre un mécanisme de verrouillage optimiste.

7. Vous envoyez une `GET` requête HTTP au point de terminaison de l'API des `/jobs/{jobId}` tâches, avec l'identifiant de tâche de l'étape 3 sous la forme`{jobId}`.
8. L'API des tâches interroge la table `jobs_table` DynamoDB pour récupérer les résultats des tâches.
9. L'API des tâches renvoie une réponse HTTP contenant les résultats des tâches.
10. Si le traitement des événements échoue, le mappage source de la fonction de traitement des événements envoie l'événement à la rubrique Amazon Simple Notification Service (Amazon SNS) consacrée à la gestion des erreurs.
11. La rubrique SNS de gestion des erreurs transmet l'événement de manière asynchrone à la fonction de gestion des erreurs.
12. La fonction de gestion des erreurs place les paramètres de la tâche dans la table DynamoDB`jobs_table`.

    Vous pouvez récupérer les paramètres des tâches en envoyant une `GET` requête HTTP au point de terminaison de l'API `/jobs/{jobId}` des tâches.
13. Si la gestion des erreurs échoue, la fonction de gestion des erreurs envoie l'événement à une archive Amazon EventBridge .

    Vous pouvez rejouer les événements archivés en utilisant EventBridge.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure cloud AWS sous forme de code.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions AWS Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres comptes AWS.

- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Autres outils

- autopep8 formate automatiquement le code Python en fonction du guide de style de la Python Enhancement Proposal (PEP) 8.
- Bandit scanne le code Python pour détecter les problèmes de sécurité courants.
- Commitizen est un vérificateur et un générateur de commit Git. `CHANGELOG`
- cfn-lint est un linter AWS CloudFormation
- Checkov est un outil d'analyse de code statique qui vérifie l'infrastructure en tant que code (IaC) pour détecter les erreurs de configuration liées à la sécurité et à la conformité.
- jq est un outil en ligne de commande pour analyser le JSON.
- Postman est une plateforme d'API.
- pre-commit est un gestionnaire de hooks Git.
- Projen est un générateur de projets.
- pytest est un framework Python pour écrire de petits tests lisibles.

Référentiel de code

Cet exemple de code d'architecture se trouve dans le référentiel GitHub Asynchronous Processing with API Gateway et DynamoDB Streams.

Bonnes pratiques

- Cet exemple d'architecture n'inclut pas la surveillance de l'infrastructure déployée. Si votre cas d'utilisation nécessite une surveillance, évaluez l'ajout de constructions de surveillance CDK ou d'une autre solution de surveillance.
- Cet exemple d'architecture utilise les autorisations IAM pour contrôler l'accès à l'API des tâches. Toute personne autorisée à assumer le `JobsAPIInvokeRole` sera en mesure d'invoquer l'API jobs. Le mécanisme de contrôle d'accès est donc binaire. Si votre cas d'utilisation nécessite un modèle d'autorisation plus complexe, évaluez-le à l'aide d'un autre mécanisme de contrôle d'accès.

- Lorsqu'un utilisateur envoie une `POST` requête HTTP au point de terminaison de l'API `/jobs` jobs, les données d'entrée sont validées à deux niveaux différents :
  - API Gateway est en charge de la validation de la première demande.
  - La fonction de traitement des événements exécute la deuxième demande.

  Aucune validation n'est effectuée lorsque l'utilisateur envoie une `GET` requête HTTP au point de terminaison de l'API `/jobs/{jobId}` des tâches. Si votre cas d'utilisation nécessite une validation des entrées supplémentaire et un niveau de sécurité accru, évaluez l'utilisation AWS WAF pour protéger votre API.

- Pour éviter toute limitation, la documentation DynamoDB Streams déconseille aux utilisateurs de lire avec plus de deux utilisateurs d'une même partition de flux. Pour augmenter le nombre de consommateurs, nous vous recommandons d'utiliser Amazon Kinesis Data Streams.
- Le verrouillage optimiste a été utilisé dans cet exemple pour garantir des mises à jour cohérentes des éléments de la table `jobs_table` DynamoDB. Selon les exigences du cas d'utilisation, vous devrez peut-être mettre en œuvre des mécanismes de verrouillage plus fiables, tels que le verrouillage pessimiste.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le dépôt localement, exécutez la commande suivante : `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-dynamodb-streams-cdk.git`	DevOps ingénieur
Configurez le projet.	Remplacez le répertoire par la racine du référentiel et	DevOps ingénieur

Tâche	Description	Compétences requises

	configurez l'environnement virtuel Python et tous les outils à l'aide de Projen :
	`cd asynchronous-event-processing-api-gateway-api-gateway-dynamodb-streams-cdk`
	`npx projen`	

Installez des hooks de pré-validation.	Pour installer des hooks de pré-validation, procédez comme suit :
	1. Activez l'environnement virtuel Python :
	`source .env/bin/activate`
	2. Installez les hooks de pré-validation :
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`
		DevOps ingénieur

Déployez l'exemple d'architecture

Tâche	Description	Compétences requises
Bootstrap. AWS CDK	Pour démarrer votre AWS CDKcompte Compte AWS, exécutez la commande suivante :	AWS DevOps

Tâche	Description	Compétences requises
	`AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	
Déployez l'exemple d'architecture.	Pour déployer l'exemple d'architecture dans votre Compte AWS, exécutez la commande suivante : `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Testez l'architecture

Tâche	Description	Compétences requises
Installez les prérequis de test.	Installez sur votre poste de travail the AWS Command Line Interface (AWS CLI), Postman et jq. L'utilisation de Postman pour tester cet exemple d'architecture est suggérée mais pas obligatoire. Si vous choisissez un autre outil de test d'API, assurez-vous qu'il prend en charge l'authentification AWS Signature version 4 et reportez-vous aux points de terminaison d'API exposés qui peuvent être inspectés en exportant l'API REST.	DevOps ingénieur

Tâche	Description	Compétences requises
Supposons que`JobsAPIInvokeRole` .	Supposons que `JobsAPIInvokeRole` ce qui a été imprimé en tant que sortie de la `deploy` commande : `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS \| jq '.Credentials''.AccessKeyId') export AWS_SECRET_ACCESS_KEY=$(cat $CREDENTIALS \| jq '.Credentials''.SecretAccessKey') export AWS_SESSION_TOKEN==$(cat $CREDENTIALS | jq '.Credentials''.SessionToken')`	AWS DevOps

Tâche	Description	Compétences requises

Configurez Postman.	• Pour importer la collection Postman incluse dans le référentiel, suivez les instructions de la documentation Postman.
	• Définissez les `JobsAPI` variables avec les valeurs suivantes :
	  • `accessKey` – La valeur de l'`Credentials.AccessKeyId` attribut issu de la `assume-role` commande.
	  • `baseUrl`– La valeur de la `JobsApiJobsAPIEndpoint` sortie de la `deploy` commande, sans la barre oblique finale.
	  • `region`– La valeur de l' Région AWS endroit où vous avez déployé l'exemple d'architecture.
	  • `seconds`– Valeur du paramètre d'entrée pour l'exemple de tâche. Il doit s'agir d'un entier positif.
	  • `secretKey` – La valeur de l'`Credentials.SecretAccessKey` attribut issu de la `assume-role` commande.
		AWS DevOps

Tâche	Description	Compétences requises
	• `sessionToken` – La valeur de l'`Credentials.SessionToken` attribut issu de la `assume-role` commande.	
Testez l'exemple d'architecture.	Pour tester l'exemple d'architecture, envoyez des demandes à l'API jobs. Pour plus d'informations, consultez la documentation de Postman.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
La destruction puis le redéploiement de l'architecture d'exemple échouent car le groupe de CloudWatch journaux Amazon Logs existe / `aws/apigateway/JobsAPIAccessLogs` déjà.	1. Si nécessaire, exportez vos données de journal vers Amazon Simple Storage Service (Amazon S3). 2. Supprimez le groupe de CloudWatch journaux Logs/`aws/apigateway/JobsAPIAccessLogs` . 3. Redéployez l'exemple d'architecture.

Ressources connexes

- Modèle de mappage API Gateway et référence à la variable de journalisation des accès
- Modifier la capture de données pour DynamoDB Streams
- Verrouillage optimiste avec numéro de version
- Utilisation de Kinesis Data Streams pour capturer les modifications apportées à DynamoDB

Traitez les événements de manière asynchrone avec Amazon API Gateway, Amazon SQS et AWS Fargate

Créée par Andrea Meroni (AWS), Alessandro Trisolini (AWS), Nadim Majed (AWS), Mariem Kthiri (AWS) et Michael Wallner (AWS)

Récapitulatif

Amazon API Gateway est un service entièrement géré que les développeurs peuvent utiliser pour créer, publier, gérer, surveiller et sécuriser APIs à n'importe quelle échelle. Il gère les tâches liées à l'acceptation et au traitement de centaines de milliers d'appels d'API simultanés.

Le délai d'intégration est un quota de service important pour API Gateway. Le délai d'attente est le délai maximal pendant lequel un service principal doit renvoyer une réponse avant que l'API REST ne renvoie une erreur. La limite stricte de 29 secondes est généralement acceptable pour les charges de travail synchrones. Toutefois, cette limite représente un défi pour les développeurs qui souhaitent utiliser API Gateway avec des charges de travail asynchrones.

Ce modèle montre un exemple d'architecture permettant de traiter les événements de manière asynchrone à l'aide d'API Gateway, d'Amazon Simple Queue Service (Amazon SQS) et de. AWS Fargate L'architecture prend en charge l'exécution de tâches de traitement sans restriction de durée et utilise une API REST de base comme interface.

Projen est utilisé pour configurer l'environnement de développement local et pour déployer l'exemple d'architecture sur une cible Compte AWS, en combinaison avec Docker et Node.js. AWS Cloud Development Kit (AWS CDK) Projen configure automatiquement un environnement virtuel Python avec le pré-commit et les outils utilisés pour l'assurance qualité du code, l'analyse de sécurité et les tests unitaires. Pour plus d'informations, consultez la section Outils.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Les outils suivants sont installés sur votre poste de travail :
  - AWS Cloud Development Kit (AWS CDK) Toolkit version 2.85.0 ou ultérieure
  - Docker version 20.10.21 ou ultérieure
  - Node.js version 18 ou ultérieure

- Projen version 0.71.111 ou ultérieure
- Python version 3.9.16 ou ultérieure

Limites

- Les tâches simultanées sont limitées à 500 tâches par minute, ce qui correspond au nombre maximum de tâches que Fargate peut fournir.

Architecture

Le schéma suivant montre l'interaction de l'API jobs avec la table `jobs` Amazon DynamoDB, le service Fargate de traitement des événements et la fonction de gestion des erreurs. AWS Lambda Les événements sont stockés dans une archive d' EventBridge événements Amazon.

Un flux de travail typique comprend les étapes suivantes :

1. Vous vous authentifiez auprès de AWS Identity and Access Management (IAM) et obtenez des informations d'identification de sécurité.
2. Vous envoyez une `POST` requête HTTP au point de terminaison de l'API des `/jobs` tâches, en spécifiant les paramètres de la tâche dans le corps de la demande.
3. L'API jobs, qui est une API REST API Gateway, vous renvoie une réponse HTTP contenant l'identifiant de la tâche.
4. L'API jobs envoie un message à la file d'attente SQS.
5. Fargate extrait le message de la file d'attente SQS, traite l'événement, puis place les résultats de la tâche dans la table DynamoDB. `jobs`
6. Vous envoyez une `GET` requête HTTP au point de terminaison de l'API des `/jobs/{jobId}` tâches, avec l'identifiant de tâche de l'étape 3 sous la forme`{jobId}`.
7. L'API des tâches interroge la table `jobs` DynamoDB pour récupérer les résultats des tâches.
8. L'API des tâches renvoie une réponse HTTP contenant les résultats des tâches.
9. Si le traitement de l'événement échoue, la file d'attente SQS envoie l'événement à la file d'attente des lettres mortes (DLQ).
10. Un EventBridge événement déclenche la fonction de gestion des erreurs.
11. La fonction de gestion des erreurs place les paramètres de la tâche dans la table DynamoDB`jobs`.

12. Vous pouvez récupérer les paramètres des tâches en envoyant une `GET` requête HTTP au point de terminaison de l'API `/jobs/{jobId}` des tâches.
13. Si la gestion des erreurs échoue, la fonction de gestion des erreurs envoie l'événement à une EventBridge archive.

    Vous pouvez rejouer les événements archivés en utilisant EventBridge.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Fargatevous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou d'instances Amazon Elastic Compute Cloud (Amazon EC2). Il est utilisé conjointement avec Amazon Elastic Container Service (Amazon ECS).
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres domaines. Comptes AWS
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

Autres outils

- autopep8 formate automatiquement le code Python en fonction du guide de style de la Python Enhancement Proposal (PEP) 8.
- Bandit scanne le code Python pour détecter les problèmes de sécurité courants.
- Commitizen est un vérificateur et un générateur de commit Git. `CHANGELOG`

- cfn-lint est un linter AWS CloudFormation
- Checkov est un outil d'analyse de code statique qui vérifie l'infrastructure en tant que code (IaC) pour détecter les erreurs de configuration liées à la sécurité et à la conformité.
- jq est un outil en ligne de commande pour analyser le JSON.
- Postman est une plateforme d'API.
- pre-commit est un gestionnaire de hooks Git.
- Projen est un générateur de projets.
- pytest est un framework Python pour écrire de petits tests lisibles.

Référentiel de code

Cet exemple de code d'architecture se trouve dans le référentiel GitHub Asynchronous Processing with API Gateway et SQS.

Bonnes pratiques

- Cet exemple d'architecture n'inclut pas la surveillance de l'infrastructure déployée. Si votre cas d'utilisation nécessite une surveillance, évaluez l'ajout de constructions de surveillance CDK ou d'une autre solution de surveillance.
- Cet exemple d'architecture utilise les autorisations IAM pour contrôler l'accès à l'API des tâches. Toute personne autorisée à assumer le `JobsAPIInvokeRole` sera en mesure d'invoquer l'API jobs. Le mécanisme de contrôle d'accès est donc binaire. Si votre cas d'utilisation nécessite un modèle d'autorisation plus complexe, évaluez-le à l'aide d'un autre mécanisme de contrôle d'accès.
- Lorsqu'un utilisateur envoie une `POST` requête HTTP au point de terminaison de l'API `/jobs` jobs, les données d'entrée sont validées à deux niveaux différents :
  - API Gateway est en charge de la validation de la première demande.
  - La fonction de traitement des événements exécute la deuxième demande.

    Aucune validation n'est effectuée lorsque l'utilisateur envoie une `GET` requête HTTP au point de terminaison de l'API `/jobs/{jobId}` des tâches. Si votre cas d'utilisation nécessite une validation des entrées supplémentaire et un niveau de sécurité accru, évaluez l'utilisation AWS WAF pour protéger votre API.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le dépôt localement, exécutez la commande suivante : `git clone https://github.com/aws-samples/asynchronous-event-processing-api-gateway-sqs-cdk.git`	DevOps ingénieur

Configurez le projet.	Remplacez le répertoire par la racine du référentiel et configurez l'environnement virtuel Python et tous les outils à l'aide de Projen :
	`cd asynchronous-event-processing-api-gateway-api-gateway-sqs-cdk`
	`npx projen`
		DevOps ingénieur

Installez des hooks de pré-validation.	Pour installer des hooks de pré-validation, procédez comme suit : 1. Activez l'environnement virtuel Python : `source .env/bin/activate`	DevOps ingénieur

Tâche	Description	Compétences requises

	2. Installez les hooks de pré-validation :
	`pre-commit install`
	`pre-commit install --hook-type commit-msg`	

Déployez l'exemple d'architecture

Tâche	Description	Compétences requises
Bootstrap. AWS CDK	Pour démarrer votre AWS CDKcompte Compte AWS, exécutez la commande suivante : `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen bootstrap`	AWS DevOps
Déployez l'exemple d'architecture.	Pour déployer l'exemple d'architecture dans votre Compte AWS, exécutez la commande suivante : `AWS_PROFILE=$YOUR_AWS_PROFILE npx projen deploy`	AWS DevOps

Testez l'architecture

Tâche	Description	Compétences requises
Installez les prérequis de test.	Installez sur votre poste de travail the AWS Command Line Interface (AWS CLI), Postman et jq. L'utilisation de Postman pour tester cet exemple d'architecture est suggérée mais pas obligatoire. Si vous choisissez un autre outil de test d'API, assurez-vous qu'il prend en charge l'authentification AWS Signature version 4 et reportez-vous aux points de terminaison d'API exposés qui peuvent être inspectés en exportant l'API REST.	DevOps ingénieur
Supposons que`JobsAPIInvokeRole` .	Supposons que `JobsAPIInvokeRole` ce qui a été imprimé en tant que sortie de la `deploy` commande : `CREDENTIALS=$(AWS_PROFILE=$<YOUR_AWS_PROFILE> aws sts assume-role \ --no-cli-pager \ --role-arn $<JOBS_API_INVOKE_ROLE_ARN> \ --role-session-name JobsAPIInvoke) export AWS_ACCESS_KEY_ID=$(cat $CREDENTIALS | jq`	AWS DevOps

Tâche	Description	Compétences requises
	``` ‘.Credentials’’.Ac cessKeyId’) export AWS_SECRE T_ACCESS_KEY=$(cat $CREDENTIALS \| jq ‘.Credentials’’.Se cretAccessKey’) export AWS_SESSI ON_TOKEN==$(cat $CREDENTIALS | jq ‘.Credentials’’.Se ssionToken’) ```	

Tâche	Description	Compétences requises

Configurez Postman.	• Pour importer la collection Postman incluse dans le référentiel, suivez les instructions de la documentation Postman.
	• Définissez les `JobsAPI` variables avec les valeurs suivantes :
	  • `accessKey` – La valeur de l'`Credentials.AccessKeyId` attribut issu de la `assume-role` commande.
	  • `baseUrl`– La valeur de la `JobsApiJobsAPIEndpoint` sortie de la `deploy` commande, sans la barre oblique finale.
	  • `region`– La valeur de l' Région AWS endroit où vous avez déployé l'exemple d'architecture.
	  • `seconds`– Valeur du paramètre d'entrée pour l'exemple de tâche. Il doit s'agir d'un entier positif.
	  • `secretKey` – La valeur de l'`Credentials.SecretAccessKey` attribut issu de la `assume-role` commande.
		AWS DevOps

Tâche	Description	Compétences requises
	• `sessionToken` – La valeur de l'`Credentials.SessionToken` attribut issu de la `assume-role` commande.	
Testez l'exemple d'architecture.	Pour tester l'exemple d'architecture, envoyez des demandes à l'API jobs. Pour plus d'informations, consultez la documentation de Postman.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
La destruction puis le redéploiement de l'architecture d'exemple échouent car le groupe de CloudWatch journaux Amazon Logs existe `/aws/apigateway/JobsAPIAccessLogs` déjà.	1. Si nécessaire, exportez vos données de journal vers Amazon Simple Storage Service (Amazon S3). 2. Supprimez le groupe de CloudWatch journaux Logs `/aws/apigateway/JobsAPIAccessLogs` . 3. Redéployez l'exemple d'architecture.
La destruction puis le redéploiement de l'architecture d'exemple échouent car le groupe de CloudWatch journaux Logs existe `/aws/ecs/EventProcessingServiceLogs` déjà.	1. Si nécessaire, exportez les données de votre journal vers Amazon S3. 2. Supprimer le groupe de CloudWatch journaux Logs `/aws/ecs/EventProcessingServiceLogs.` 3. Redéployez l'exemple d'architecture.

Ressources connexes

- Modèle de mappage API Gateway et référence à la variable de journalisation des accès
- Comment intégrer une API REST API Gateway à Amazon SQS et résoudre les erreurs courantes ?

Exécutez les tâches d'automatisation d'AWS Systems Manager de manière synchrone depuis AWS Step Functions

Créée par Elie El khoury (AWS)

Récapitulatif

Ce modèle explique comment intégrer AWS Step Functions à AWS Systems Manager. Il utilise les intégrations de services du AWS SDK pour appeler l'startAutomationExecutionAPI Systems Manager à l'aide d'un jeton de tâche issu d'un flux de travail basé sur une machine à états, et fait une pause jusqu'à ce que le jeton revienne en cas de réussite ou d'échec d'un appel. Pour démontrer l'intégration, ce modèle implémente un wrapper de document d'automatisation (runbook) autour du `AWS-RunPowerShellScript` document `AWS-RunShellScript` or, et l'utilise `.waitForTaskToken` pour appeler ou de manière synchrone. `AWS-RunShellScript` `AWS-RunPowerShellScript` Pour plus d'informations sur les intégrations de services AWS SDK dans Step Functions, consultez le guide du AWS Step Functions développeur.

Step Functions est un service de flux de travail visuel à faible code que vous pouvez utiliser pour créer des applications distribuées, automatiser les processus informatiques et commerciaux, et créer des pipelines de données et d'apprentissage automatique à l'aide de AWS services. Les flux de travail gèrent les échecs, les nouvelles tentatives, la parallélisation, les intégrations de services et l'observabilité afin que vous puissiez vous concentrer sur une logique métier à plus forte valeur ajoutée.

L'automatisation, une fonctionnalité de AWS Systems Manager, simplifie les tâches courantes de maintenance, de déploiement et de correction pour Services AWS Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS), Amazon Redshift et Amazon Simple Storage Service (Amazon S3). L'automatisation vous permet de contrôler de manière précise la simultanéité de vos automatisations. Par exemple, vous pouvez spécifier le nombre de ressources à cibler simultanément et le nombre d'erreurs susceptibles de se produire avant l'arrêt d'une automatisation.

Pour les détails de mise en œuvre, y compris les étapes du runbook, les paramètres et les exemples, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un AWS compte actif
- AWS Identity and Access Management Autorisations (IAM) pour accéder à Step Functions et Systems Manager
- Une EC2 instance sur laquelle l'agent Systems Manager (agent SSM) est installé
- Un profil d'instance IAM pour Systems Manager attaché à l'instance sur laquelle vous prévoyez d'exécuter le runbook
- Un rôle Step Functions doté des autorisations IAM suivantes (selon le principe du moindre privilège) :

```
{
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": "*"
 }
```

Versions du produit

- Schéma de document SSM version 0.3 ou ultérieure
- Agent SSM version 2.3.672.0 ou ultérieure

Architecture

Pile technologique cible

- AWS Step Functions
- AWS Systems Manager Automatisation

Architecture cible

Automatisation et mise à l'échelle

- Ce modèle fournit un AWS CloudFormation modèle que vous pouvez utiliser pour déployer les runbooks sur plusieurs instances. (Voir le référentiel d'implémentation de GitHub Step Functions et Systems Manager.)

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.

Code

Le code de ce modèle est disponible dans le référentiel d'implémentation de GitHub Step Functions and Systems Manager.

Épopées

Créez des runbooks

Tâche	Description	Compétences requises
Téléchargez le CloudFormation modèle.	Téléchargez le `ssm-automation-documents.cfn.json` modèle depuis le `cloudformation` dossier du GitHub référentiel.	AWS DevOps
Créez des runbooks.	Connectez-vous au AWS Management Console, ouvrez la AWS CloudFormation console et déployez le	AWS DevOps

Tâche	Description	Compétences requises
	modèle. Pour plus d'informations sur le déploiement CloudFormation de modèles, consultez la section Création d'une pile sur la AWS CloudFormation console dans la CloudFormation documentation. Le CloudFormation modèle déploie trois ressources : • `SfnRunCommandByInstanceIds` — Runbook qui vous permet d'exécuter `AWS-RunShellScript` ou `AWS-RunPowerShellScript` d'utiliser une instance IDs. • `SfnRunCommandByTargets` — Runbook qui vous permet de courir `AWS-RunShellScript` ou d'utiliser `AWS-RunPowerShellScript` des cibles. • `SSMSyncRole` — Le rôle IAM assumé par les runbooks.	

Création d'un exemple de machine à états

Tâche	Description	Compétences requises
Créez une machine à états de test.	Suivez les instructions du guide du AWS Step Functions développeur pour créer et exécuter une machine à états. Pour la définition, utilisez le code suivant. Assurez-vous de mettre à jour la `InstanceIds` valeur avec l'ID d'une instance valide compatible avec Systems Manager dans votre compte. `{ "Comment": "A description of my state machine", "StartAt": "StartAutomationWaitForCallBack", "States": { "StartAutomationWaitForCallBack": { "Type": "Task", "Resource": "arn:aws:states:::aws-sdk:ssm:startAutomationExecution.waitForTaskToken", "Parameters": { "DocumentName": "SfnRunCommandByInstanceIds", "Parameters": { "InstanceIds": ["i-1234567890abcdef0"`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>],
	          "taskToken.
	$": "States.Array($$.T
	ask.Token)",
	          "workingD
	irectory": [
	            "/home/ssm-
	user/"
	          ],
	          "Commands": [
	            "echo \"This
	 is a test running
	 automation waitForTa
	skToken\" >> automatio
	n.log",
	            "sleep 100"
	          ],
	          "executio
	nTimeout": [
	              "10800"
	          ],
	          "delivery
	Timeout": [
	              "30"
	          ],
	          "shell": [
	              "Shell"
	          ]
	            }
	      },
	      "End": true
	    }
	  }
	}</pre> Ce code appelle le runbook pour exécuter deux commandes illustrant l'`waitForTaskToken` appel	

Tâche	Description	Compétences requises
	à Systems Manager Automation. La valeur du `shell` paramètre (`ShellouPowerShell`) détermine si le document d'automatisation s'exécute `AWS-RunShellScript` ou`AWS-RunPowerShellScript` . La tâche écrit « Ceci est un waitForTask jeton d'automatisation de test » dans le `/home/ssm-user/automation.log` fichier, puis s'arrête pendant 100 secondes avant de répondre avec le jeton de tâche et de libérer la tâche suivante dans le flux de travail. Si vous souhaitez plutôt appeler le `SfnRunCommandByTargets` runbook, remplacez la `Parameters` section du code précédent par la suivante : `"Parameters": { "Targets": [ { "Key": "InstanceIds", "Values": [`	

Tâche	Description	Compétences requises

	<pre>"i-02573cafcfEXAMPLE",
	"i-0471e04240EXAMPLE"
	]
	}
	],</pre>	

Mettez à jour le rôle IAM pour la machine d'état.	L'étape précédente crée automatiquement un rôle IAM dédié pour la machine à états. Cependant, il n'accorde pas l'autorisation d'appeler le runbook. Mettez à jour le rôle en ajoutant les autorisations suivantes :
	<pre>{
	"Effect": "Allow",
	"Action": "ssm:StartAutomationExecution",
	"Resource": "*"
	}</pre>
		AWS DevOps

Validez les appels synchrones.	Exécutez la machine d'état pour valider l'appel synchrone entre Step Functions et Systems Manager Automation. Pour un exemple de sortie, consultez la section Informations supplémentaires.	AWS DevOps

Ressources connexes

- Mise en route avec AWS Step Functions (Guide AWS Step Functions du développeur)
- Attendez un rappel avec le jeton de tâche (guide du AWS Step Functions développeur, modèles d'intégration des services)
- Appels d'API send_task_success et send_task_failure (documentation Boto3)
- AWS Systems Manager Automatisation (guide de AWS Systems Manager l'utilisateur)

Informations supplémentaires

Détails de l'implémentation

Ce modèle fournit un CloudFormation modèle qui déploie deux runbooks de Systems Manager :

- `SfnRunCommandByInstanceIds`exécute la `AWS-RunPowerShellScript` commande `AWS-RunShellScript` or en utilisant l'instance IDs.
- `SfnRunCommandByTargets`exécute la `AWS-RunPowerShellScript` commande `AWS-RunShellScript` or en utilisant des cibles.

Chaque runbook met en œuvre quatre étapes pour obtenir un appel synchrone lors de l'utilisation de l'`.waitForTaskToken`option dans Step Functions.

Step (Étape)	Action	Description
1	`Branch`	Vérifie la valeur du `shell` paramètre (`ShellouPowerShell`) pour décider s'il convient de l'exécuter `AWS-RunShellScript` pour Linux ou `AWS-RunPowerShellScript` pour Windows.
2	`RunCommand_Shell` ou `RunCommand_PowerShell`	Prend plusieurs entrées et exécute la `RunPowerShellScript` commande `RunShellScript` or. Pour

		plus d'informations, consultez l'onglet Détails du document `RunCommand_Shell` ou `RunCommand_PowerShell` Automation sur la console Systems Manager.
3	`SendTaskFailure`	S'exécute lorsque l'étape 2 est abandonnée ou annulée. Il appelle l'API send_task_failure de Step Functions, qui accepte trois paramètres en entrée : le jeton transmis par la machine d'état, l'erreur de défaillance et une description de la cause de la panne.
4	`SendTaskSuccess`	S'exécute lorsque l'étape 2 est réussie. Il appelle l'API send_task_success de Step Functions, qui accepte le jeton transmis par la machine d'état en entrée.

Paramètres du Runbook

`SfnRunCommandByInstanceIds`carnet de course :

Nom du paramètre	Type	Facultatif ou obligatoire	Description
`shell`	Chaîne	Obligatoire	L'interpréteur de commandes des instances permet de décider s'ils `AWS-RunShellScript` doivent être exécutés

			sous Linux ou `AWS-RunPowerShellScript` sous Windows.
`deliveryTimeout`	Entier	Facultatif	Temps d'attente, en secondes, avant qu'une commande soit remise à l'agent SSM sur une instance. Ce paramètre a une valeur minimale de 30 (0,5 minute) et une valeur maximale de 2592000 (720 heures).
`executionTimeout`	Chaîne	Facultatif	Durée, en secondes, nécessaire à l'exécution d'une commande avant qu'elle ne soit considérée comme ayant échoué. La valeur par défaut est 3 600 (1 heure). La valeur maximale est 172800 (48 heures).
`workingDirectory`	Chaîne	Facultatif	Chemin d'accès au répertoire de travail sur votre instance.
`Commands`	StringList	Obligatoire	Le script ou la commande shell à exécuter.

`InstanceIds`	StringList	Obligatoire	Les IDs instances dans lesquelles vous souhaitez exécuter la commande.
`taskToken`	Chaîne	Obligatoire	Le jeton de tâche à utiliser pour les réponses de rappel.

`SfnRunCommandByTargets`carnet de course :

Nom	Type	Facultatif ou obligatoire	Description
`shell`	Chaîne	Obligatoire	L'interpréteur de commandes des instances permet de décider s'ils `AWS-RunShellScript` doivent être exécutés sous Linux ou `AWS-RunPowerShellScript` sous Windows.
`deliveryTimeout`	Entier	Facultatif	Temps d'attente, en secondes, avant qu'une commande soit remise à l'agent SSM sur une instance. Ce paramètre a une valeur minimale de 30 (0,5 minute) et une valeur maximale

			de 2592000 (720 heures).
`executionTimeout`	Entier	Facultatif	Durée, en secondes, nécessaire à l'exécution d'une commande avant qu'elle ne soit considérée comme ayant échoué. La valeur par défaut est 3 600 (1 heure). La valeur maximale est 172800 (48 heures).
`workingDirectory`	Chaîne	Facultatif	Chemin d'accès au répertoire de travail sur votre instance.
`Commands`	StringList	Obligatoire	Le script ou la commande shell à exécuter.
`Targets`	MapList	Obligatoire	Tableau de critères de recherche qui identifie les instances à l'aide de paires clé-valeur que vous spécifiez. Par exemple : `[{"Key":"InstanceIds","Values":["i-02573cafcfEXAMPLE","i-0471e04240EXAMPLE"]}]`

`taskToken`	Chaîne	Obligatoire	Le jeton de tâche à utiliser pour les réponses de rappel.

Exemple de sortie

Le tableau suivant fournit un exemple de sortie de la fonction step. Cela montre que le temps d'exécution total est supérieur à 100 secondes entre l'étape 5 (`TaskSubmitted`) et l'étape 6 (`TaskSucceeded`). Cela montre que la fonction step a attendu la fin de la `sleep 100` commande avant de passer à la tâche suivante du flux de travail.

ID	Type	Step (Étape)	Ressource	Temps écoulé (ms)	Horodatage
1	`Execution Started`		-	0	11 mars 2022 14h50:34 ,303
2	`TaskState Entered`	`StartAutomationWaitForCallBack`	-	40	11 mars 2022 14 h 50 : 34 .343
3	`TaskScheduled`	`StartAutomationWaitForCallBack`	-	40	11 mars 2022 14 h 50 : 34 .343
4	`TaskStarted`	`StartAutomationWaitForCallBack`	-	154	11 mars 2022 14 h 50 : 34 .457
5	`TaskSubmitted`	`StartAutomationWaitForCallBack`	-	657	11 mars 2022 14 h 50 : 34 960

6	TaskSucceeded	StartAutomationWaitForCallBack	-	103835	11 mars 2022 14h52:18 138
7	TaskStateExited	StartAutomationWaitForCallBack	-	103860	11 mars 2022 14h52:18 163
8	ExecutionSucceeded		-	103897	11 mars 2022 14h52:18 200

Exécuter des lectures parallèles d'objets S3 en utilisant Python dans une AWS Lambda fonction

Créée par Eduardo Bortoluzzi (AWS)

Récapitulatif

Vous pouvez utiliser ce modèle pour récupérer et résumer une liste de documents à partir des buckets Amazon Simple Storage Service (Amazon S3) en temps réel. Le modèle fournit un exemple de code pour lire en parallèle des objets à partir de compartiments S3 sur Amazon Web Services (AWS). Le modèle montre comment exécuter efficacement des tâches liées aux E/S avec des AWS Lambda fonctions utilisant Python.

Une société financière a utilisé ce modèle dans une solution interactive pour approuver ou rejeter manuellement les transactions financières corrélées en temps réel. Les documents relatifs aux transactions financières étaient stockés dans un compartiment S3 lié au marché. Un opérateur a sélectionné une liste de documents dans le compartiment S3, a analysé la valeur totale des transactions calculées par la solution et a décidé d'approuver ou de rejeter le lot sélectionné.

Les tâches liées aux E/S prennent en charge plusieurs threads. Dans cet exemple de code, le fichier concurrent.futures. ThreadPoolExecutorest utilisé avec un maximum de 30 threads simultanés, même si les fonctions Lambda prennent en charge jusqu'à 1 024 threads (l'un de ces threads étant votre processus principal). Cette limite est due au fait qu'un trop grand nombre de threads crée des problèmes de latence en raison du changement de contexte et de l'utilisation des ressources informatiques. Vous devez également augmenter le nombre maximum de connexions au pool `botocore` afin que tous les threads puissent effectuer le téléchargement de l'objet S3 simultanément.

L'exemple de code utilise un objet de 8,3 Ko, avec des données JSON, dans un compartiment S3. L'objet est lu plusieurs fois. Une fois que la fonction Lambda a lu l'objet, les données JSON sont décodées en un objet Python. En décembre 2024, le résultat après l'exécution de cet exemple était de 1 000 lectures traitées en 2,3 secondes et de 10 000 lectures traitées en 27 secondes à l'aide d'une fonction Lambda configurée avec 2 304 Mo de mémoire. AWS Lambda prend en charge les configurations de mémoire de 128 Mo à 10 240 Mo (10 Go), mais l'augmentation de la mémoire Lambda au-delà de 2 304 Mo n'a pas contribué à réduire le temps d'exécution de cette tâche spécifique liée aux E/S.

L'outil AWS Lambda Power Tuning a été utilisé pour tester différentes configurations de mémoire Lambda et vérifier le meilleur performance-to-cost ratio pour la tâche. Pour les résultats des tests, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Maîtrise du développement en Python

Limites

- Une fonction Lambda peut comporter au maximum 1 024 processus ou threads d'exécution.
- Comptes AWS Les nouveaux ont une limite de mémoire Lambda de 3 008 Mo. Réglez l'outil AWS Lambda Power Tuning en conséquence. Pour plus d'informations, consultez la section Dépannage.
- Amazon S3 impose une limite de 5 500 requêtes GET/HEAD par seconde et par préfixe partitionné.

Versions du produit

- Python 3.9 ou version ultérieure
- AWS Cloud Development Kit (AWS CDK) v2
- AWS Command Line Interface (AWS CLI) version 2
- AWS Lambda Power Tuning 4.3.6 (en option)

Architecture

Pile technologique cible

- AWS Lambda
- Amazon S3
- AWS Step Functions (si AWS Lambda Power Tuning est déployé)

Architecture cible

Le schéma suivant montre une fonction Lambda qui lit des objets depuis un compartiment S3 en parallèle. Le diagramme contient également un flux de travail Step Functions pour l'outil AWS Lambda Power Tuning afin d'affiner la mémoire des fonctions Lambda. Ce réglage précis permet d'atteindre un bon équilibre entre les coûts et les performances.

Automatisation et mise à l'échelle

Les fonctions Lambda évoluent rapidement lorsque cela est nécessaire. Pour éviter 503 erreurs de ralentissement causées par Amazon S3 en cas de forte demande, nous vous recommandons de limiter le dimensionnement.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK) La v2 est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code. L'exemple d'infrastructure a été créé pour être déployé avec AWS CDK.
- AWS Command Line InterfaceAWS CLIest un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande. Dans ce modèle, AWS CLI la version 2 est utilisée pour télécharger un exemple de fichier JSON.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service Amazon S3 est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous permet de combiner des AWS Lambda fonctions et d'autres services AWS pour créer des applications critiques pour l'entreprise.

Autres outils

- Python est un langage de programmation informatique polyvalent. La réutilisation des threads de travail inactifs a été introduite dans la version 3.8 de Python, et le code de fonction Lambda de ce modèle a été créé pour Python version 3.9 et versions ultérieures.

Référentiel de code

Le code de ce modèle est disponible dans le aws-lambda-parallel-download GitHub référentiel.

Bonnes pratiques

- Cette AWS CDK construction repose sur les autorisations Compte AWS utilisateur dont vous disposez pour déployer l'infrastructure. Si vous envisagez d'utiliser des AWS CDK pipelines ou des déploiements entre comptes, consultez la section Synthétiseurs Stack.
- Dans cet exemple d'application, les journaux d'accès ne sont pas activés dans le compartiment S3. Il est recommandé d'activer les journaux d'accès dans le code de production.

Épopées

Préparer l'environnement de développement

Tâche	Description	Compétences requises
Vérifiez la version de Python installée.	Ce code a été testé spécifiquement sur Python 3.9 et Python 3.13, et il devrait fonctionner sur toutes les versions entre ces versions. Pour vérifier votre version de Python, `python3 -V` lancez-la dans votre terminal et installez une version plus récente si nécessaire. Pour vérifier que les modules requis sont installés, exécutez`python3 -c "import pip, venv"`. L'absence de message d'erreur signifie que les modules sont correctement	Architecte du cloud

Tâche	Description	Compétences requises
	installés et que vous êtes prêt à exécuter cet exemple.	
Installez AWS CDK.	Pour installer le AWS CDK s'il n'est pas déjà installé, suivez les instructions de la section Mise en route avec le AWS CDK. Pour vérifier que la AWS CDK version installée est 2.0 ou ultérieure, exécutez`cdk --version`.	Architecte du cloud
Bootstrap votre environnement.	Pour démarrer votre environnement, si ce n'est pas déjà fait, suivez les instructions de la section Bootstrap votre environnement pour une utilisation avec le. AWS CDK	Architecte du cloud

Cloner le référentiel d'exemple

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner la dernière version du référentiel, exécutez la commande suivante : `git clone --depth 1 --branch v1.2.0 \ git@github.com:aws-samples/aws-lambda-parallel-download.git`	Architecte du cloud
Remplacez le répertoire de travail par le référentiel cloné.	Exécutez la commande suivante :	Architecte du cloud

Tâche	Description	Compétences requises
	`cd aws-lambda-parallel-download`	
Créez l'environnement virtuel Python.	Pour créer un environnement virtuel Python, exécutez la commande suivante : `python3 -m venv .venv`	Architecte du cloud
Activez l’environnement virtuel.	Pour activer l'environnement virtuel, exécutez la commande suivante : `source .venv/bin/activate`	Architecte du cloud
Installez les dépendances.	Pour installer les dépendances Python, exécutez la `pip` commande suivante : `pip install -r requirements.txt`	Architecte du cloud
Parcourez le code.	(Facultatif) L'exemple de code qui télécharge un objet depuis le compartiment S3 se trouve sur`resources/parallel.py` . Le code d'infrastructure se trouve dans le `parallel_download` dossier.	Architecte du cloud

Déployez et testez l'application

Tâche	Description	Compétences requises
Déployez l’application.	Exécutez `cdk deploy`. Notez les AWS CDK sorties : • `ParallelDownloadStack.LambdaFunctionARN` • `ParallelDownloadStack.SampleS3BucketName` • `ParallelDownloadStack.StateMachineARN`	Architecte du cloud
Téléchargez un exemple de fichier JSON.	Le référentiel contient un exemple de fichier JSON d'environ 9 Ko. Pour télécharger le fichier dans le compartiment S3 de la pile créée, exécutez la commande suivante : `aws s3 cp sample.json s3://<ParallelDownloadStack.SampleS3BucketName>` Remplacez `<ParallelDownloadStack.SampleS3BucketName>` par la valeur correspondante de la AWS CDK sortie.	Architecte du cloud

Tâche	Description	Compétences requises
Lancez l'application.	Pour exécuter l'application, procédez comme suit : 1. Connectez-vous au AWS Management Console, accédez à la console Lambda et recherchez la fonction Lambda dont l'ARN provient de la sortie. AWS CDK `ParallelDownloadStack.LambdaFunctionARN` 2. Dans l'onglet Test, modifiez le JSON de l'événement comme suit : `{"objectKey": "sample.json"}` 3. Sélectionnez Tester). 4. Pour voir le résultat, sélectionnez Détails. Les détails indiqueront les statistiques du téléchargement parallèle, les informations relatives à l'exécution et les journaux.	Architecte du cloud

Tâche	Description	Compétences requises
Ajoutez le nombre de téléchargements.	(Facultatif) Pour exécuter 1 500 appels d'objets get, utilisez le code JSON suivant dans le JSON d'événement du `Test` paramètre : `{"repeat": 1500, "objectKey": "sample.json"}`	Architecte du cloud

Facultatif : exécutez AWS Lambda Power Tuning

Tâche	Description	Compétences requises
Exécutez l'outil AWS Lambda Power Tuning.	1. Connectez-vous à la console et accédez à Step Functions. 2. Localisez la machine à états dont l'ARN provient de la AWS CDK sortie `ParallelDownloadStack.StateMachineARN` . 3. Choisissez Démarrer l'exécution, puis collez le code JSON suivant : `{ "lambdaARN": "<ParallelDownloadStack.LambdaFunctionARN>", "num": 10, "strategy": "balanced",`	Architecte du cloud

Tâche	Description	Compétences requises

	<pre>"payload":
	{"repeat": 2000,
	"objectKey":
	"sample.json"}
	}</pre>
	N'oubliez pas de `<ParallelDownloadStack.LambdaFunctionARN>` remplacer par la valeur de la AWS CDK sortie.
	
	À la fin de l'exécution, le résultat sera affiché dans l'onglet d'entrée et de sortie d'exécution.	

Affichez les résultats du AWS Lambda Power Tuning sous forme de graphique.	Dans l'onglet Entrée et sortie d'exécution, copiez le lien de `visualization` propriété et collez-le dans un nouvel onglet du navigateur.	Architecte du cloud

Nettoyage

Tâche	Description	Compétences requises

Supprimez les objets du compartiment S3.	Avant de détruire les ressources déployées, vous devez supprimer tous les objets du compartiment S3 :
	
	<pre>aws s3 rm s3://<Par
	allelDownloadStack</pre>
		Architecte du cloud

Tâche	Description	Compétences requises
	`.SampleS3BucketName> \ --recursive` N'oubliez pas `<ParallelDownloadStack.SampleS3BucketName>` de remplacer par la valeur des AWS CDK sorties.	
Détruisez les ressources.	Pour détruire toutes les ressources créées pour ce pilote, exécutez la commande suivante : `cdk destroy`	Architecte du cloud

Résolution des problèmes

Problème	Solution
`'MemorySize' value failed to satisfy constraint: Member must have value less than or equal to 3008`	Pour les nouveaux comptes, il se peut que vous ne puissiez pas configurer plus de 3 008 Mo dans vos fonctions Lambda. Pour tester l'utilisation de AWS Lambda Power Tuning, ajoutez la propriété suivante au JSON d'entrée lorsque vous démarrez l'exécution de Step Functions : `"powerValues": [ 512, 1024, 1536, 2048, 2560, 3008`

Problème	Solution
	]]

Ressources connexes

- Python — concurrent.futures. ThreadPoolExecutor
- Quotas Lambda : configuration, déploiement et exécution des fonctions
- Travailler avec le AWS CDK en Python
- Fonctions de profilage avec AWS Lambda Power Tuning

Informations supplémentaires

Code

L'extrait de code suivant exécute le traitement des E/S parallèles :

```
with ThreadPoolExecutor(max_workers=MAX_WORKERS) as executor:
  for result in executor.map(a_function, (the_arguments)):
    ...
```

Les fils `ThreadPoolExecutor` de discussion sont réutilisés lorsqu'ils sont disponibles.

Tests et résultats

Ces tests ont été réalisés en décembre 2024.

Le premier test a traité 2 500 lectures d'objets, avec le résultat suivant.

À partir de 3 009 Mo, le temps de traitement est resté pratiquement le même quelle que soit l'augmentation de la mémoire, mais le coût a augmenté à mesure que la taille de la mémoire augmentait.

Un autre test a examiné la plage comprise entre 1 536 Mo et 3 072 Mo de mémoire, en utilisant des valeurs multiples de 256 Mo et en traitant 10 000 lectures d'objets, avec les résultats suivants.

Le meilleur performance-to-cost ratio a été obtenu avec la configuration Lambda de 2 304 Mo de mémoire.

À titre de comparaison, un processus séquentiel de 2 500 lectures d'objets a pris 47 secondes. Le processus parallèle utilisant la configuration Lambda de 2 304 Mo a pris 7 secondes, soit 85 % de moins.

Envoyez des données de télémétrie de AWS Lambda vers OpenSearch pour des analyses et des visualisations en temps réel

Créée par Tabby Ward (AWS), Guy Bachar (AWS) et David Kilzer (AWS)

Récapitulatif

Les applications modernes sont de plus en plus distribuées et axées sur les événements, ce qui renforce le besoin de surveillance et d'observabilité en temps réel. AWS Lambda est un service informatique sans serveur qui joue un rôle crucial dans la création d'architectures évolutives et axées sur les événements. Cependant, la surveillance et le dépannage des fonctions Lambda peuvent s'avérer difficiles si vous vous fiez uniquement à Amazon CloudWatch Logs, ce qui peut entraîner une latence et des périodes de rétention limitées.

Pour relever ce défi, nous avons AWS introduit l'API de télémétrie Lambda, qui permet aux fonctions Lambda d'envoyer des données de télémétrie directement à des outils de surveillance et d'observabilité tiers. Cette API prend en charge le streaming en temps réel des journaux, des métriques et des traces, et fournit une vue complète et opportune des performances et de l'état de vos fonctions Lambda.

Ce modèle explique comment intégrer l'API de télémétrie Lambda à un moteur OpenSearchde recherche et d'analyse distribué open source. OpenSearch propose une plate-forme puissante et évolutive pour l'ingestion, le stockage et l'analyse de gros volumes de données, ce qui en fait un choix idéal pour les données de télémétrie Lambda. Plus précisément, ce modèle montre comment envoyer des journaux à partir d'une fonction Lambda écrite en Python directement à un OpenSearch cluster en utilisant une extension Lambda fournie par. AWS Cette solution est flexible et personnalisable. Vous pouvez donc créer votre propre extension Lambda ou modifier l'exemple de code source pour modifier le format de sortie comme vous le souhaitez.

Le modèle explique comment configurer l'intégration de l'API de télémétrie Lambda avec OpenSearch, et inclut les meilleures pratiques en matière de sécurité, d'optimisation des coûts et d'évolutivité. L'objectif est de vous aider à mieux comprendre vos fonctions Lambda et à améliorer l'observabilité globale de vos applications sans serveur.

> **Note**
>
> Ce modèle se concentre sur l'intégration de l'API de télémétrie Lambda à Managed. OpenSearch Toutefois, les principes et techniques présentés sont également applicables à l'autogestion OpenSearch et à Elasticsearch.

Conditions préalables et limitations

Avant de commencer le processus d'intégration, assurez-vous que les conditions préalables suivantes sont réunies :

Compte AWS: un actif Compte AWS doté des autorisations appropriées pour créer et gérer les AWS ressources suivantes :

- AWS Lambda
- AWS Identity and Access Management (JE SUIS)
- Amazon OpenSearch Service (si vous utilisez un OpenSearch cluster géré)

OpenSearch grappe :

- Vous pouvez utiliser un OpenSearch cluster autogéré existant ou un service géré tel que OpenSearch Service.
- Si vous utilisez OpenSearch Service, configurez votre OpenSearch cluster en suivant les instructions de la section Getting started with Amazon OpenSearch Service dans la documentation du OpenSearch Service.
- Assurez-vous que le OpenSearch cluster est accessible depuis votre fonction Lambda et qu'il est configuré avec les paramètres de sécurité nécessaires, tels que les politiques d'accès, le chiffrement et l'authentification.
- Configurez le OpenSearch cluster avec les mappages d'index et les paramètres nécessaires pour ingérer les données de télémétrie Lambda. Pour plus d'informations, consultez la section Chargement de données de streaming dans Amazon OpenSearch Service dans la documentation du OpenSearch service.

Connectivité réseau :

- Assurez-vous que votre fonction Lambda dispose de la connectivité réseau nécessaire pour accéder au OpenSearch cluster. Pour obtenir des conseils sur la configuration des paramètres du cloud privé virtuel (VPC), consultez la section Lancement de vos domaines Amazon OpenSearch Service au sein d'un VPC dans la documentation du service. OpenSearch

Rôles et politiques IAM :

- Créez un rôle IAM avec les autorisations nécessaires pour que votre fonction Lambda puisse accéder au cluster et accéder OpenSearch à vos informations d'identification qui y sont stockées. AWS Secrets Manager
- Associez les politiques IAM appropriées au rôle, telles que la `AWSLambdaBasicExecutionRole` politique et les autorisations supplémentaires requises pour interagir avec OpenSearch.
- Vérifiez que les autorisations IAM accordées à votre fonction Lambda lui permettent d'écrire des données dans le cluster. OpenSearch Pour plus d'informations sur la gestion des autorisations IAM, consultez la section Définition des autorisations de fonction Lambda avec un rôle d'exécution dans la documentation Lambda.

Connaissances du langage de programmation :

- Vous devez avoir des connaissances de base en Python (ou le langage de programmation de votre choix) pour comprendre et modifier l'exemple de code de la fonction Lambda et de l'extension Lambda.

Environnement de développement :

- Configurez un environnement de développement local avec les outils et les dépendances nécessaires pour créer et déployer des fonctions et des extensions Lambda.

AWS CLI ou AWS Management Console :

- Installez et configurez le AWS Command Line Interface (AWS CLI) ou utilisez-le AWS Management Console avec les informations d'identification appropriées pour interagir avec les informations requises Services AWS.

Surveillance et journalisation :

- Familiarisez-vous avec les meilleures pratiques en matière de surveillance et de journalisation AWS, notamment sur des services tels qu'Amazon CloudWatch et à des AWS CloudTrail fins de surveillance et d'audit.
- Consultez les CloudWatch journaux de votre fonction Lambda afin d'identifier les erreurs ou exceptions liées à l'intégration de l'API de télémétrie Lambda. Pour obtenir des conseils de dépannage, consultez la documentation de l'API de télémétrie Lambda.

Architecture

Ce modèle utilise le OpenSearch service pour stocker les journaux et les données de télémétrie générés par les fonctions Lambda. Cette approche vous permet de diffuser rapidement les journaux directement vers votre OpenSearch cluster, ce qui réduit la latence et les coûts associés à l'utilisation CloudWatch des journaux comme intermédiaire.

> **Note**
>
> Votre code d'extension Lambda peut transférer la télémétrie à OpenSearch Service, soit en utilisant directement l' OpenSearch API, soit en utilisant une bibliothèque cliente. OpenSearch L'extension Lambda peut utiliser les opérations en masse prises en charge par l' OpenSearch API pour regrouper des événements de télémétrie et les envoyer au OpenSearch Service en une seule demande.

Le schéma de flux de travail suivant illustre le flux de travail de journalisation des fonctions Lambda lorsque vous utilisez un OpenSearch cluster comme point de terminaison.

L'architecture inclut les composants suivants :

- Fonction Lambda : fonction sans serveur qui génère des journaux et des données de télémétrie lors de l'exécution.
- Extension Lambda : extension basée sur Python qui utilise l'API de télémétrie Lambda pour s'intégrer directement au cluster. OpenSearch Cette extension s'exécute parallèlement à la fonction Lambda dans le même environnement d'exécution.

- API de télémétrie Lambda : API qui permet aux extensions Lambda d'envoyer des données de télémétrie, notamment des journaux, des métriques et des traces, directement à des outils de surveillance et d'observabilité tiers.
- Cluster Amazon OpenSearch Service : OpenSearch cluster géré hébergé sur AWS. Ce cluster est chargé d'ingérer, de stocker et d'indexer les données de journal diffusées par la fonction Lambda via l'extension Lambda.

Le flux de travail comprend les étapes suivantes :

1. La fonction Lambda est appelée et génère des journaux et des données de télémétrie lors de son exécution.
2. L'extension Lambda s'exécute parallèlement à la fonction permettant de capturer les journaux et les données de télémétrie à l'aide de l'API de télémétrie Lambda.
3. L'extension Lambda établit une connexion sécurisée avec le cluster de OpenSearch services et diffuse les données du journal en temps réel.
4. Le cluster de OpenSearch services ingère, indexe et stocke les données du journal pour les rendre disponibles à des fins de recherche, d'analyse et de visualisation à l'aide d'outils tels que Kibana ou d'autres applications compatibles.

En contournant les CloudWatch journaux et en envoyant les données des journaux directement au OpenSearch cluster, cette solution offre plusieurs avantages :

- Streaming et analyse des journaux en temps réel, permettant un dépannage plus rapide et une meilleure observabilité.
- Réduction de la latence et des limites de rétention potentielles associées aux CloudWatch journaux.
- Possibilité de personnaliser l'extension Lambda ou de créer votre propre extension pour des formats de sortie spécifiques ou des traitements supplémentaires.
- Intégration aux fonctionnalités de recherche, d'analyse et de visualisation de OpenSearch Service pour l'analyse et la surveillance des journaux.

La section Epics fournit des step-by-step instructions pour configurer l'extension Lambda, configurer la fonction Lambda et intégrer le cluster de services. OpenSearch Pour les considérations relatives à la sécurité, les stratégies d'optimisation des coûts et les conseils de surveillance et de dépannage de la solution, consultez la section Bonnes pratiques.

Outils

Services AWS

- AWS Lambda est un service informatique qui vous permet d'exécuter un code sans demander la mise en service ou la gestion des serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon OpenSearch Service est un service entièrement géré fourni par AWS qui facilite le déploiement, l'exploitation et le dimensionnement des OpenSearch clusters dans le cloud.
- Les extensions Lambda étendent les fonctionnalités de vos fonctions Lambda en exécutant du code personnalisé à côté de celles-ci. Vous pouvez utiliser les extensions Lambda pour intégrer Lambda à divers outils de surveillance, d'observabilité, de sécurité et de gouvernance.
- AWS Lambda L'API de télémétrie vous permet d'utiliser des extensions pour capturer des données de surveillance et d'observabilité améliorées directement depuis Lambda et les envoyer vers la destination de votre choix.
- AWS CloudFormationvous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications.

Référentiels de code

- AWS Lambda Les extensions incluent des démos et des exemples de projets élaborés par des AWS partenaires AWS et destinés à vous aider à créer vos propres extensions.
- Example Lambda Telemetry Integrations for fournit OpenSearch un exemple d'extension Lambda qui montre comment envoyer des journaux depuis une fonction Lambda vers un cluster. OpenSearch

Autres outils

- OpenSearchest un moteur de recherche et d'analyse distribué open source qui fournit une plate-forme puissante pour l'ingestion, le stockage et l'analyse de gros volumes de données.
- Kibana est un outil de visualisation et d'exploration de données open source que vous pouvez utiliser. OpenSearch Notez que la mise en œuvre de la visualisation et de l'analyse dépasse le cadre de ce modèle. Pour plus d'informations, consultez la documentation de Kibana et d'autres ressources.

Bonnes pratiques

Lorsque vous intégrez l'API de télémétrie Lambda à OpenSearch, tenez compte des meilleures pratiques suivantes.

Sécurité et contrôle d'accès

- Communication sécurisée : chiffrez toutes les communications entre vos fonctions Lambda et OpenSearch le cluster à l'aide du protocole HTTPS. Configurez les paramètres SSL/TLS nécessaires dans votre extension et configuration Lambda. OpenSearch
- Autorisations IAM :
  - Les extensions s'exécutent dans le même environnement d'exécution que la fonction Lambda. Elles héritent donc du même niveau d'accès aux ressources telles que le système de fichiers, le réseau et les variables d'environnement.
  - Accordez les autorisations IAM minimales nécessaires à vos fonctions Lambda pour accéder à l'API de télémétrie Lambda et écrire des données dans le cluster. OpenSearch Utilisez le principe du moindre privilège pour limiter l'étendue des autorisations.
- OpenSearch contrôle d'accès : implémentez un contrôle d'accès précis dans votre OpenSearch cluster afin de restreindre l'accès aux données sensibles. Utilisez les fonctionnalités de sécurité intégrées, telles que l'authentification des utilisateurs, le contrôle d'accès basé sur les rôles et les autorisations au niveau de l'index, dans. OpenSearch
- Extensions fiables : installez toujours les extensions provenant d'une source fiable uniquement. Utilisez des outils d'infrastructure en tant que code (IaC) AWS CloudFormation pour simplifier le processus consistant à associer la même configuration d'extension, y compris les autorisations IAM, à plusieurs fonctions Lambda. Les outils IaC fournissent également un enregistrement d'audit des extensions et des versions utilisées précédemment.
- Gestion des données sensibles : lors de la création d'extensions, évitez de consigner des données sensibles. Nettoyez les charges utiles et les métadonnées avant de les enregistrer ou de les conserver à des fins d'audit.

Optimisation des coûts

- Surveillance et alertes : configurez des mécanismes de surveillance et d'alerte pour suivre le volume de données envoyées OpenSearch depuis vos fonctions Lambda. Cela vous aidera à identifier les éventuels dépassements de coûts et à y remédier.

- Conservation des données : réfléchissez soigneusement à la période de conservation des données appropriée pour vos données de télémétrie Lambda dans. OpenSearch Des périodes de rétention plus longues peuvent augmenter les coûts de stockage. Trouvez donc un équilibre entre vos besoins d'observabilité et l'optimisation des coûts.
- Compression et indexation : activez la compression des données et optimisez votre stratégie d' OpenSearch indexation afin de réduire l'encombrement de stockage de vos données de télémétrie Lambda.
- Réduction de la dépendance à l'égard de CloudWatch : en intégrant directement l'API de télémétrie Lambda OpenSearch, vous pouvez potentiellement réduire votre dépendance à l'égard des CloudWatch journaux, ce qui peut entraîner des économies de coûts. En effet, l'API de télémétrie Lambda vous permet d'envoyer des journaux directement à OpenSearch, ce qui évite d'avoir à stocker et à traiter les données. CloudWatch

Évolutivité et fiabilité

- Traitement asynchrone : utilisez des modèles de traitement asynchrones, tels qu'Amazon Simple Queue Service (Amazon SQS) ou Amazon Kinesis, pour dissocier l'exécution de la fonction Lambda de l'ingestion de données. OpenSearch Cela permet de maintenir la réactivité de vos fonctions Lambda et d'améliorer la fiabilité globale du système.
- OpenSearch dimensionnement du cluster : surveillez les performances et l'utilisation des ressources de votre OpenSearch cluster, et augmentez-le ou diminuez-le selon les besoins pour gérer le volume croissant de données de télémétrie Lambda.
- Basculement et reprise après sinistre : mettez en œuvre une stratégie de reprise après sinistre robuste pour votre OpenSearch cluster, notamment des sauvegardes régulières et la capacité de restaurer rapidement les données en cas de panne.

Observabilité et surveillance

- Tableaux de bord et visualisations : utilisez Kibana ou d'autres outils de tableau de bord pour créer des tableaux de bord et des visualisations personnalisés qui fournissent des informations sur les performances et l'état de vos fonctions Lambda en fonction des données de télémétrie contenues dans. OpenSearch
- Alertes et notifications : configurez des alertes et des notifications pour surveiller de manière proactive les anomalies, les erreurs ou les problèmes de performance dans vos fonctions Lambda. Intégrez ces alertes et notifications à vos processus de gestion des incidents existants.

- Suivi et corrélation : assurez-vous que vos données de télémétrie Lambda incluent des informations de suivi pertinentes, telles que les demandes IDs ou les corrélations IDs, afin de permettre l' end-to-endobservabilité et le dépannage dans l'ensemble de vos applications distribuées sans serveur.

En suivant ces bonnes pratiques, vous pouvez vous assurer que votre intégration de l'API de télémétrie Lambda OpenSearch est sécurisée, rentable et évolutive, et qu'elle fournit une observabilité complète pour vos applications sans serveur.

Épopées

Création et déploiement de la couche d'extension Lambda

Tâche	Description	Compétences requises
Téléchargez le code source.	Téléchargez les exemples d'extensions depuis le référentiel d'AWS Lambda extensions.	Développeur d'applications, architecte cloud
Accédez au dossier `python-example-telemetry-opensearch-extension` .	Le référentiel d'AWS Lambda extensions que vous avez téléchargé contient de nombreux exemples relatifs à plusieurs cas d'utilisation et à plusieurs environnements d'exécution de langage. Accédez au dossier python-example-telemetry-opensearch-extension pour utiliser l' OpenSearch extension Python, qui envoie les journaux à OpenSearch.	Développeur d'applications, architecte cloud
Ajoutez des autorisations pour exécuter le point de terminaison de l'extension.	Exécutez la commande suivante pour rendre le point de terminaison de l'extension exécutable :	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	`chmod +x python-example-telemetry-opensearch-extension/extension.py`	
Installez les dépendances de l'extension localement.	Exécutez la commande suivante pour installer les dépendances locales pour le code Python : `pip3 install -r python-example-telemetry-opensearch-extension/requirements.txt -t ./python-example-telemetry-opensearch-extension/` Ces dépendances seront montées avec le code d'extension.	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises

Créez un package .zip pour l'extension afin de la déployer en tant que couche.	Le fichier d'extension .zip doit contenir un répertoire racine appelé`extensions/`, où se trouve le fichier exécutable de l'extension, et un autre répertoire racine appelé`python-example-telemetry-opensearch-extension/`, où se trouvent la logique de base de l'extension et ses dépendances.
	
	Créez le package .zip pour l'extension :
	
	`chmod +x extensions/python-example-telemetry-opensearch-extension`
	`zip -r extension.zip extensions python-example-telemetry-opensearch-extension`
		Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
Déployez l'extension en tant que couche Lambda.	Publiez la couche à l'aide de votre fichier d'extension .zip et de la commande suivante : `aws lambda publish-layer-version \ --layer-name "python-example-telemetry-opensearch-extension" \ --zip-file "fileb://extension.zip"`	Développeur d'applications, architecte cloud

Intégrez l'extension dans votre fonction

Tâche	Description	Compétences requises
Ajoutez la couche à votre fonction.	1. Connectez-vous à la page Fonctions de la AWS Lambda console AWS Management Console et ouvrez-la. 2. Sélectionnez votre fonction. 3. Sous Couches, choisissez Ajouter une couche. 4. Sous Choisir une couche, choisissez Couches personnalisées comme source de couche et ajoutez votre couche. Pour plus d'informations sur l'ajout d'une couche à votre	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	fonction Lambda, consultez la documentation Lambda.	

Tâche	Description	Compétences requises
Définissez les variables d'environnement pour la fonction.	Sur la page des fonctions, choisissez l'onglet Configuration et ajoutez les variables d'environnement suivantes à votre fonction : • `URL`— L'URI de votre OpenSearch point de terminaison où vos journaux seront envoyés. • `AUTH_SECRET` — L'ARN de vos OpenSearch informations d'identification stockées dans AWS Secrets Manager. Cela doit être stocké sous forme de paire clé-valeur et comporter deux clés : `username` et. `password` • `PLATFORM_INDEX` ,`FUNCTION_INDEX` , et `EXTENSION_INDEX` — Les noms des index qui stockeront vos données de télémétrie, vos journaux de fonctions et vos journaux d'extension. Assurez-vous qu'ils respectent les critères de dénomination appropriés. Dans le cas contraire, vos index ne seront pas créés. • `DISPATCH_MIN_BATCH_SIZE` — Le nombre	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	d'événements du journal que vous souhaitez regrouper. Toutefois, lorsque la fonction s'arrête, vos journaux seront envoyés quel que soit ce paramètre.	

Ajoutez des instructions de journalisation et testez votre fonction

Tâche	Description	Compétences requises

Ajoutez des instructions de journalisation à votre fonction.	Ajoutez des instructions de journalisation à votre fonction en utilisant l'un des mécanismes de journalisation intégrés ou le module de journalisation de votre choix.
	
	Voici des exemples de journalisation de messages en Python :
	
	`print("Your Log Message Here")`
	`logger = logging.getLogger(__name__)`
	
	`logger.info("Test Info Log.")`
	`logger.error("Test Error Log.")`
		Développeur d'applications, architecte cloud

Testez votre fonction .	1. Sur la page des fonctions, choisissez l'onglet Tester.	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	2. Créez un événement de test pour votre fonction et lancez le test. Pour plus d'informations, consultez la section Tester les fonctions Lambda dans la console dans la documentation Lambda. Vous devriez voir Exécution de la fonction : réussi si tout fonctionne correctement.	

Afficher vos identifiants OpenSearch

Tâche	Description	Compétences requises
Interrogez vos index.	Dans OpenSearch, exécutez la commande suivante pour interroger vos index : `SELECT * FROM index-name` Vos journaux devraient être affichés dans les résultats de la requête.	Architecte du cloud

Résolution des problèmes

Problème	Solution
Problèmes de connectivité	• Vérifiez que votre fonction Lambda dispose de la connectivité réseau nécessaire pour accéder au OpenSearch cluster. Consultez la documentation du OpenSearch service pour obtenir des conseils sur la configuration des paramètres VPC. • Vérifiez que les autorisations IAM accordées à votre fonction Lambda lui permetten t d'écrire des données dans le cluster. OpenSearch Consultez la documentation Lambda pour plus d'informations sur la gestion des autorisations IAM.
Erreurs d'ingestion de données	• Consultez les CloudWatch journaux de votre fonction Lambda afin d'identifier les erreurs ou exceptions liées à l'intégration de l'API de télémétrie Lambda. Consultez la documenta tion de l'API de télémétrie Lambda pour obtenir des conseils de dépannage. • Vérifiez que le OpenSearch cluster est correctement configuré et qu'il possède les mappages d'index et les paramètres nécessaires pour ingérer les données de télémétrie Lambda. Consultez la OpenSearc h documentation pour plus d'informations.

Ressources connexes

- Exemple d'intégrations de télémétrie Lambda pour (référentiel) OpenSearch GitHub
- Augmentez les fonctions Lambda à l'aide d'extensions Lambda (documentation Lambda)
- API de télémétrie Lambda (documentation Lambda)

- Présentation de l'API de AWS Lambda télémétrie (AWS article de blog)
- Intégration de l'API de AWS Lambda télémétrie à Prometheus et (article de blog) OpenSearch AWS

Informations supplémentaires

Modification de la structure du journal

Par défaut, l'extension envoie les journaux sous forme de document OpenSearch imbriqué à. Cela vous permet d'effectuer des requêtes imbriquées pour récupérer des valeurs de colonnes individuelles.

Si la sortie du journal par défaut ne répond pas à vos besoins spécifiques, vous pouvez la personnaliser en modifiant le code source de l'extension Lambda fournie par. AWS AWS encourage les clients à adapter le résultat aux besoins de leur entreprise. Pour modifier la sortie du journal, localisez la `dispatch_to_opensearch` fonction dans le `telemetry_dispatcher.py` fichier dans le code source de l'extension et apportez les modifications nécessaires.

Configuration d'un routeur cellulaire sans serveur pour une architecture basée sur les cellules

Créée par Mian Tariq (AWS) et Ioannis Lioupras (AWS)

Récapitulatif

En tant que point d'entrée du système global d'une application cellulaire, le routeur cellulaire est chargé d'affecter efficacement les utilisateurs aux cellules appropriées et de fournir les points de terminaison aux utilisateurs. Le routeur cellulaire gère des fonctions telles que le stockage des user-to-cell mappages, la surveillance de la capacité des cellules et la demande de nouvelles cellules en cas de besoin. Il est important de maintenir le fonctionnement du routeur cellulaire en cas d'interruption potentielle.

Dans ce modèle, le cadre de conception des routeurs cellulaires met l'accent sur la résilience, l'évolutivité et l'optimisation des performances globales. Le modèle utilise un routage statique, dans lequel les clients mettent en cache les points de terminaison lors de la connexion initiale et communiquent directement avec les cellules. Ce découplage améliore la résilience du système en garantissant le fonctionnement ininterrompu de l'application cellulaire en cas de défaillance d'un routeur cellulaire.

Ce modèle utilise un AWS CloudFormation modèle pour déployer l'architecture. Pour plus de détails sur ce que le modèle déploie, ou pour déployer la même configuration à l'aide du AWS Management Console, consultez la section Informations supplémentaires.

> **Important**
>
> La démonstration, le code et le AWS CloudFormation modèle présentés dans ce modèle sont uniquement destinés à des fins explicatives. Le matériel fourni est uniquement destiné à illustrer le modèle de conception et à faciliter la compréhension. La démo et le code ne sont pas prêts pour la production et ne doivent pas être utilisés pour des activités de production en direct. Toute tentative d'utilisation du code ou de la démo dans un environnement de production est fortement déconseillée et se fait à vos propres risques. Nous vous recommandons de consulter les professionnels appropriés et d'effectuer des tests approfondis avant d'implémenter ce modèle ou l'un de ses composants dans un environnement de production.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- La dernière version de AWS Command Line Interface (AWS CLI)
- Informations d'identification AWS avec les autorisations nécessaires pour créer la AWS CloudFormation pile, AWS Lambda les fonctions et les ressources associées

Versions du produit

- Python 3.12

Architecture

Le schéma suivant montre une conception de haut niveau du routeur cellulaire.

Le diagramme décrit le flux de travail suivant :

1. L'utilisateur contacte Amazon API Gateway, qui sert de façade aux points de terminaison de l'API du routeur cellulaire.
2. Amazon Cognito gère l'authentification et l'autorisation.
3. Le AWS Step Functions flux de travail comprend les éléments suivants :
   - Orchestrateur – `Orchestrator` Utilisations AWS Step Functions pour créer un flux de travail ou une machine à états. Le flux de travail est déclenché par l'API du routeur cellulaire. `Orchestrator`Exécute les fonctions Lambda en fonction du chemin de la ressource.
   - Dispatcher – La fonction `Dispatcher` Lambda identifie et affecte une cellule statique par nouvel utilisateur enregistré. La fonction recherche la cellule comportant le moins d'utilisateurs, l'affecte à l'utilisateur et renvoie les points de terminaison.
   - Mappeur – L'`Mapper`opération gère les user-to-cell mappages au sein de la `RoutingDB` base de données Amazon DynamoDB créée par le modèle. AWS CloudFormation Lorsqu'elle est déclenchée, la `Mapper` fonction fournit aux utilisateurs déjà assignés leurs points de terminaison.
   - Scaler – La `Scaler` fonction assure le suivi de l'occupation des cellules et de la capacité disponible. En cas de besoin, la `Scaler` fonction peut envoyer une demande via Amazon

Simple Queue Service (Amazon SQS) à la couche Provision and Deploy pour demander de nouvelles cellules.

- Validateur – La `Validator` fonction valide les extrémités des cellules et détecte tout problème potentiel.

4. `RoutingDB`Stocke les informations et les attributs des cellules (points de terminaison de l'API Région AWS, état, métriques).
5. Lorsque la capacité disponible des cellules dépasse un seuil, le routeur cellulaire demande des services de provisionnement et de déploiement via Amazon SQS pour créer de nouvelles cellules.

Lorsque de nouvelles cellules sont créées, elles sont mises `RoutingDB` à jour à partir de la couche Provision and Deploy. Toutefois, ce processus dépasse le cadre de ce modèle. Pour une vue d'ensemble des prémisses de conception de l'architecture basée sur les cellules et des détails sur la conception du routeur cellulaire utilisée dans ce modèle, consultez la section Informations supplémentaires.

Outils

Services AWS

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.
- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour les applications Web et mobiles.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des fonctions Lambda et d'autres fonctions pour créer des applications critiques Services AWS pour l'entreprise.

Autres outils

- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Serverless-Cell-Router.

Bonnes pratiques

Pour connaître les meilleures pratiques en matière de création d'architectures basées sur des cellules, consultez le guide AWS Well-Architected suivant :

- Réduction de la portée de l'impact grâce à une architecture basée sur les cellules
- AWS Pilier de fiabilité du framework Well-Architected REL1 : 0-BP04 Utiliser des architectures de cloisons pour limiter la portée de l'impact

Épopées

Préparation des fichiers source

Tâche	Description	Compétences requises
Clonez le référentiel d'exemples de code.	Pour cloner le Serverless-Cell-Router GitHub dépôt sur votre ordinateur, utilisez la commande suivante : `git clone https://github.com/aws-samp`	Developer

Tâche	Description	Compétences requises
	`les/Serverless-Cell-Router/`	
Configurez des informations d'identification AWS CLI temporaires.	Configurez le AWS CLI avec des informations d'identification pour votre Compte AWS. Cette procédure pas à pas utilise les informations d'identification temporaires fournies par la ligne de commande ou l'option d'accès programmatique d' AWS IAM Identity Center. Cela définit les variables`AWS_ACCESS_KEY_ID` ,`AWS_SECRET_ACCESS_KEY` , et d'`AWS_SESSION_TOKEN` AWS environnement avec les informations d'identification appropriées à utiliser avec le AWS CLI.	Developer

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment S3 qui sera utilisé pour stocker et accéder aux fonctions Serverless-Cell-Router Lambda à déployer par le AWS CloudFormation modèle. Pour créer le compartiment S3, utilisez la commande suivante : `aws s3api create-bucket --bucket <bucket name> --region eu-central-1 --create-bucket-configuration LocationConstraint=eu-central-1`	Developer

Tâche	Description	Compétences requises

Créez des fichiers .zip.	Créez un fichier .zip pour chaque fonction Lambda située dans le répertoire Functions. Ces fichiers .zip seront utilisés pour déployer les fonctions Lambda. Sur un Mac, utilisez les `zip` commandes suivantes :
	`zip -j mapper-scr.zip Functions/Mapper.py`
	`zip -j dispatcher-scr.zip Functions/Dispatcher.py`
	`zip -j scaler-scr.zip Functions/Scaler.py`
	`zip -j cp validator -scr.zip Functions/Validator.py`
	`zip -j dynamodbD ummyData-scr.zip Functions/Dynamodb DummyData.py`
		Developer

Tâche	Description	Compétences requises

Copiez les fichiers .zip dans le compartiment S3.	Pour copier tous les fichiers .zip de la fonction Lambda dans le compartiment S3, utilisez les commandes suivantes :
	`aws s3 cp mapper-scr.zip s3://<bucket name>`
	`aws s3 cp dispatcher-scr.zip s3://<bucket name>`
	`aws s3 cp scaler-scr.zip s3://<bucket name>`
	`aws s3 cp validator-scr.zip s3://<bucket name>`
	`aws s3 cp dynamodbDummyData-scr.zip s3://<bucket name>`
		Developer

Créez la AWS CloudFormation pile

Tâche	Description	Compétences requises
Déployez le AWS CloudFormation modèle.	Pour déployer le AWS CloudFormation modèle, exécutez la AWS CLI commande suivante : `aws cloudformation create-stack --stack-name serverless.cell-router \`	Developer

Tâche	Description	Compétences requises
	`--template-body file://Serverless-Cell-Router-Stack-v10.yaml \ --capabilities CAPABILITY_IAM \ --parameters ParameterKey=LambdaFunctionMapperS3KeyParameterSCR,ParameterValue=mapper-scr.zip \ ParameterKey=LambdaFunctionDispatcherS3KeyParameterSCR,ParameterValue=dispatcher-scr.zip \ ParameterKey=LambdaFunctionScalerS3KeyParameterSCR,ParameterValue=scaler-scr.zip \ ParameterKey=LambdaFunctionAddDynamoDBDummyItemsS3KeyParameterSCR,ParameterValue=dynamodbDummyData-scr.zip \ ParameterKey=LambdaFunctionsS3BucketParameterSCR,ParameterValue=<S3 bucket storing lambda zip files> \ ParameterKey=CognitoDomain,ParameterValue=<Cognito Domain Name> \ --region <enter your aws region id, e.g. "eu-central-1">`	

Tâche	Description	Compétences requises
Vérifiez les progrès.	Connectez-vous au AWS Management Console, ouvrez la AWS CloudFormation console sur https://console.aws.amazon.com/cloudformation/et vérifiez la progression du développement de la pile. Lorsque le statut est définiCREATE_COMPLETE , la pile a été déployée avec succès.	Developer

Évaluer et vérifier

Tâche	Description	Compétences requises
Attribuez des cellules à l'utilisateur.	Pour lancer leOrchestrator , exécutez la commande curl suivante : `curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxx.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/cells` Orchestrator Déclenche l'exécution de la Dispatcher fonction. À son tourDispatcher , il vérifie l'existence de l'utilisateur.	Developer

Tâche	Description	Compétences requises
	Si l'utilisateur est trouvé, il `Dispatcher` renvoie l'ID de cellule et le point de terminaison associés URLs. Si l'utilisateur n'est pas trouvé, une cellule lui est `Dispatcher` allouée et envoie l'identifiant de la cellule à la `Scaler` fonction pour évaluer la capacité résiduelle de la cellule attribuée. La réponse de la `Scaler` fonction est la suivante : `"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1.amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api.eu-central-1.amazonaws.com/"`	

Tâche	Description	Compétences requises

Récupérez les cellules des utilisateurs.	Pour exécuter la `Orchestrator Mapper` fonction, exécutez la commande suivante :
	`curl -X POST \ -H "Authorization: Bearer {User id_token}" \ https://xxxxxxxxx.execute-api.eu-central-1.amazonaws.com/Cell_Router_Development/mapper`
	`Orchestrator` Recherche la cellule assignée à l'utilisateur et renvoie l'ID de la cellule ainsi URLs que la réponse suivante :
	`"cellID : cell-0002 , endPoint_1 : https://xxxxx.execute-api.eu-north-1.amazonaws.com/ , endPoint_2 : https://xxxxxxx.execute-api.eu-central-1.amazonaws.com/"`
		Developer

Nettoyage

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour éviter d'encourir des frais supplémentaires sur votre compte, procédez comme suit : 1. Videz le compartiment S3 que vous avez créé pour les fonctions Lambda. 2. Supprimez le compartiment. 3. Supprimez la AWS CloudFormation pile.	Développeur d’applications

Ressources connexes

Références

- Stabilité statique avec les zones de disponibilité
- Limites d'isolation des pannes AWS : stabilité statique

Vidéo

Physalia : architecture basée sur les cellules pour améliorer la disponibilité sur Amazon EBS

https://www.youtube-nocookie.com/embed/6 Tu sais ? RZMFic contrôles = 0

Informations supplémentaires

Locaux de conception d'une architecture basée sur les cellules

Bien que ce modèle se concentre sur le routeur cellulaire, il est important de comprendre l'environnement dans son ensemble. L'environnement est structuré en trois couches distinctes :

- La couche de routage, ou couche mince, qui contient le routeur cellulaire
- La couche cellulaire, composée de différentes cellules

- La couche de mise à disposition et de déploiement, qui approvisionne les cellules et déploie l'application

Chaque couche conserve ses fonctionnalités même en cas de détérioration affectant les autres couches. Comptes AWS servent de limite d'isolation des défauts.

Le schéma suivant montre les couches à un niveau élevé. La couche Cell et la couche Provision and Deploy ne sont pas concernées par ce modèle.

Pour plus d'informations sur l'architecture basée sur les cellules, voir Réduction de la portée de l'impact grâce à l'architecture basée sur les cellules : routage des cellules.

Modèle de conception du routeur cellulaire

Le routeur cellulaire est un composant partagé entre les cellules. Pour atténuer les impacts potentiels, il est important que la couche de routage utilise une conception simpliste et évolutive horizontalement aussi fine que possible. En tant que point d'entrée du système, la couche de routage comprend uniquement les composants nécessaires pour affecter efficacement les utilisateurs aux cellules appropriées. Les composants de cette couche ne participent pas à la gestion ou à la création de cellules.

Ce modèle utilise un routage statique, ce qui signifie que le client met en cache les points de terminaison lors de la connexion initiale et établit ensuite une communication directe avec la cellule. Des interactions périodiques entre le client et le routeur cellulaire sont initiées pour confirmer l'état actuel ou récupérer des mises à jour. Ce découplage intentionnel permet aux utilisateurs existants de fonctionner sans interruption en cas d'indisponibilité du routeur cellulaire, tout en garantissant la continuité des fonctionnalités et de la résilience au sein du système.

Dans ce modèle, le routeur cellulaire prend en charge les fonctionnalités suivantes :

- Extraction des données cellulaires de la base de données de cellules dans la couche Provision and Deploy et stockage ou mise à jour de la base de données locale.
- Affectation d'une cellule à chaque nouvel utilisateur enregistré de l'application à l'aide de l'algorithme d'attribution de cellule.
- user-to-cellsStockage du mappage dans la base de données locale.
- Vérification de la capacité des cellules lors de l'affectation des utilisateurs et activation d'un événement pour le distributeur automatique dans la couche Provision and Deploy afin de créer des cellules.

- Utilisation de l'algorithme des critères de création de cellules pour fournir cette fonctionnalité.
- Répondre aux demandes des utilisateurs nouvellement enregistrés en fournissant URLs les cellules statiques. Ils URLs seront mis en cache sur le client avec une durée de vie (TTL).
- Répondre aux demandes d'utilisateurs existantes concernant une URL non valide en fournissant une URL nouvelle ou mise à jour.

Pour mieux comprendre le routeur cellulaire de démonstration configuré par le AWS CloudFormation modèle, passez en revue les composants et les étapes suivants :

1. Configurez et configurez le groupe d'utilisateurs Amazon Cognito.
2. Configurez et configurez l'API API Gateway pour le routeur cellulaire.
3. Créez une table DynamoDB.
4. Créez et configurez une file d'attente SQS.
5. Implémentez le`Orchestrator`.
6. Implémentez les fonctions Lambda :`Dispatcher`,,`Scaler`,`Mapper`. `Validator`
7. Évaluez et vérifiez.

Le présupposé est que la couche Provision and Deploy est déjà établie. Les détails de sa mise en œuvre dépassent le cadre de cet artefact.

Ces composants étant définis et configurés par un AWS CloudFormation modèle, les étapes suivantes sont présentées de manière descriptive et détaillée. L'hypothèse est que vous possédez les AWS compétences requises pour effectuer l'installation et la configuration.

1. Configuration et configuration du groupe d'utilisateurs Amazon Cognito

Connectez-vous à la AWS Management Console console Amazon Cognito et ouvrez-la à l'adresse. https://console.aws.amazon.com/cognito/ Configurez et configurez un groupe d'utilisateurs Amazon Cognito nommé`CellRouterPool`, avec intégration d'applications, interface utilisateur hébergée et autorisations nécessaires.

2. Installation et configuration de l'API API Gateway pour le routeur cellulaire

Ouvrez la console API Gateway à l'adresse https://console.aws.amazon.com/apigateway/. Configurez et configurez une API nommée `CellRouter` à l'aide d'un autorisateur Amazon Cognito intégré au groupe d'utilisateurs Amazon Cognito. `CellRouterPool` Implémentez les éléments suivants :

- `CellRouter`Ressources d'API, y compris `POST` les méthodes
- Intégration au flux de travail Step Functions implémenté à l'étape 5
- Autorisation via l'autorisateur Amazon Cognito
- Mappages de demandes et de réponses d'intégration
- Attribution des autorisations nécessaires

3. Création d'une table DynamoDB

Ouvrez la console DynamoDB https://console.aws.amazon.com/dynamodb/à l'adresse et créez une table DynamoDB standard appelée avec la configuration suivante : `tbl_router`

- Clé de partition – `marketId`
- Clé de tri – `cellId`
- Mode capacité – Provisionné
- Point-in-time restauration (PITR) – Désactivé

Dans l'onglet Indexes, créez un index secondaire global appelé`marketId-currentCapacity-index`. La fonction `Scaler` Lambda utilisera l'index pour effectuer des recherches efficaces dans la cellule ayant le plus petit nombre d'utilisateurs assignés.

Créez la structure du tableau avec les attributs suivants :

- `marketId`– L'Europe
- `cellId`– cellule-0002
- `currentCapacity`– 2
- `endPoint_1`– <your endpoint for the first Region>
- `endPoint_2`– <your endpoint for the second Region>
- `IsHealthy`– Vrai
- `maxCapacity`– 10
- `regionCode_1` – `eu-north-1`
- `regionCode_2` – `eu-central-1`
- `userIds`– <your email address>

4. Création et configuration d'une file d'attente SQS

Ouvrez la console Amazon SQS à https://console.aws.amazon.com/sqs/l'adresse et créez une file d'attente SQS standard appelée `CellProvisioning` configurée avec le chiffrement par clé Amazon SQS.

5. Implémenter l'orchestrateur

Développez un flux de travail Step Functions qui servira `Orchestrator` de fil au routeur. Le flux de travail est appelable via l'API du routeur cellulaire. Le flux de travail exécute les fonctions Lambda désignées en fonction du chemin de ressource. Intégrez la fonction step à l'API API Gateway du routeur `CellRouter` cellulaire et configurez les autorisations nécessaires pour appeler les fonctions Lambda.

Le schéma suivant montre le flux de travail. L'état du choix invoque l'une des fonctions Lambda. Si la fonction Lambda est réussie, le flux de travail se termine. Si la fonction Lambda échoue, l'état d'échec est appelé.

6. Implémenter les fonctions Lambda

`Dispatcher`Implémentez les `Validator` fonctions `MapperScaler`,, et. Lorsque vous configurez et configurez chaque fonction dans la démonstration, définissez un rôle pour la fonction et attribuez les autorisations nécessaires pour effectuer les opérations requises sur la table DynamoDB`tbl_router`. Intégrez également chaque fonction dans le flux de travail`Orchestrator`.

Fonction Dispatcher

La `Dispatcher` fonction est chargée d'identifier et d'attribuer une seule cellule statique à chaque nouvel utilisateur enregistré. Lorsqu'un nouvel utilisateur s'enregistre auprès de l'application globale, la demande est envoyée à la `Dispatcher` fonction. La fonction traite la demande en utilisant des critères d'évaluation prédéfinis tels que les suivants :

1. Région – Sélectionnez la cellule du marché où se trouve l'utilisateur. Par exemple, si l'utilisateur accède à l'application globale depuis l'Europe, sélectionnez une cellule qui utilise Régions AWS en Europe.
2. Proximité ou latence – Sélectionnez la cellule la plus proche de l'utilisateur Par exemple, si l'utilisateur accède à l'application depuis les Pays-Bas, la fonction considère une cellule qui utilise Francfort et l'Irlande. La décision concernant la cellule la plus proche est basée sur des métriques telles que le temps de latence entre l'emplacement de l'utilisateur et les régions de la cellule. Pour

cet exemple de modèle, les informations sont alimentées de manière statique à partir de la couche Provision and Deploy.

3. Santé – La `Dispatcher` fonction vérifie si la cellule sélectionnée est saine en fonction de l'état de cellule indiqué (Healthy = vrai ou faux).
4. Capacité – La distribution des utilisateurs est basée sur le nombre minimal d'utilisateurs dans une logique de cellule, de sorte que l'utilisateur est affecté à la cellule qui compte le moins d'utilisateurs.

> **Note**
>
> Ces critères sont présentés uniquement pour expliquer cet exemple de modèle. Pour une implémentation réelle d'un routeur cellulaire, vous pouvez définir des critères plus précis et utiliser des critères basés sur des cas.

`Orchestrator`Invoque la fonction Dispatcher pour affecter les utilisateurs aux cellules. Dans cette fonction de démonstration, la valeur de marché est un paramètre statique défini comme`europe`.

La `Dispatcher` fonction détermine si une cellule est déjà attribuée à l'utilisateur. Si la cellule est déjà affectée, la `Dispatcher` fonction renvoie les extrémités de la cellule. Si aucune cellule n'est attribuée à l'utilisateur, la fonction recherche la cellule qui compte le moins d'utilisateurs, l'affecte à l'utilisateur et renvoie les points de terminaison. L'efficacité de la requête de recherche de cellules est optimisée en utilisant l'index secondaire global.

Fonction de mappage

La `Mapper` fonction supervise le stockage et la maintenance des user-to-cell mappages dans la base de données. Une cellule singulière est attribuée à chaque utilisateur enregistré. Chaque cellule possède deux cellules distinctes URLs, une pour chaque région AWS. Servant de points de terminaison d'API hébergés sur API Gateway, URLs ils fonctionnent comme des points entrants vers l'application globale.

Lorsque la `Mapper` fonction reçoit une demande de l'application cliente, elle exécute une requête sur la `tbl_router` table DynamoDB pour récupérer user-to-cell le mappage associé à l'identifiant e-mail fourni. Si elle trouve une cellule assignée, la `Mapper` fonction fournit rapidement les deux cellules URLs. La `Mapper` fonction surveille également activement les modifications apportées à la cellule URLs et lance des notifications ou des mises à jour des paramètres utilisateur.

Fonction Scaler

La `Scaler` fonction gère la capacité résiduelle de la cellule. Pour chaque nouvelle demande d'enregistrement d'utilisateur, la `Scaler` fonction évalue la capacité disponible de la cellule que la `Dispatcher` fonction a attribuée à l'utilisateur. Si la cellule a atteint sa limite prédéterminée conformément aux critères d'évaluation spécifiés, la fonction lance une demande via une file d'attente Amazon SQS vers la couche Provision and Deploy, sollicitant le provisionnement et le déploiement de nouvelles cellules. La mise à l'échelle des cellules peut être exécutée en fonction d'un ensemble de critères d'évaluation tels que les suivants :

1. Nombre maximum d'utilisateurs – Chaque cellule peut avoir un nombre maximum de 500 utilisateurs.
2. Capacité tampon – La capacité tampon de chaque cellule est de 20 %, ce qui signifie que chaque cellule peut être affectée à 400 utilisateurs à tout moment. Les 20 % de capacité tampon restants sont réservés aux futurs cas d'utilisation et à la gestion de scénarios inattendus (par exemple, lorsque les services de création et de provisionnement de cellules ne sont pas disponibles).
3. Création de cellules – Dès qu'une cellule existante atteint 70 % de sa capacité, une demande est déclenchée pour créer une cellule supplémentaire.

> **Note**
>
> Ces critères sont présentés uniquement pour expliquer cet exemple de modèle. Pour une implémentation réelle d'un routeur cellulaire, vous pouvez définir des critères plus précis et utiliser des critères basés sur des cas.

Le `Scaler` code de démonstration est exécuté `Orchestrator` après avoir attribué `Dispatcher` avec succès une cellule à l'utilisateur nouvellement enregistré. Sur réception de l'identifiant de cellule du`Dispatcher`, évalue si la cellule désignée a une capacité suffisante pour accueillir des utilisateurs supplémentaires, sur la base de critères d'évaluation prédéfinis. `Scaler` Si la capacité de la cellule est insuffisante, la `Scaler` fonction envoie un message au service Amazon SQS. Ce message est récupéré par le service dans la couche Provision and Deploy, ce qui lance le provisionnement d'une nouvelle cellule.

Fonction de validation

La `Validator` fonction identifie et résout les problèmes relatifs à l'accès aux cellules. Lorsqu'un utilisateur se connecte à l'application globale, l'application extrait les cellules des paramètres URLs

du profil utilisateur et achemine les demandes des utilisateurs vers l'une des deux régions attribuées dans la cellule. S' URLs ils sont inaccessibles, l'application peut envoyer une demande d'URL de validation au routeur cellulaire. Le routeur cellulaire `Orchestrator` invoque le. `Validator` `Validator`Lance le processus de validation. La validation peut inclure, entre autres, les vérifications suivantes :

- Référencement croisé entre la cellule URLs de la demande et la cellule URLs stockée dans la base de données pour identifier et traiter les mises à jour potentielles
- Exécution d'un bilan de santé approfondi (par exemple, une `HTTP GET` demande adressée au point de terminaison de la cellule)

En conclusion, la `Validator` fonction fournit des réponses aux demandes des applications clientes, en fournissant le statut de validation ainsi que les étapes de correction requises.

`Validator`Il est conçu pour améliorer l'expérience utilisateur. Imaginons un scénario dans lequel certains utilisateurs rencontrent des difficultés pour accéder à l'application globale en raison d'un incident qui rend les cellules temporairement indisponibles. Au lieu de présenter des erreurs génériques, la `Validator` fonction peut fournir des étapes de correction instructives. Ces étapes peuvent inclure les actions suivantes :

- Informez les utilisateurs de l'incident.
- Indiquez le temps d'attente approximatif avant la disponibilité du service.
- Indiquez le numéro de téléphone du service d'assistance pour obtenir des informations supplémentaires.

Le code de démonstration de la `Validator` fonction vérifie que la cellule fournie par l'utilisateur URLs dans la demande correspond aux enregistrements stockés dans la `tbl_router` table. La `Validator` fonction vérifie également si les cellules sont saines.

Configurer un accès privé à un compartiment Amazon S3 via un point de terminaison VPC

Créée par Martin Maritsch (AWS), Gabriel Rodriguez Garcia (AWS), Shukhrat Khodjaev (AWS), Nicolas Jacob Baer (AWS), Mohan Gowda Purushothama (AWS) et Joaquin Rinaudo (AWS)

Récapitulatif

Dans Amazon Simple Storage Service (Amazon S3), les fichiers URLs présignés vous permettent de partager des fichiers de taille arbitraire avec des utilisateurs cibles. Par défaut, les Amazon S3 presigned URLs sont accessibles depuis Internet dans un délai d'expiration, ce qui les rend pratiques à utiliser. Cependant, les environnements d'entreprise nécessitent souvent que l'accès à Amazon S3 présigné URLs soit limité à un réseau privé uniquement.

Ce modèle présente une solution sans serveur pour interagir en toute sécurité avec les objets S3 en utilisant une signature préalable URLs depuis un réseau privé sans traversée d'Internet. Dans l'architecture, les utilisateurs accèdent à un Application Load Balancer via un nom de domaine interne. Le trafic est acheminé en interne via Amazon API Gateway et un point de terminaison de cloud privé virtuel (VPC) pour le compartiment S3. La AWS Lambda fonction génère des fichiers présignés URLs pour les téléchargements via le point de terminaison VPC privé, ce qui permet d'améliorer la sécurité et la confidentialité des données sensibles.

Conditions préalables et limitations

Prérequis

- Un VPC qui inclut un sous-réseau déployé dans un réseau Compte AWS d'entreprise connecté (par exemple, via). AWS Direct Connect

Limites

- Le compartiment S3 doit porter le même nom que le domaine. Nous vous recommandons donc de vérifier les règles de dénomination des compartiments Amazon S3.
- Cet exemple d'architecture n'inclut pas de fonctionnalités de surveillance pour l'infrastructure déployée. Si votre cas d'utilisation nécessite une surveillance, pensez à ajouter AWS des services de surveillance.

- Cet exemple d'architecture n'inclut pas la validation des entrées. Si votre cas d'utilisation nécessite une validation des entrées et un niveau de sécurité accru, envisagez de l'utiliser AWS WAF pour protéger votre API.
- Cet exemple d'architecture n'inclut pas la journalisation des accès avec l'Application Load Balancer. Si votre cas d'utilisation nécessite la journalisation des accès, pensez à activer les journaux d'accès de l'équilibreur de charge.

Versions

- Python version 3.11 ou ultérieure
- Terraform version 1.6 ou ultérieure

Architecture

Pile technologique cible

Les services AWS suivants sont utilisés dans la pile technologique cible :

- Amazon S3 est le service de stockage principal utilisé pour charger, télécharger et stocker des fichiers en toute sécurité.
- Amazon API Gateway expose les ressources et les points de terminaison permettant d'interagir avec le compartiment S3. Ce service joue un rôle dans la génération de données présignées URLs pour le téléchargement ou le chargement de données.
- AWS Lambdagénère des fichiers présignés URLs pour le téléchargement de fichiers depuis Amazon S3. La fonction Lambda est appelée par API Gateway.
- Amazon VPC déploie des ressources au sein d'un VPC pour isoler le réseau. Le VPC inclut des sous-réseaux et des tables de routage pour contrôler le flux de trafic.
- Application Load Balancer achemine le trafic entrant soit vers API Gateway, soit vers le point de terminaison VPC du compartiment S3. Il permet aux utilisateurs du réseau d'entreprise d'accéder aux ressources en interne.
- Le point de terminaison VPC pour Amazon S3 permet une communication directe et privée entre les ressources du VPC et Amazon S3 sans passer par l'Internet public.
- AWS Identity and Access Management (IAM) contrôle l'accès aux AWS ressources. Les autorisations sont configurées pour garantir des interactions sécurisées avec l'API et les autres services.

Architecture cible

Le diagramme illustre les éléments suivants :

1. Les utilisateurs du réseau d'entreprise peuvent accéder à l'Application Load Balancer via un nom de domaine interne. Nous supposons qu'une connexion existe entre le réseau d'entreprise et le sous-réseau intranet dans le Compte AWS (par exemple, via une AWS Direct Connect connexion).
2. L'Application Load Balancer achemine le trafic entrant soit vers API Gateway pour générer des données présignées URLs pour le téléchargement ou le chargement vers Amazon S3, soit vers le point de terminaison VPC du compartiment S3. Dans les deux scénarios, les demandes sont acheminées en interne et n'ont pas besoin de passer par Internet.
3. API Gateway expose les ressources et les points de terminaison pour interagir avec le compartiment S3. Dans cet exemple, nous fournissons un point de terminaison pour télécharger des fichiers depuis le compartiment S3, mais cela pourrait également être étendu pour fournir une fonctionnalité de téléchargement.
4. La fonction Lambda génère l'URL présignée pour télécharger un fichier depuis Amazon S3 en utilisant le nom de domaine de l'Application Load Balancer au lieu du domaine public Amazon S3.
5. L'utilisateur reçoit l'URL présignée et l'utilise pour télécharger le fichier depuis Amazon S3 à l'aide de l'Application Load Balancer. L'équilibreur de charge inclut une route par défaut pour envoyer le trafic qui n'est pas destiné à l'API vers le point de terminaison VPC du compartiment S3.
6. Le point de terminaison VPC achemine l'URL présignée avec le nom de domaine personnalisé vers le compartiment S3. Le compartiment S3 doit porter le même nom que le domaine.

Automatisation et mise à l'échelle

Ce modèle utilise Terraform pour déployer l'infrastructure depuis le référentiel de code dans un. Compte AWS

Outils

Outils

- Python est un langage de programmation informatique polyvalent.
- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les AWS services par le biais de commandes dans votre interface de ligne de commande.

Référentiel de code

Le code de ce modèle est disponible dans un GitHub dépôt sur https://github.com/aws-samples/private-s3-vpce.

Bonnes pratiques

L'exemple d'architecture de ce modèle utilise les autorisations IAM pour contrôler l'accès à l'API. Toute personne disposant d'informations d'identification IAM valides peut appeler l'API. Si votre cas d'utilisation nécessite un modèle d'autorisation plus complexe, vous souhaiterez peut-être utiliser un autre mécanisme de contrôle d'accès.

Épopées

Déployez la solution dans un Compte AWS

Tâche	Description	Compétences requises
Obtenez des AWS informations d'identification.	Vérifiez vos AWS informations d'identification et votre accès à votre compte. Pour obtenir des instructions, consultez la section Configuration et paramètres des fichiers d'identification dans la AWS CLI documentation.	AWS DevOps, AWS en général
Pour cloner le référentiel.	Clonez le GitHub référentiel fourni avec ce modèle : `git clone https://github.com/aws-samples/private-s3-vpce`	AWS DevOps, AWS en général

Tâche	Description	Compétences requises
Configurez les variables.	1. Sur votre ordinateur, dans le GitHub référentiel, ouvrez le `terraform` dossier : `cd terraform` 2. Ouvrez le `example.tfvars` fichier et personnalisez les paramètres en fonction de vos besoins.	AWS DevOps, AWS en général
Déployez la solution.	1. Dans le `terraform` dossier, exécutez Terraform et transmettez les variables que vous avez personnalisées : `terraform apply -var-file="example.tfvars"` 2. Vérifiez que les ressources indiquées dans le schéma d'architecture ont été déployées avec succès.	AWS DevOps, AWS en général

Tester la solution

Tâche	Description	Compétences requises
Créez un fichier de test.	Chargez un fichier sur Amazon S3 afin de créer un scénario de test pour le téléchargement du fichier. Vous pouvez utiliser la	AWS DevOps, AWS en général

Tâche	Description	Compétences requises
	console Amazon S3 ou la AWS CLI commande suivante : `aws s3 cp /path/to/testfile s3://your-bucket-name/testfile`	
Testez la fonctionnalité des URL présignées.	1. Envoyez une demande à l'Application Load Balancer pour créer une URL présignée pour le fichier de test à l'aide de awscurl : `awscurl https://your-domain-name/api/get_url?key=testfile` Cette étape crée une signature valide à partir de vos informations d'identif ication, qui sera validée par API Gateway. 2. Analysez le lien contenu dans la réponse que vous avez reçue à l'étape précédente et ouvrez l'URL présignée pour télécharger le fichier.	AWS DevOps, AWS en général
Nettoyer.	Assurez-vous de supprimer les ressources lorsqu'elles ne sont plus nécessaires : `terraform destroy`	AWS DevOps, AWS en général

Résolution des problèmes

Problème	Solution
Les noms de clés d'objets S3 comportant des caractères spéciaux tels que des signes numériques (#) interrompent les paramètres d'URL et génèrent des erreurs.	Codez correctement les paramètres d'URL et assurez-vous que le nom de la clé de l'objet S3 est conforme aux directives d'Amazon S3.

Ressources connexes

Amazon S3 :

- Partage d'objets avec présigné URLs
- Contrôle de l'accès depuis les points de terminaison VPC à l'aide de politiques de compartiment

Amazon API Gateway :

- Utiliser les politiques de point de terminaison VPC pour le mode privé APIs dans API Gateway

Application Load Balancer :

- Hébergement de sites Web statiques HTTPS internes avec ALB, S3 et PrivateLink (article de AWS blog)

Résoudre les problèmes liés aux états en AWS Step Functions utilisant Amazon Bedrock

Créée par Aniket Kurzadkar (AWS) et Sangam Kushwaha (AWS)

Récapitulatif

AWS Step Functions les fonctionnalités de gestion des erreurs peuvent vous aider à détecter une erreur qui se produit pendant un état dans un flux de travail, mais il peut toujours être difficile de trouver la cause première d'une erreur et de la déboguer. Ce modèle répond à ce défi et montre comment Amazon Bedrock peut vous aider à résoudre les erreurs qui se produisent pendant les états dans Step Functions.

Step Functions assure l'orchestration des flux de travail, ce qui permet aux développeurs d'automatiser plus facilement les processus. Step Functions propose également une fonctionnalité de gestion des erreurs qui offre les avantages suivants :

- Les développeurs peuvent créer des applications plus résilientes qui n'échouent pas complètement en cas de problème.
- Les flux de travail peuvent inclure une logique conditionnelle pour gérer différemment les différents types d'erreurs.
- Le système peut réessayer automatiquement les opérations qui ont échoué, peut-être avec un retard exponentiel.
- Des chemins d'exécution alternatifs peuvent être définis pour les scénarios d'erreur, ce qui permet au flux de travail de s'adapter et de poursuivre le traitement.

Lorsqu'une erreur se produit dans un flux de travail Step Functions, ce modèle montre comment le message d'erreur et le contexte peuvent être envoyés à un modèle de base (FM) tel que Claude 3 qui est pris en charge par Step Functions. Le FM peut analyser l'erreur, la classer et suggérer des mesures correctives potentielles.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Compréhension de base AWS Step Functions des flux de travail

- Connectivité à l'API Amazon Bedrock

Limites

- Vous pouvez utiliser l'approche de ce modèle pour différents Services AWS. Cependant, les résultats peuvent varier en fonction de l'invite créée AWS Lambda qui est ensuite évaluée par Amazon Bedrock.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Le schéma montre le flux de travail automatisé pour la gestion des erreurs et la notification dans une machine à états Step Functions :

1. Le développeur lance l'exécution d'une machine à états.
2. La machine à états Step Functions commence à traiter ses états. Deux résultats sont possibles :
   - (a) Si tous les états s'exécutent correctement, le flux de travail est transmis directement à Amazon SNS pour recevoir une notification de réussite par e-mail.
   - (b) Si un état échoue, le flux de travail passe à la fonction Lambda de gestion des erreurs.
3. En cas d'erreur, les événements suivants se produisent :
   - (a) La fonction Lambda (gestionnaire d'erreurs) est déclenchée. La fonction Lambda extrait le message d'erreur à partir des données d'événement que la machine d'état Step Functions lui a transmises. La fonction Lambda prépare ensuite une invite basée sur ce message d'erreur et envoie l'invite à Amazon Bedrock. L'invite demande des solutions et des suggestions relatives à l'erreur spécifique rencontrée.
   - (b) Amazon Bedrock, qui héberge le modèle d'IA génératif, traite l'invite de saisie. (Ce modèle utilise le modèle de fondation Anthropic Claude 3 (FM), qui est l'un des nombreux FMs modèles proposés par Amazon Bedrock.) Le modèle d'IA analyse le contexte d'erreur. Le modèle génère ensuite une réponse qui peut inclure des explications expliquant pourquoi l'erreur s'est produite,

des solutions potentielles pour résoudre l'erreur et des suggestions pour éviter de refaire les mêmes erreurs à l'avenir.

Amazon Bedrock renvoie sa réponse générée par l'IA à la fonction Lambda. La fonction Lambda traite la réponse, éventuellement en la formatant ou en extrayant des informations clés. La fonction Lambda envoie ensuite la réponse à la sortie de la machine à états.

4. Après la gestion des erreurs ou une exécution réussie, le flux de travail se termine en déclenchant l'envoi d'une notification par e-mail par Amazon SNS.

Outils

Services AWS

- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.

Bonnes pratiques

- Amazon Bedrock étant un modèle d'intelligence artificielle génératif qui apprend à partir de données entraînées, il utilise également ces données pour former et générer du contexte. Il est recommandé de dissimuler toute information privée susceptible d'entraîner des problèmes de fuite de données.
- Bien que l'IA générative puisse fournir des informations précieuses, les décisions critiques en matière de gestion des erreurs doivent tout de même impliquer une supervision humaine, en particulier dans les environnements de production.

Épopées

Créez une machine à états pour votre flux de travail

Tâche	Description	Compétences requises
Créez une machine d'état .	Pour créer une machine à états adaptée à votre flux de travail, procédez comme suit : 1. Connectez-vous à la AWS Management Console AWS Step Functions console et ouvrez-la. 2. Dans le volet de navigation de gauche, sélectionnez State machines. 3. Choisissez Create state machine (Créer une machine d'état). 4. Choisissez un modèle en fonction de votre cas d'utilisation ou choisissez Blank pour créer un modèle adapté à vos besoins.	AWS DevOps

Création d’une fonction Lambda

Tâche	Description	Compétences requises
Créez une fonction Lambda.	Pour créer une fonction Lambda, procédez comme suit :	AWS DevOps

Tâche	Description	Compétences requises
	1. Dans le AWS Management Console, accédez à la AWS Lambda console. 2. Dans le panneau de navigation, choisissez Functions (Fonctions), puis Create function (Créer une fonction). 3. Sur la page Créer une fonction, choisissez l'une des options pour créer une fonction. Entrez ensuite un nom dans Nom de la fonction et choisissez la langue appropriée dans la liste déroulante de Runtime. 4. Choisissez Créer une fonction.	

Tâche	Description	Compétences requises
Configurez la logique requise dans le code Lambda.	• Pour vous connecter à l'API Amazon Bedrock à l'aide du AWS SDK pour Python (Boto3), utilisez le code suivant. Ce code configure un client pour Amazon Bedrock, prépare les paramètres nécessaires, puis envoie une demande au modèle Claude 3 avec une invite spécifiée. Ce modèle invoque le modèle Claude 3. Pour plus d'informations sur tous les modèles de fondation pris en charge, y compris le modèle associé IDs, consultez la section Modèles de fondation pris en charge dans Amazon Bedrock dans la documentation Amazon Bedrock. `client = boto3.client( service_name="bedrock-runtime", region_name="selected-region" ) # Invoke Claude 3 with the text prompt`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>model_id = "your-mod
	el-id" # Select your
	 Model ID, Based on the
	 Model Id, Change the
	 body format
	
	try:
	response =
	 client.invoke_model(
	modelId=m
	odel_id,
	body=json
	.dumps(
	{
	
	 "anthropic_version":
	 "bedrock-2023-05-31",
	
	 "max_tokens": 1024,
	
	 "messages": [
	
	 {
	
	"role": "user",
	
	"content"
	: [{"type": "text",
	 "text": prompt}],
	
	 }
	],
	}
	),
	)</pre>
	• (Facultatif) Remplacez le compte Compte AWS IDs IDs par un espace réservé. Pour des raisons	

Tâche	Description	Compétences requises

	de sécurité, cette approche peut être utile pour nettoyer les journaux, les messages d'erreur ou toute autre sortie susceptible de contenir des informations de compte sensibles.
	
	Le code suivant permet de détecter toute occurrence d'un nombre à 12 chiffres entre deux points (format utilisé Compte AWS IDs dans Amazon Resource Names (ARNs) et d'autres AWS identifiants) et de le remplacer par l'identifiant de compte fictif. `":123456789012:"`
	
	`def replace_account_id(input_string):`
	
	`    # Use a regular expression to find the AWS account ID pattern`
	`    account_id_pattern = r'(:\d{12}:)'`
	
	`    # Replace the matched pattern with ":123456789012:"`
	`    modified_string = re.sub(account_id_pattern, ":1234567`	

Tâche	Description	Compétences requises
	89012:", input_str ing) return modified_ string	

Intégrez Step Functions à Lambda

Tâche	Description	Compétences requises
Configurez Lambda pour gérer les erreurs dans Step Functions.	Pour configurer Step Functions afin de gérer les erreurs sans perturber le flux de travail, procédez comme suit : 1. Dans la console Step Functions, accédez à la machine à états que vous avez créée précédemment. 2. Choisissez Modifier, puis choisissez le service pour lequel vous souhaitez configurer la gestion des erreurs, puis sélectionnez Gestion des erreurs. 3. Choisissez Add new catcher, et pour Fallback state, choisissez Lambda, puis choisissez la fonction Lambda que vous avez créée précédemment. Pour plus d'informations, consultez la section Catch	AWS DevOps

Tâche	Description	Compétences requises
	errors dans la documentation de Step Functions.	

Résolution des problèmes

Problème	Solution
Lambda ne peut pas accéder à l'API Amazon Bedrock (utilisation non autorisée)	Cette erreur se produit lorsque le rôle Lambda n'est pas autorisé à accéder à l'API Amazon Bedrock. Pour résoudre ce problème, ajoutez la `AmazonBedrockFullAccess` politique pour le rôle Lambda. Pour plus d'informations, consultez AmazonBedrockFullAccessle Guide de référence des politiques AWS gérées.
Erreur de temporisation Lambda	Parfois, cela peut prendre plus de 30 secondes pour générer une réponse et la renvoyer, selon l'invite. Pour résoudre ce problème, augmentez le temps de configuration. Pour plus d'informations, voir Configurer le délai d'expiration de la fonction Lambda dans le Guide du AWS Lambda développeur.

Ressources connexes

- Amazon Bedrock
- Accès à l'API Amazon Bedrock
- Créez votre première fonction Lambda
- Développement de flux de travail avec Step Functions
- AWS Step Functions

Enchaînez les services AWS en utilisant une approche sans serveur

Créée par Aniket Braganza (AWS)

Récapitulatif

Ce modèle illustre une approche évolutive et sans serveur pour traiter un fichier importé en enchaînant Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) et AWS Lambda. L'exemple de fichier téléchargé est destiné à des fins de démonstration. Vous pouvez utiliser une approche sans serveur pour effectuer d'autres tâches en enchaînant les différents services AWS nécessaires pour atteindre vos objectifs commerciaux. L'approche sans serveur utilise un flux de travail asynchrone qui repose sur des notifications pilotées par des événements, un stockage résilient et une fonction en tant que service (FaaS) pour traiter les demandes. Vous pouvez utiliser l'approche sans serveur pour évoluer afin de répondre à la demande tout en minimisant les coûts.

> **Note**
>
> Il existe plusieurs options pour enchaîner les services AWS par le biais d'une approche sans serveur. Par exemple, vous pouvez utiliser une approche qui combine Lambda avec Amazon S3 au lieu d'Amazon SNS et Amazon SQS. Toutefois, ce modèle utilise Amazon SNS et Amazon SQS, car cette approche permet d'ajouter plusieurs points d'intégration dans le processus d'invocation Lambda lors d'une notification d'événement et d'étendre l'implémentation pour inclure plusieurs écouteurs dans une orchestration sans serveur tout en minimisant la charge de traitement.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Accès programmatique au compte AWS. Pour plus d'informations, consultez :
  - Conditions requises dans la documentation du AWS Cloud Development Kit (AWS CDK)
  - Conditions requises dans la documentation de l'interface de ligne de commande AWS (AWS CLI)
- AWS CDK, installé

- CLI AWS, installée et configurée
- Python 3.9

Versions du produit

- AWS CDK 2.x
- Python 3.9

Architecture

Le schéma suivant montre comment les services AWS enchaînés peuvent permettre à un utilisateur de télécharger un fichier dans un compartiment S3 pour le traiter.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur télécharge un fichier dans le compartiment S3.
2. Le téléchargement déclenche un événement S3 qui publie un message sur une rubrique SNS. Le message contient les détails de l'événement S3.
3. Le message publié dans la rubrique SNS est inséré dans une file d'attente SQS, qui est abonnée et reçoit des notifications pour cette rubrique.
4. Une fonction Lambda interroge la file d'attente SQS (en tant que source d'événements) et attend le traitement des messages.
5. Lorsque la fonction Lambda reçoit des messages de la file d'attente SQS, elle les traite et accuse réception de ces messages.
6. Si un message n'est pas traité par Lambda, il est renvoyé dans la file d'attente SQS et est finalement transféré dans une file d'attente de lettres mortes SQS.

Pile technologique

- Amazon S3
- Amazon SNS
- Amazon SQS
- AWS Lambda

Outils

Services AWS

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Autres outils

- AWS Cloud Development Kit (AWS CDK) est le principal outil permettant d'interagir avec votre application AWS CDK. Il exécute votre application, interroge le modèle d'application que vous avez défini, produit et déploie les CloudFormation modèles AWS générés par le CDK AWS.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Python est un langage de programmation de haut niveau interprété à usage général.

Code

Le code de ce modèle est disponible dans le référentiel GitHub Chaining S3 to SNS to SQS to Lambda.

Épopées

Développez votre environnement sans serveur

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le référentiel et naviguez jusqu'au `python/s3-sns-sqs-lambda-chain` dossier.	Développeur d'applications
Configurez un environnement virtuel.	1. Dans le kit AWS CDK, exécutez la `python3 -m venv .venv` commande. 2. Exécutez la `source .venv/bin/activate` commande sous macOS/Linux ou `.venv\Scripts\activate.bat` sous Windows.	Développeur d'applications
Installez les dépendances.	Exécutez la commande `pip install -r requirements.txt .`	Développeur d'applications

Testez la CloudFormation pile

Tâche	Description	Compétences requises
Exécutez des tests unitaires.	1. Exécutez la commande `pip install -r requirements-dev.txt .` 2. **Important** (Facultatif) Exécutez la `cdk`	Développeur d'applications, ingénieur de test

Tâche	Description	Compétences requises
	`synth --no-staging > template.yml` commande pour générer la CloudForm ation pile. Vous pouvez inspecter la pile, mais évitez de générer des ressources et des artefacts intermédi aires. 3. Exécutez la `pytest` commande pour exécuter tous les tests unitaires. 4. (Facultatif) Exécutez la `pytest tests/uni t/<test_filename>` commande pour exécuter des tests pour un fichier spécifique.	

Déployez la CloudFormation pile

Tâche	Description	Compétences requises
Configurez l'environnement bootstrap.	Suivez les instructions de la section Bootstrapping de la documentation AWS pour amorcer l'environnement de déploiement d'AWS CDK dans chaque région AWS où	Développeur d'applications, DevOps ingénieur, ingénieur de données

Tâche	Description	Compétences requises
	la CloudFormation pile sera déployée. **Note** Cette étape nécessite que vous disposiez d'informations d'identification avec accès par programmation.	
Déployez la CloudFormation pile.	Exécutez la `cdk deploy` commande pour créer et déployer la pile sur le compte AWS.	Développeur d'applications, DevOps ingénieur, AWS DevOps

Nettoyez les ressources de votre environnement

Tâche	Description	Compétences requises
Supprimez la CloudFormation pile et supprimez les ressources associées.	Pour supprimer la CloudFormation pile créée et supprimer toutes les ressources associées, exécutez la commande `run cdk` destroy.	Développeur d’applications

Plus de modèles

- Accédez aux tables Amazon DynamoDB, interrogez-les et joignez-les à l'aide d'Athena
- Données agrégées dans Amazon DynamoDB pour les prévisions de machine learning dans Athena
- Automatisez les CodeGuru révisions Amazon pour les applications AWS CDK Python à l'aide d' GitHub Actions
- Automatisez l'évaluation des ressources AWS
- Automatisez le déploiement d'applications imbriquées à l'aide d'AWS SAM
- Automatisez la réplication des instances Amazon RDS sur Comptes AWS
- Archivez automatiquement les éléments sur Amazon S3 à l'aide de DynamoDB TTL
- Détectez automatiquement les modifications et lancez différents CodePipeline pipelines pour un monorepo dans CodeCommit
- Créez une architecture faiblement couplée avec des microservices en utilisant DevOps Practices et AWS Cloud9
- Créez une architecture sans serveur multi-locataires dans Amazon Service OpenSearch
- Créez un visualiseur de fichiers mainframe avancé dans le cloud AWS
- Calculez la valeur à risque (VaR) à l'aide des services AWS
- Copiez les produits AWS Service Catalog sur différents comptes AWS et régions AWS
- Créez automatiquement des pipelines CI dynamiques pour les projets Java et Python
- Décomposez les monolithes en microservices en utilisant le CQRS et le sourcing d'événements
- Déployez une application monopage basée sur React sur Amazon S3 et CloudFront
- Déployez une API Amazon API Gateway sur un site Web interne à l'aide de points de terminaison privés et d'un Application Load Balancer
- Déploiement et débogage de clusters Amazon EKS
- Déployez et gérez un lac de données sans serveur sur le cloud AWS en utilisant l'infrastructure sous forme de code
- Déployez un cas d'utilisation de RAG AWS en utilisant Terraform et Amazon Bedrock
- Développez un assistant entièrement automatisé basé sur le chat en utilisant les agents et les bases de connaissances Amazon Bedrock
- Développez des assistants avancés basés sur l'IA générative basés sur le chat en utilisant RAG et des instructions ReAct

- Générez dynamiquement une politique IAM avec IAM Access Analyzer à l'aide de Step Functions
- Assurez-vous que la journalisation d'Amazon EMR sur Amazon S3 est activée au lancement
- Estimation du coût d'une table DynamoDB pour une capacité à la demande
- Générez des recommandations personnalisées et reclassées à l'aide d'Amazon Personalize
- Génération de données de test à l'aide d'une tâche AWS Glue et de Python
- SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL
- Implémentez le modèle de saga sans serveur à l'aide d'AWS Step Functions
- Améliorez les performances opérationnelles en activant Amazon DevOps Guru dans plusieurs régions AWS, sur plusieurs comptes et OUs avec le kit AWS CDK
- Lancez un CodeBuild projet sur des comptes AWS à l'aide de Step Functions et d'une fonction proxy Lambda
- Migrez les charges de travail Apache Cassandra vers Amazon Keyspaces à l'aide d'AWS Glue
- Surveillez l'utilisation d'une Amazon Machine Image partagée sur plusieurs Comptes AWS
- Optimisez les déploiements multicomptes sans serveur en utilisant les flux de travail et AWS CDK Actions GitHub
- Orchestrez un pipeline ETL avec validation, transformation et partitionnement à l'aide d'AWS Step Functions
- Interrogez les tables Amazon DynamoDB avec SQL à l'aide d'Amazon Athena
- Exécutez des charges de travail planifiées et pilotées par des événements à grande échelle avec AWS Fargate
- Diffusez du contenu statique dans un compartiment Amazon S3 via un VPC en utilisant Amazon CloudFront
- Simplifiez le développement et le déploiement des robots Amazon Lex à l'aide d'un flux de travail automatisé
- Structurer un projet Python dans une architecture hexagonale à l'aide d'AWS Lambda
- Translate le langage naturel en requêtes DSL pour OpenSearch et requêtes Elasticsearch
- Désactiver les contrôles standard de sécurité sur tous les comptes membres du Security Hub dans un environnement multi-comptes
- Déchargez les données d'un cluster Amazon Redshift entre différents comptes vers Amazon S3
- Coordonnez la dépendance des ressources et l'exécution des tâches à l'aide de la structure AWS Fargate WaitCondition hook

- Utilisez les agents Amazon Bedrock pour automatiser la création de contrôles d'accès dans Amazon EKS via des instructions textuelles

Réseaux

Rubriques

- Automatisez la configuration du peering interrégional avec AWS Transit Gateway
- Centralisez la connectivité réseau à l'aide d'AWS Transit Gateway
- Configurer le chiffrement HTTPS pour Oracle JD Edwards EnterpriseOne sur Oracle à l'aide WebLogic d'un Application Load Balancer
- Connectez-vous aux données et aux plans de contrôle du service de migration des applications via un réseau privé
- Créez des objets Infoblox à l'aide des ressources CloudFormation personnalisées AWS et d'Amazon SNS
- Personnalisez les CloudWatch alertes Amazon pour AWS Network Firewall
- Déployez des ressources dans une AWS Wavelength zone à l'aide de Terraform
- Migrer des enregistrements DNS en masse vers une zone hébergée privée Amazon Route 53
- Modifiez les en-têtes HTTP lors de la migration de F5 vers un Application Load Balancer sur AWS
- Accédez en privé à un point de terminaison de service AWS central à partir de plusieurs VPCs
- Créez un rapport sur les résultats de l'analyseur d'accès réseau pour l'accès Internet entrant en plusieurs Comptes AWS
- Configuration de la résolution DNS pour les réseaux hybrides dans un environnement multi-comptes AWS
- Vérifiez que les équilibreurs de charge ELB nécessitent une terminaison TLS
- Consultez les journaux et les statistiques d'AWS Network Firewall à l'aide de Splunk
- Plus de modèles

Automatisez la configuration du peering interrégional avec AWS Transit Gateway

Créée par Ram Kandaswamy (AWS)

Récapitulatif

AWS Transit Gateway connecte des clouds privés virtuels (VPCs) et des réseaux sur site via un hub central. Le trafic de Transit Gateway reste toujours sur le backbone mondial d'Amazon Web Services (AWS) et ne traverse pas l'Internet public, ce qui réduit les vecteurs de menaces, tels que les exploits courants et les attaques par déni de service (DDoS) distribué.

Si vous devez communiquer entre deux ou plusieurs régions AWS, vous pouvez utiliser le peering interrégional pour établir des connexions de peering entre les passerelles de transit de différentes régions. Cependant, la configuration manuelle du peering interrégional avec Transit Gateway peut être un processus fastidieux qui comporte plusieurs étapes. Ce modèle fournit un processus automatisé pour supprimer ces étapes manuelles en utilisant du code pour effectuer le peering. Vous pouvez utiliser cette approche si vous devez configurer plusieurs régions et comptes AWS à plusieurs reprises lors de la configuration d'une organisation multirégionale.

Ce modèle utilise une CloudFormation pile AWS qui inclut le flux de travail AWS Step Functions, les fonctions AWS Lambda, les rôles AWS Identity and Access Management (IAM) et les groupes de logs dans Amazon Logs. CloudWatch Vous pouvez ensuite lancer une exécution de Step Functions et créer la connexion de peering inter-régions pour vos passerelles de transport en commun. Pour configurer manuellement le peering interrégional, consultez Peer VPCs dans différentes régions AWS à l'aide d'AWS Transit Gateway.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un bucket Amazon Simple Storage Service (Amazon S3) existant.
- Passerelles de transit, créées et configurées dans la région demandeuse et dans les régions acceptrices. La région demandeuse est celle d'où provient une demande de peering et les régions acceptrices acceptent la demande de peering. Pour plus d'informations à ce sujet, consultez Création et acceptation d'une connexion d'appairage VPC dans la documentation Amazon VPC.

- VPCs, installé et configuré dans les régions de l'accepteur et du demandeur. Pour connaître les étapes de création d'un VPC, consultez la section Créer le VPC depuis Get Started with Amazon VPC dans la documentation Amazon VPC.
- Ils VPCs doivent utiliser la `addToTransitGateway` balise et `true` la valeur.
- Groupes de sécurité et listes de contrôle d'accès réseau (ACLs) pour vous VPCs, configurés selon vos besoins. Pour plus d'informations à ce sujet, consultez la section Groupes de sécurité pour votre VPC et votre réseau ACLs dans la documentation Amazon VPC.

Régions et limites AWS

- Seules certaines régions AWS prennent en charge le peering interrégional. Pour obtenir la liste complète des régions qui prennent en charge le peering interrégional, consultez AWS Transit Gateway. FAQs
- Dans l'exemple de code ci-joint, la région du demandeur est supposée êtreus-east-2, et la région de l'accepteur est supposée être. `us-west-2` Si vous souhaitez configurer différentes régions, vous devez modifier ces valeurs dans tous les fichiers Python. Pour implémenter une configuration plus complexe impliquant plus de deux régions, vous pouvez modifier la fonction Step pour transmettre les régions en tant que paramètre à la fonction Lambda et exécuter la fonction pour chaque combinaison.

Architecture

Le diagramme montre un flux de travail comportant les étapes suivantes :

1. L'utilisateur crée une CloudFormation pile AWS.
2. AWS CloudFormation crée une machine d'état Step Functions qui utilise une fonction Lambda. Pour plus d'informations à ce sujet, consultez la section Création d'une machine d'état Step Functions utilisant Lambda dans la documentation AWS Step Functions.
3. Step Functions appelle une fonction Lambda pour le peering.
4. La fonction Lambda crée une connexion d'appairage entre les passerelles de transit.
5. Step Functions appelle une fonction Lambda pour modifier la table de routage.
6. La fonction Lambda modifie les tables de routage en ajoutant le bloc Classless Inter-Domain Routing (CIDR) du. VPCs

Flux de travail Step Functions

Le diagramme montre le flux de travail Step Functions suivant :

1. Le flux de travail Step Functions appelle la fonction Lambda pour le peering de la passerelle de transit.
2. Il y a un appel du chronomètre pour attendre une minute.
3. L'état du peering est récupéré et envoyé au bloc de conditions. Le bloc est responsable de la boucle.
4. Si la condition de réussite n'est pas remplie, le flux de travail est codé pour passer à l'étape du chronomètre.
5. Si la condition de réussite est remplie, une fonction Lambda est appelée pour modifier les tables de routage. Après cet appel, le flux de travail Step Functions prend fin.

Outils

- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos ressources AWS.
- Amazon CloudWatch Logs — CloudWatch Logs vous permet de centraliser les journaux de tous vos systèmes, applications et services AWS que vous utilisez.
- AWS Identity and Access Management (IAM) — IAM est un service Web permettant de contrôler en toute sécurité l'accès aux services AWS.
- AWS Lambda — Lambda exécute votre code sur une infrastructure de calcul à haute disponibilité et exécute l'ensemble de l'administration des ressources de calcul.
- AWS Step Functions — Step Functions facilite la coordination des composants des applications distribuées sous la forme d'une série d'étapes dans un flux de travail visuel.

Épopées

Automatisez le peering

Tâche	Description	Compétences requises
Téléchargez les fichiers joints dans votre compartiment S3.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon S3, puis téléchargez les `get-transit-gateway-peering-status.zip` fichiers `modify-transit-gateway-routes.zip` `peer-transit-gateway.zip` , et (joints) dans votre compartiment S3.	AWS général
Créez la CloudFormation pile AWS.	Exécutez la commande suivante pour créer une CloudFormation pile AWS à l'aide du `transit-gateway-peering.json` fichier (joint) : `aws cloudformation create-stack --stack-name myteststack --template-body file://sampletemplate.json` La CloudFormation pile AWS crée le flux de travail Step Functions, les fonctions Lambda, les rôles IAM et CloudWatch les groupes de logs.	DevOps ingénieur

Tâche	Description	Compétences requises
	Assurez-vous que le CloudFormation modèle AWS fait référence au compartiment S3 qui contient les fichiers que vous avez chargés précédemment. **Note** Vous pouvez également créer une pile à l'aide de la CloudFormation console AWS. Pour plus d'informations à ce sujet, consultez la section Création d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation AWS.	

Tâche	Description	Compétences requises
Lancez une nouvelle exécution dans Step Functions .	Ouvrez la console Step Functions et lancez une nouvelle exécution. Step Functions appelle la fonction Lambda et crée la connexion d'appairage pour les passerelles de transit. Vous n'avez pas besoin d'un fichier JSON d'entrée. Vérifiez qu'une pièce jointe est disponible et que le type de connexion est Peering. Pour plus d'informations à ce sujet, consultez Démarrer une nouvelle exécution dans Getting started with AWS Step Functions dans la documentation AWS Steps Functions.	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
Vérifiez les itinéraires dans les tables de routage.	Le peering interrégional est établi entre les passerelles de transit. Les tables de routage sont mises à jour avec la plage de blocs IPv4 CIDR du VPC de la région homologue. Ouvrez la console Amazon VPC et choisissez l'onglet Associations dans la table de routage qui correspond à la pièce jointe de la passerelle de transit. Vérifiez la plage de blocs d'adresse CIDR VPC des régions homologues. Pour obtenir des instructi ons et des étapes détaillées, consultez la section Associer une table de routage de passerelle de transit dans la documentation Amazon VPC.	Administrateur réseau

Ressources connexes

- Exécutions dans Step Functions
- Accessoires de peering Transit Gateway
- VPCs Collaborez dans différentes régions AWS à l'aide d'AWS Transit Gateway
- Interconnexion entre VPCs les régions AWS à l'aide d'AWS Transit Gateway - Démo (vidéo)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Centralisez la connectivité réseau à l'aide d'AWS Transit Gateway

Créée par Mydhili Palagummi (AWS) et Nikhil Marrapu (AWS)

Récapitulatif

Ce modèle décrit la configuration la plus simple dans laquelle AWS Transit Gateway peut être utilisé pour connecter un réseau sur site à des clouds privés virtuels (VPCs) dans plusieurs comptes AWS au sein d'une région AWS. À l'aide de cette configuration, vous pouvez établir un réseau hybride qui connecte plusieurs réseaux VPC dans une région et un réseau sur site. Cela se fait en utilisant une passerelle de transit et une connexion de réseau privé virtuel (VPN) au réseau local.

Conditions préalables et limitations

Prérequis

- Un compte pour héberger des services réseau, géré en tant que compte membre d'une organisation dans AWS Organizations
- VPCs dans plusieurs comptes AWS, sans chevauchement de blocs de routage interdomaines sans classe (CIDR)

Limites

Ce modèle ne permet pas d'isoler le trafic entre certains réseaux VPCs ou le réseau local. Tous les réseaux rattachés à la passerelle de transit pourront se joindre les uns aux autres. Pour isoler le trafic, vous devez utiliser des tables de routage personnalisées sur la passerelle de transit. Ce modèle connecte uniquement le réseau VPCs et le réseau local à l'aide d'une seule table de routage de passerelle de transit par défaut, ce qui constitue la configuration la plus simple.

Architecture

Pile technologique cible

- AWS Transit Gateway
- Site-to-SiteVPN AWS
- VPC
- AWS Resource Access Manager (AWS RAM)

Architecture cible

Outils

Services AWS

- AWS Resource Access Manager (AWS RAM) vous permet de partager en toute sécurité vos ressources entre vos comptes AWS, vos unités organisationnelles ou l'ensemble de votre organisation depuis AWS Organizations.
- AWS Transit Gateway est un hub central qui connecte des clouds privés virtuels (VPCs) et des réseaux sur site.

Épopées

Création d'une passerelle de transit dans le compte de services réseau

Tâche	Description	Compétences requises
Créez une passerelle de transit.	Dans le compte AWS sur lequel vous souhaitez héberger les services réseau, créez une passerelle de transit dans la région AWS cible. Pour obtenir des instructions, voir Création d'une passerelle de transit. Remarques : • Sélectionnez Association de table de routage par défaut. • Sélectionnez Propagation de la table de routage par défaut.	Administrateur réseau

Connectez la passerelle de transit à votre réseau local

Tâche	Description	Compétences requises
Configurez un dispositif de passerelle client pour la connexion VPN.	Le dispositif de passerelle client est connecté du côté local de la connexion Site-to-Site VPN entre la passerell e de transit et votre réseau local. Pour plus d'informa tions, consultez la section Votre dispositif de passerell e client dans la documenta tion du Site-to-Site VPN AWS. Identifiez ou lancez un appareil client sur site pris en charge et notez son adresse IP publique. La configuration du VPN sera terminée plus tard dans cette épopée.	Administrateur réseau
Dans le compte de services réseau, créez une connexion VPN à la passerelle de transit.	Pour configurer une connexion , créez une pièce jointe VPN pour la passerelle de transit. Pour obtenir des instructi ons, consultez la section Pièces jointes du VPN Transit Gateway.	Administrateur réseau
Configurez le VPN sur le dispositif de passerelle client de votre réseau local.	Téléchargez le fichier de configuration de la connexion Site-to-Site VPN associée à la passerelle de transit et configurez les paramètre s VPN sur le périphérique de passerelle client. Pour obtenir des instructions, voir	Administrateur réseau

Tâche	Description	Compétences requises
	Télécharger le fichier de configuration.	

Partagez la passerelle de transit du compte de services réseau avec d'autres comptes AWS ou avec votre organisation

Tâche	Description	Compétences requises
Dans le compte de gestion AWS Organizations, activez le partage.	Pour partager la passerelle de transit avec votre organisation ou avec certaines unités organisationnelles, activez le partage dans AWS Organizations. Dans le cas contraire, vous devrez partager la passerelle de transit pour chaque compte individuellement. Pour obtenir des instructions, consultez Activer le partage de ressources au sein d'AWS Organizations.	Administrateur système AWS
Créez le partage de ressources de la passerelle de transit dans le compte de services réseau.	Pour autoriser VPCs d'autres comptes AWS de votre organisation à se connecter à la passerelle de transit, dans le compte de services réseau, utilisez la console AWS RAM pour partager les ressources de la passerelle de transit. Pour obtenir des instructions, voir Création d'un partage de ressources.	Administrateur système AWS

Connect VPCs à la passerelle de transit

Tâche	Description	Compétences requises
Créez des pièces jointes VPC dans des comptes individuels.	Dans les comptes avec lesquels la passerelle de transit a été partagée, créez des pièces jointes VPC de passerelle de transit. Pour obtenir des instructions, consultez la section Créer une passerelle de transit attachée à un VPC.	Administrateur réseau
Acceptez les demandes de pièces jointes VPC.	Dans le compte de services réseau, acceptez les demandes de rattachement VPC de la passerelle de transit. Pour obtenir des instructions, voir Accepter une pièce jointe partagée.	Administrateur réseau

Configurer le routage

Tâche	Description	Compétences requises
Configurez les itinéraires dans un compte individuel VPCs.	Dans chaque compte VPC individuel, ajoutez des itinéraires vers le réseau local et vers d'autres réseaux VPC, en utilisant la passerelle de transit comme cible. Pour obtenir des instructions, voir Ajouter et supprimer des itinéraires dans une table de routage.	Administrateur réseau

Tâche	Description	Compétences requises
Configurez les itinéraires dans la table des itinéraires de la passerelle de transit.	Les itinéraires en provenance VPCs et la connexion VPN doivent être propagés et doivent apparaître dans la table de routage par défaut de la passerelle de transit. Si nécessaire, créez des itinéraires statiques (par exemple des itinéraires statiques pour la connexion VPN statique) dans la table de routage par défaut de la passerelle de transit. Pour obtenir des instructions, consultez la section Création d'un itinéraire statique.	Administrateur réseau
Ajoutez des règles de groupe de sécurité et de liste de contrôle d'accès réseau (ACL).	Pour les EC2 instances et autres ressources du VPC, assurez-vous que les règles du groupe de sécurité et les règles ACL du réseau autorisent le trafic entre VPCs le réseau local et le réseau local. Pour obtenir des instructions, voir Contrôler le trafic vers les ressources à l'aide de groupes de sécurité et Ajouter et supprimer des règles dans une ACL.	Administrateur réseau

Testez la connectivité

Tâche	Description	Compétences requises
Testez la connectivité entre VPCs.	Assurez-vous que les ACL du réseau et les groupes de sécurité autorisent le trafic ICMP (Internet Control Message Protocol), puis envoyez un ping depuis les instances d'un VPC vers un autre VPC également connecté à la passerelle de transit.	Administrateur réseau
Testez la connectivité entre le réseau local VPCs et le réseau local.	Assurez-vous que les règles ACL du réseau, les règles des groupes de sécurité et les éventuels pare-feux autorisen t le trafic ICMP, puis envoyez un ping entre le réseau local et les EC2 instances du. VPCs La communication réseau doit d'abord être initiée à partir du réseau local pour que la connexion VPN soit rétablieUP.	Administrateur réseau

Ressources connexes

- Création d'une infrastructure réseau AWS multi-VPC évolutive et sécurisée (livre blanc AWS)
- Utilisation de ressources partagées (documentation AWS RAM)
- Utilisation des passerelles de transit (documentation AWS Transit Gateway)

Configurer le chiffrement HTTPS pour Oracle JD Edwards EnterpriseOne sur Oracle à l'aide WebLogic d'un Application Load Balancer

Créée par Thanigaivel Thirumalai (AWS)

Récapitulatif

Ce modèle explique comment configurer le chiffrement HTTPS pour le déchargement SSL dans Oracle JD Edwards EnterpriseOne sur des charges de WebLogic travail Oracle. Cette approche chiffre le trafic entre le navigateur de l'utilisateur et un équilibreur de charge afin de soulager les serveurs de la charge de chiffrement. EnterpriseOne

De nombreux utilisateurs font évoluer le niveau de la machine virtuelle EnterpriseOne JAVA (JVM) horizontalement à l'aide d'un AWS Application Load Balancer.L'équilibreur de charge sert de point de contact unique pour les clients et répartit le trafic entrant sur plusieurs JVMs sites. En option, l'équilibreur de charge peut répartir le trafic entre plusieurs zones de disponibilité et augmenter la disponibilité de EnterpriseOne.

Le processus décrit dans ce modèle configure le chiffrement entre le navigateur et l'équilibreur de charge au lieu de chiffrer le trafic entre l'équilibreur de charge et le. EnterpriseOne JVMs Cette approche est connue sous le nom de déchargement SSL. Le transfert du processus de déchiffrement SSL du serveur EnterpriseOne Web ou du serveur d'applications vers l'Application Load Balancer réduit la charge de travail du côté de l'application. Après l'arrêt du protocole SSL au niveau de l'équilibreur de charge, le trafic non chiffré est acheminé vers l'application sur AWS.

Oracle JD Edwards EnterpriseOne est une solution de planification des ressources d'entreprise (ERP) destinée aux entreprises qui fabriquent, construisent, distribuent, entretiennent ou gèrent des produits ou des actifs physiques. JD Edwards EnterpriseOne prend en charge divers matériels, systèmes d'exploitation et plateformes de base de données.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Rôle AWS Identity and Access Management (IAM) autorisé à effectuer des appels de service AWS et à gérer les ressources AWS
- Un certificat SSL

Versions du produit

- Ce modèle a été testé avec Oracle WebLogic 12c, mais vous pouvez également utiliser d'autres versions.

Architecture

Il existe plusieurs approches pour effectuer le déchargement SSL. Ce modèle utilise un Application Load Balancer et un serveur HTTP Oracle (OHS), comme illustré dans le schéma suivant.

Le schéma suivant montre la structure JVM de JD Edwards EnterpriseOne, d'Application Load Balancer et de Java Application Server (JAS).

Outils

Services AWS

- Les équilibreurs de charge des applications distribuent le trafic applicatif entrant sur plusieurs cibles, telles qu'Amazon Elastic Compute Cloud (EC2 instances Amazon), dans plusieurs zones de disponibilité.
- AWS Certificate Manager (ACM) vous aide à créer, stocker et renouveler les certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et applications AWS.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.

Bonnes pratiques

- Pour connaître les meilleures pratiques d'ACM, consultez la documentation d'ACM.

Épopées

Configuration WebLogic et SST

Tâche	Description	Compétences requises
Installez et configurez les composants Oracle.	1. Installez Fusion Middlewar e Infrastructure en suivant	JDE CNC, administrateur WebLogic

Tâche	Description	Compétences requises
	le processus d'installation standard. Ce programme permet d'installer et de configurer un WebLogic domaine. Pour obtenir des instructions, consultez la documentation Oracle. 2. Installez OHS en suivant le processus d'installation standard. Pour obtenir des instructions, consultez la documentation Oracle. 3. Lorsque l'installation est terminée, lancez l'assistant de configuration (`config.sh` fichier) pour configurer OHS. • Vous pouvez mettre à jour un domaine existant ou en créer un nouveau. Ce modèle suppose que vous mettez à jour un domaine existant. • Pour les modèles disponibles, choisissez Oracle Enterprise Manager-Restricted JRF et Oracle HTTP Server (Restricted JRF). La sélection de ces options JRF (Java Required Files) élimine la connexion à une base de données externe.	

Tâche	Description	Compétences requises
	• Pour les serveurs gérés, les clusters, les modèles de serveurs, les clusters de cohérence, les machines, l'attribution de serveurs aux machines, les cibles virtuelles et les partitions, acceptez les valeurs de configuration par défaut et choisisse z Next pour passer à la catégorie suivante. • Complétez les détails de configuration (par exemple, hôte et port de l'administrateur, adresse et port d'écoute, nom du serveur) pour l'instance OHS (par exemple,`ohs1`).	

Tâche	Description	Compétences requises
Activez le WebLogic plugin au niveau du domaine.	Le WebLogic plugin est nécessaire pour l'équilibrage de charge. Pour activer le plugin, procédez comme suit : 1. Connectez-vous à la console d' WebLogic administration en utilisant le lien suivant : `http://<WeblogicServer>:<Adminport>/console` 2. Choisissez Verrouiller et modifier, puis Configuration, Applications Web. 3. Choisissez le WebLogic plugin activé (case à cocher ou option déroulante). 4. Choisissez Enregistrer et activer les modifications.	JDE CNC, administrateur WebLogic

Tâche	Description	Compétences requises

Modifiez le fichier de configuration.	Le `mod_wl_ohs.conf` fichier configure les demandes de proxy d'OHS à WebLogic.
	1. Modifiez ce fichier. Il est situé à l'adresse suivante :
	`$ORACLE_HOME/user_projects/domains/`
	Par exemple :
	`/home/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/config/fmwconfig/components/OHS/instances/ohs1`
	2. Ajoutez les valeurs WebLogic host (`WebLogicHost`) et port (`WebLogicPort`) (ce modèle suppose localhost et port 8000.)
	3. Ajoutez `WLProxySSL` et `WLProxySSLPassThrough` valorisez comme suit :
	`<VirtualHost *:8000>`
	`<Location /jde>`
	`WLSRequest On`
	`SetHandler weblogic-handler`
		JDE CNC, administrateur WebLogic

Tâche	Description	Compétences requises

	`WebLogicHost localhost`
	`WebLogicPort 8000`
	`WLProxySSL On`
	`WLProxySSLPassThrough On`
	`</Location>`
	`</VirtualHost>`	

Tâche	Description	Compétences requises
Démarrez OHS à l'aide de l'Enterprise Manager.	1. Connectez-vous à Enterprise Manager Fusion Middleware en utilisant le lien suivant : `http://<WeblogicServer>:<Adminport>/em/` 2. Dans Target Navigation, sous Serveur HTTP, sélectionnez l'instance OHS (par exemple,`ohs1`). 3. Choisissez Arrêter et démarrer pour redémarrer l'instance OHS. 4. Lorsque la configuration OHS est terminée, vous pouvez vous connecter au client EnterpriseOne HTML en utilisant le nom d'hôte de votre serveur HTTP avec le port 8000 au lieu du nom d'hôte EnterpriseOne du serveur. • Ancien lien : `http://<Webserver>:80/jde/owhtml` • Nouveau lien : `http://<HTTP server or web server>:8000/jde/owhtml` Si vous utilisez un port autre que le port HTTP	JDE CNC, administrateur WebLogic

Tâche	Description	Compétences requises

	Oracle par défaut, modifiez le `httpd.conf` fichier pour ajouter un écouteur pour ce port à deux endroits :
	`#[Listen] OHS_LISTEN_PORT`
	`Listen 8000`
	et :
	`#`
	`ServerName <Weblogic Server1>:8000`	

Configuration de l'Application Load Balancer

Tâche	Description	Compétences requises
Configurez un groupe cible.	1. Créez un groupe cible pour le port 8000 du serveur HTTP. 2. Enregistrez les cibles sous le groupe cible avec le même port. 3. Vérifiez l'état des cibles pour confirmer qu'elles sont saines. 4. Configurez les paramètres du bilan de santé selon vos besoins.	Administrateur AWS

Tâche	Description	Compétences requises
	Pour obtenir des instructions détaillées, consultez la documentation d'Elastic Load Balancing.	
Configurez l'équilibreur de charge.	1. Créez un Application Load Balancer avec les attributs par défaut et le cloud privé virtuel (VPC), les groupes de sécurité et les sous-réseaux requis. Pour obtenir des instructions, consultez la documentation d'Elastic Load Balancing. 2. Ajoutez une entrée d'écoute pour HTTPS 443 et transmettez-la au groupe cible que vous avez créé à l'étape précédente. (Pour obtenir des instructions, consultez la documentation d'Elastic Load Balancing.) Un écouteur HTTPS nécessite un certificat SSL. Vous pouvez choisir un certificat auprès d'ACM ou en télécharger un. 3. Pour les deux écouteurs, activez l'adhérence en suivant les instructions de la documentation d'Elastic Load Balancing.	Administrateur AWS

Tâche	Description	Compétences requises
Ajoutez un enregistrement Route 53 (DNS).	(Facultatif) Vous pouvez ajouter un enregistrement DNS Amazon Route 53 pour le sous-domaine. Cet enregistrement pointerait vers votre Application Load Balancer. Pour obtenir des instructions, consultez la documentation de Route 53.	Administrateur AWS

Résolution des problèmes

Problème	Solution
Le serveur HTTP ne s'affiche pas.	Si le serveur HTTP n'apparaît pas dans la liste de navigation cible de la console Enterprise Manager, procédez comme suit : 1. Sous WebLogic Domaine, Administration, sélectionnez Instances OHS. 2. Choisissez Create pour créer une nouvelle instance OHS. 3. Entrez un nom d'instance, puis cliquez sur OK pour créer l'instance. Lorsque l'instance a été créée et que les modifications ont été activées, vous pouvez voir le serveur HTTP dans le panneau de navigation Target.

Ressources connexes

Documentation AWS

- Application Load Balancers
- Utilisation de zones hébergées publiques
- Utilisation des zones hébergées privées

Documentation Oracle :

- Présentation du plug-in Oracle WebLogic Server Proxy
- Installation WebLogic du serveur à l'aide de l'installateur d'infrastructure
- Installation et configuration du serveur HTTP Oracle

Connectez-vous aux données et aux plans de contrôle du service de migration des applications via un réseau privé

Créée par Dipin Jain (AWS) et Mike Kuznetsov (AWS)

Récapitulatif

Ce modèle explique comment vous connecter à un plan de AWS Application Migration Service données et à un plan de contrôle sur un réseau privé sécurisé à l'aide de points de terminaison VPC d'interface.

Le service de migration d'applications est une solution hautement automatisée lift-and-shift (réhébergement) qui simplifie, accélère et réduit le coût de la migration des applications vers. AWS Il permet aux entreprises de réhéberger un grand nombre de serveurs physiques, virtuels ou cloud sans problèmes de compatibilité, sans interruption des performances ou sans longues périodes de transition. Le service de migration des applications est disponible auprès du AWS Management Console. Cela permet une intégration fluide avec d'autres entreprises Services AWS AWS CloudTrail, telles qu'Amazon CloudWatch et AWS Identity and Access Management (IAM).

Vous pouvez vous connecter d'un centre de données source à un plan de données, c'est-à-dire à un sous-réseau servant de zone intermédiaire pour la réplication des données dans le VPC de destination AWS VPN , via une connexion privée à l'aide de services AWS Direct Connect ou du peering VPC dans Application Migration Service. Vous pouvez également utiliser les points de terminaison VPC d'interface alimentés par AWS PrivateLink pour vous connecter à un plan de contrôle du service de migration d'applications via un réseau privé.

Conditions préalables et limitations

Prérequis

- Sous-réseau de zone intermédiaire : avant de configurer le service de migration d'applications, créez un sous-réseau à utiliser comme zone intermédiaire pour les données répliquées depuis vos serveurs sources vers AWS (c'est-à-dire un plan de données). Vous devez spécifier ce sous-réseau dans le modèle de paramètres de réplication lorsque vous accédez pour la première fois à la console du service de migration d'applications. Vous pouvez remplacer ce sous-réseau pour des serveurs source spécifiques dans le modèle de paramètres de réplication. Bien que vous puissiez utiliser un sous-réseau existant dans votre Compte AWS, nous vous recommandons de créer un nouveau sous-réseau dédié à cette fin.

- Configuration réseau requise — Les serveurs de réplication lancés par Application Migration Service dans votre sous-réseau de zone de transit doivent être en mesure d'envoyer des données au point de terminaison de l'API Application Migration Service à l'adresse`https://mgn.<region>.amazonaws.com/`, où se `<region>` trouve le code vers lequel Région AWS vous effectuez la réplication (par exemple,`https://mgn.us-east-1.amazonaws.com`). Le service Amazon Simple Storage Service (Amazon S3) est requis pour télécharger le logiciel Application Migration URLs Service.
  - Le programme d'installation de l'agent de AWS réplication doit avoir accès à l'URL du compartiment Amazon Simple Storage Service (Amazon S3) que vous utilisez avec Application Migration Service. Région AWS
  - Le sous-réseau de la zone de transit doit avoir accès à Amazon S3.
  - Les serveurs sources sur lesquels l'agent de AWS réplication est installé doivent être en mesure d'envoyer des données aux serveurs de réplication du sous-réseau de la zone de transit et au point de terminaison de l'API du service de migration des applications à `https://mgn.<region>.amazonaws.com/` l'adresse.

Le tableau suivant répertorie les ports requis.

Source	Destination (Destination)	Port	Pour plus d'informations, voir
Centre de données source	Service Amazon S3 URLs	443 (TCP)	Communication via le port TCP 443
Centre de données source	Région AWS-adresse de console spécifique pour le service de migration d'applications	443 (TCP)	Communication entre les serveurs sources et le service de migration d'applications via le port TCP 443
Centre de données source	Sous-réseau de zone de transit	1500 (TCP)	Communication entre les serveurs sources et le sous-réseau de la zone de transit via le port TCP 1500

Sous-réseau de zone de transit	Région AWS-adresse de console spécifique pour le service de migration d'applications	443 (TCP)	Communication entre le sous-réseau de la zone de transit et le service de migration des applications via le port TCP 443
Sous-réseau de zone de transit	Service Amazon S3 URLs	443 (TCP)	Communication via le port TCP 443
Sous-réseau de zone de transit	Point de terminaison Amazon Elastic Compute Cloud (Amazon EC2) du sous-réseau Région AWS	443 (TCP)	Communication via le port TCP 443

Limitations liées à

Le service de migration d'applications n'est actuellement pas disponible sur tous Régions AWS les systèmes d'exploitation.

- Soutenu Régions AWS
- Systèmes d'exploitation pris en charge

Architecture

Le schéma suivant illustre l'architecture réseau d'une migration classique. Pour plus d'informations sur cette architecture, consultez la documentation du service de migration des applications et la vidéo sur l'architecture du service de migration des applications et l'architecture réseau.

La vue détaillée suivante montre la configuration des points de terminaison VPC d'interface dans la zone de transit (VPC) pour connecter Amazon S3 et Application Migration Service.

Outils

- AWS Application Migration Servicesimplifie, accélère et réduit le coût de réhébergement des applications sur. AWS
- Les points de terminaison VPC d'interface vous permettent de vous connecter à des services alimentés par AWS PrivateLink sans avoir besoin d'une passerelle Internet, d'un périphérique NAT, d'une connexion VPN ou d'une connexion. AWS Direct Connect Les instances de votre VPC ne requièrent pas d'adresses IP publiques pour communiquer avec les ressources du service. Le trafic entre votre VPC et les autres services ne quitte pas le réseau Amazon.

Épopées

Créez des points de terminaison pour Application Migration Service EC2, Amazon et Amazon S3

Tâche	Description	Compétences requises
Configurez le point de terminaison de l'interface pour le service de migration d'applications.	Le centre de données source et le VPC de la zone de transit se connectent de manière privée au plan de contrôle du service de migration des applications via le point de terminaison d'interface que vous créez dans le VPC de la zone de transit cible. Pour créer le point de terminaison : 1. Ouvrez la console Amazon Virtual Private Cloud (Amazon VPC). 2. Dans le volet de navigation, sélectionnez Points de terminaison, Créer un point de terminaison.	Responsable de la migration

Tâche	Description	Compétences requises
	3. Pour Service category (Catégorie de service), choisissez Services AWS. 4. Dans Nom du service, entrez`com.amazonaws.<region>.mgn`. Pour Type, choisissez Interface. 5. Pour le VPC, sélectionnez un VPC de zone intermédiaire cible pour créer le point de terminaison. 6. Pour les sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer les interfaces réseau des points de terminaison. 7. Pour activer le DNS privé pour le point de terminaison de l'interface, dans la section Paramètres supplémentaires, sélectionnez Activer le nom DNS. 8. Sélectionnez un groupe de sécurité qui autorise l'entrée depuis le sous-réseau VPC de la zone intermédiaire via TCP 443. 9. Choisissez Créer un point de terminaison.	

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Accès et Service AWS utilisation d'un point de terminaison VPC d'interface dans la documentation Amazon VPC.	
Configurez le point de terminaison de l'interface pour Amazon EC2.	Le VPC de zone de transit se connecte de manière privée à l' EC2 API Amazon via le point de terminaison d'interface que vous créez dans le VPC de zone de transit cible. Pour créer le point de terminaison, suivez les instructions fournies dans l'article précédent. • Pour le nom du service, entrez `com.amazonaws.<region>.ec2` . Pour Type, choisissez Interface. • Le groupe de sécurité doit autoriser le trafic HTTPS entrant depuis le sous-réseau VPC de la zone de transit via le port 443. • Dans la section Paramètres supplémentaires, sélectionnez Activer le nom DNS.	Responsable de la migration

Tâche	Description	Compétences requises
Configurez le point de terminaison de l'interface pour Amazon S3.	Le centre de données source et le VPC de la zone de transit se connectent de manière privée à l'API Amazon S3 via le point de terminaison d'interface que vous créez dans le VPC de la zone de transit cible. Pour créer le point de terminaison, suivez les instructions fournies dans le premier article. • Dans Nom du service, entrez`com.amazonaws.<region>.s3` . Pour Type, choisissez Interface. • Le groupe de sécurité VPC doit autoriser le trafic HTTPS entrant depuis le sous-réseau VPC de la zone de transit via le port 443. • Dans la section Paramètres supplémentaires, désélectionnez Activer le nom DNS. Les points de terminaison de l'interface Amazon S3 ne prennent pas en charge les noms DNS privés.	Responsable de la migration

Tâche	Description	Compétences requises
	Note Vous utilisez un point de terminaison d'interface car les connexions de point de terminaison de passerelle ne peuvent pas être étendues hors d'un VPC. (Pour plus de détails, consultez la AWS PrivateLink documentation.)	

Tâche	Description	Compétences requises
Configurez le point de terminaison Amazon S3 Gateway.	Pendant la phase de configuration, le serveur de réplication doit se connecter à un compartiment S3 pour télécharger les mises à jour logicielles du serveur de AWS réplication. Toutefois, les points de terminaison de l'interface Amazon S3 ne prennent pas en charge les noms DNS privés, et il n'existe aucun moyen de fournir un nom DNS de point de terminaison Amazon S3 à un serveur de réplication. Pour atténuer ce problème, vous créez un point de terminaison de passerelle Amazon S3 dans le VPC auquel appartient le sous-réseau de la zone de transit, et vous mettez à jour les tables de routage du sous-réseau de transit avec les routes pertinentes. Pour plus d'informations, consultez la section Créer un point de terminaison de passerelle dans la AWS PrivateLink documentation.	Administrateur du cloud

Tâche	Description	Compétences requises
Configurez le DNS local pour résoudre les noms DNS privés des points de terminaison.	Les points de terminaison de l'interface pour Application Migration Service et Amazon EC2 possèdent des noms DNS privés qui peuvent être résolus dans le VPC. Toutefois, vous devez également configurer des serveurs locaux pour résoudre les noms DNS privés pour ces points de terminaison d'interface. Il existe plusieurs manières de configurer ces serveurs. Dans ce modèle, nous avons testé cette fonctionnalité en transférant les requêtes DNS locales au point de terminaison Amazon Route 53 Resolver entrant dans le VPC de la zone de transit. Pour plus d'informations, consultez la section Résolution des requêtes DNS entre VPCs et votre réseau dans la documentation Route 53.	Ingénieur en migration

Connectez-vous au plan de contrôle du service de migration des applications via un lien privé

Tâche	Description	Compétences requises
Installez l'agent AWS de réplication à l'aide de AWS PrivateLink.	1. Téléchargez l'agent de AWS réplication dans un compartiment S3 privé de la région de destination. 2. Connectez-vous aux serveurs sources à migrer. Le programme d'install ation de l'agent de AWS réplication a besoin d'un accès réseau au service de migration d'applications et aux points de terminaison Amazon S3. Étant donné que votre réseau sur site n'est pas ouvert aux points de terminaison publics d'Application Migration Service et Amazon S3, vous devez installer l'agent à l'aide des points de terminaison d'interface que vous avez créés au cours des étapes précédentes à l'aide de. AWS PrivateLink Voici un exemple pour Linux : 1. Téléchargez l'agent à l'aide de la commande suivante : `wget -O ./aws-replication-installer-init.py \`	Ingénieur en migration

Tâche	Description	Compétences requises

	`https://aws-application-migration-service-<aws_region>.bucket.<s3-endpoint-DNS-name>/latest/linux/aws-replication-installer-init.py`
	
	Par exemple, si le nom DNS du point de terminaison de l'interface Amazon S3 est `vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com` et Région AWS est `us-west-1`, vous devez utiliser la commande suivante :
	
	`wget -O ./aws-replication-installer-init.py \ https://aws-application-migration-service-us-west-1.bucket.vpce-009c8b07adb052a11-qgf8q50y.s3.us-west-1.vpce.amazonaws.com/latest/linux/aws-replication-installer-init.py`	

Tâche	Description	Compétences requises

> **Note**
>
> `bucket`est un mot clé statique que vous devez ajouter avant le nom DNS du point de terminaison de l'interface Amazon S3. Pour plus d'informations, consultez la documentation Amazon S3.

2. Installez l'agent :
   - Si vous avez sélectionné Activer le nom DNS lorsque vous avez créé un point de terminaison d'interface pour le service de migration d'applications, exécutez la commande :

```
    sudo python3
 aws-replication-in
staller-init.py \
    --region
 <aws_region> \
    --aws-access-
key-id <access-k
ey> \
    --aws-secret-
access-key <secret-
key> \
```

Tâche	Description	Compétences requises

	<pre>--no-prompt \
	--s3-endpoint
	<s3-endpoint-DNS-name></pre>
	• Si vous n'avez pas sélectionné Activer le nom DNS lorsque vous avez créé le point de terminaison de l'interface pour le service de migration d'applications, exécutez la commande :
	<pre>sudo python3
	aws-replication-installer-init.py \
	--region
	<aws_region> \
	--aws-access-key-id <access-key> \
	--aws-secret-access-key <secret-key> \
	--no-prompt \
	--s3-endpoint
	<s3-endpoint-DNS-name> \
	--endpoint
	<mgn-endpoint-DNS-name></pre>
	Pour plus d'informations, consultez les instructions d'installation de l'agent de AWS réplication dans la documentation du service de migration d'applications.	

Tâche	Description	Compétences requises
	Après avoir établi votre connexion avec le service de migration d'applications et installé l'agent de AWS réplication, suivez les instructions de la documentation du service de migration d'applications pour migrer vos serveurs sources vers votre VPC et votre sous-réseau cibles.	

Ressources connexes

Documentation du service de migration d'applications

- Concepts
- Flux de travail de migration
- Guide de démarrage rapide
- FAQ
- Dépannage

Ressources supplémentaires

- Réhébergement de vos applications dans une architecture multi-comptes en AWS utilisant des points de terminaison d'interface VPC (guide prescriptif)AWS
- AWS Application Migration Service — Une introduction technique (présentation détaillée de AWS la formation et de la certification)
- AWS Application Migration Service architecture et architecture réseau (vidéo)

Informations supplémentaires

Résolution des problèmes d'installation de l'agent de AWS réplication sur des serveurs Linux

Si une erreur gcc s'affiche sur un serveur Amazon Linux, configurez le référentiel de packages et utilisez la commande suivante :

```
## sudo yum groupinstall "Development Tools"
```

Créez des objets Infoblox à l'aide des ressources CloudFormation personnalisées AWS et d'Amazon SNS

Créée par Tim Sutton (AWS)

Récapitulatif

Remarque : n' AWS Cloud9 est plus disponible pour les nouveaux clients. Les clients existants de AWS Cloud9 peuvent continuer à utiliser le service normalement. En savoir plus

Le système de noms de domaine (DNS) Infoblox, le protocole DHCP (Dynamic Host Configuration Protocol) et la gestion des adresses IP (Infoblox DDI) vous permettent de centraliser et de contrôler efficacement un environnement hybride complexe. Avec Infoblox DDI, vous pouvez découvrir et enregistrer tous les actifs du réseau dans une base de données de gestion des adresses IP (IPAM) faisant autorité, en plus de gérer le DNS sur site et sur le cloud Amazon Web Services (AWS) en utilisant les mêmes appareils.

Ce modèle décrit comment utiliser une ressource CloudFormation personnalisée AWS pour créer des objets Infoblox (par exemple, des enregistrements DNS ou des objets IPAM) en appelant l'API Infoblox WAPI. Pour plus d'informations sur l'Infoblox WAPI, consultez la documentation WAPI dans la documentation Infoblox.

En utilisant l'approche de ce modèle, vous pouvez obtenir une vue unifiée des enregistrements DNS et des configurations IPAM pour vos environnements AWS et sur site, en plus de supprimer les processus manuels qui créent des enregistrements et approvisionnent vos réseaux. Vous pouvez utiliser l'approche de ce modèle pour les cas d'utilisation suivants :

- Ajouter un enregistrement A après avoir créé une instance Amazon Elastic Compute Cloud (Amazon EC2)
- Ajouter un enregistrement CNAME après avoir créé un Application Load Balancer
- Ajouter un objet réseau après la création d'un cloud privé virtuel (VPC)
- Fournir la plage réseau suivante et utiliser cette plage pour créer des sous-réseaux

Vous pouvez également étendre ce modèle et utiliser d'autres fonctionnalités de l'appareil Infoblox, telles que l'ajout de différents types d'enregistrement DNS ou la configuration d'Infoblox vDiscovery.

Le modèle utilise une hub-and-spoke conception dans laquelle le hub nécessite une connectivité à l'appliance Infoblox sur le cloud AWS ou sur site et utilise AWS Lambda pour appeler l'API Infoblox.

Le spoke se trouve sur le même compte ou sur un compte différent de la même organisation dans AWS Organizations et appelle la fonction Lambda à l'aide d'une ressource CloudFormation personnalisée AWS.

Conditions préalables et limitations

Prérequis

- Une appliance ou une grille Infoblox existante, installée sur le cloud AWS, sur site, ou les deux, et configurée avec un utilisateur administrateur capable d'administrer les actions IPAM et DNS. Pour plus d'informations à ce sujet, consultez la section À propos des comptes d'administrateur dans la documentation d'Infoblox.
- Zone DNS autoritaire existante à laquelle vous souhaitez ajouter des enregistrements sur l'appliance Infoblox. Pour plus d'informations à ce sujet, consultez la section Configuration des zones faisant autorité dans la documentation d'Infoblox.
- Deux comptes AWS actifs dans AWS Organizations. L'un des comptes est le compte hub et l'autre est le compte Spoke.
- Les comptes hub et spoke doivent se trouver dans la même région AWS.
- Le VPC du compte hub doit se connecter à l'appliance Infoblox, par exemple en utilisant AWS Transit Gateway ou le peering VPC.
- AWS Serverless Application Model (AWS SAM), installé et configuré localement avec AWS Cloud9 ou AWS. CloudShell
- Les `ClientTest.yaml` fichiers `Infoblox-Hub.zip` et (joints), téléchargés dans l'environnement local qui contient AWS SAM.

Limites

- Le jeton de service de la ressource CloudFormation personnalisée AWS doit provenir de la même région que celle dans laquelle la pile est créée. Nous vous recommandons d'utiliser un compte hub dans chaque région, au lieu de créer une rubrique Amazon Simple Notification Service (Amazon SNS) dans une région et d'appeler la fonction Lambda dans une autre région.

Versions du produit

- API Infoblox version 2.7

Architecture

Les diagrammes suivants montrent le flux de travail de ce modèle.

Le schéma montre les composants suivants pour la solution de ce modèle :

1. CloudFormation Les ressources personnalisées AWS vous permettent d'écrire une logique de provisionnement personnalisée dans des modèles qu'AWS CloudFormation exécute lorsque vous créez, mettez à jour ou supprimez des piles. Lorsque vous créez une pile, AWS CloudFormation envoie une `create` demande à une rubrique SNS surveillée par une application exécutée sur une EC2 instance.
2. La notification Amazon SNS provenant de la ressource CloudFormation personnalisée AWS est chiffrée au moyen d'une clé AWS Key Management Service (AWS KMS) spécifique et l'accès est limité aux comptes de votre organisation dans Organizations. La rubrique SNS lance la ressource Lambda qui appelle l'API WAPI Infoblox.
3. Amazon SNS invoque les fonctions Lambda suivantes qui utilisent l'URL de l'API Infoblox, le nom d'utilisateur et le mot de passe AWS Secrets Manager Amazon Resource Names () comme variables d'environnement : ARNs
   - `dnsapi.lambda_handler`— Reçoit les `DNSValue` valeurs `DNSNameDNSType`, et de la ressource CloudFormation personnalisée AWS et les utilise pour créer des enregistrements DNS A et des CNAMES.
   - `ipaddr.lambda_handler`— Reçoit les `Network Name` valeurs `VPCCIDR TypeSubnetPrefix`,, et de la ressource CloudFormation personnalisée AWS et les utilise pour ajouter les données réseau dans la base de données Infoblox IPAM ou fournir la ressource personnalisée au prochain réseau disponible pouvant être utilisé pour créer de nouveaux sous-réseaux.
   - `describeprefixes.lambda_handler`— Appelle l'API `describe_managed_prefix_lists` AWS en utilisant le `"com.amazonaws."+Region +".s3"` filtre pour récupérer les informations requises`prefix ID`.

> **Important**
>
> Ces fonctions Lambda sont écrites en Python et sont similaires les unes aux autres, mais leurs appels sont différents. APIs

4. Vous pouvez déployer la grille Infoblox sous forme d'appliances réseau physiques, virtuelles ou basées sur le cloud. Il peut être déployé sur site ou en tant qu'appliance virtuelle à l'aide d'une gamme d'hyperviseurs, notamment VMware ESXi Microsoft Hyper-V, Linux KVM et Xen. Vous pouvez également déployer la grille Infoblox sur le cloud AWS avec une Amazon Machine Image (AMI).
5. Le schéma montre une solution hybride pour la grille Infoblox qui fournit le DNS et l'IPAM aux ressources sur le cloud AWS et sur site.

Pile technologique

- AWS CloudFormation
- IAM
- AWS KMS
- AWS Lambda
- AWS SAM
- AWS Secrets Manager
- Amazon SNS
- Amazon VPC

Outils

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizations est un service de gestion de comptes qui vous aide à consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.

- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- AWS Serverless Application Model (AWS SAM) est un framework open source qui vous aide à créer des applications sans serveur dans le cloud AWS.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Code

Vous pouvez utiliser l'`ClientTest.yaml`exemple de CloudFormation modèle AWS (ci-joint) pour tester le hub Infoblox. Vous pouvez personnaliser le CloudFormation modèle AWS pour inclure les ressources personnalisées du tableau suivant.

Créez un enregistrement A à l'aide de la ressource personnalisée Infoblox Spoke	Valeurs renvoyées :
	`infobloxref` — Références d'Infoblox
	Exemple de ressource :
	`ARECORDCustomResource:`
	`Type: "Custom::InfobloxAPI"`
	`Properties:`
	`ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxDNSFunction`
	`DNSName: 'arecordtest.company.com'`
	`DNSType: 'ARecord'`

```
    DNSValue: '10.0.0.1'
```

Créez un enregistrement CNAME à l'aide de la ressource personnalisée Infoblox Spoke

Valeurs renvoyées :

`infobloxref` — Références d'Infoblox

Exemple de ressource :

```
CNAMECustomResource:

  Type: "Custom::InfobloxAPI"

  Properties:

    ServiceToken: !Sub arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfoblox

    DNSFunction

    DNSName: 'cnametest.company.com'

    DNSType: 'cname'

    DNSValue: 'aws.amazon.com'
```

Créez un objet réseau à l'aide de la ressource personnalisée Infoblox Spoke

Valeurs renvoyées :

`infobloxref` — Références d'Infoblox

`network`— Portée du réseau (identique à`VPCCIDR`)

Exemple de ressource :

```
VPCCustomResource:

  Type: 'Custom::InfobloxAPI'

  Properties:

    ServiceToken: !Sub  arn:aws:sns:
${AWS::Region}:${HubAccountID}:Ru
nInfobloxNextSubnetFunction

    VPCCIDR: !Ref VpcCIDR

    Type: VPC

    NetworkName: My-VPC
```

Récupérez le prochain sous-réseau disponible à l'aide de la ressource personnalisée Infoblox Spoke	Valeurs renvoyées :
	`infobloxref` — Références d'Infoblox
	`network` — La portée réseau du sous-réseau
	Exemple de ressource :
	`Subnet1CustomResource:`
	`  Type: 'Custom::InfobloxAPI'`
	`  DependsOn: VPCCustomResource`
	`  Properties:`
	`  ServiceToken: !Sub arn:aws:sns:${AWS::Region}:${HubAccountID}:RunInfobloxNextSubnetFunction`
	`  VPCCIDR: !Ref VpcCIDR`
	`  Type: Subnet`
	`  SubnetPrefix: !Ref SubnetPrefix`
	`NetworkName: My-Subnet`

Épopées

Création et configuration du VPC du compte hub

Tâche	Description	Compétences requises
Créez un VPC avec une connexion à l'appliance Infoblox.	Connectez-vous à la console de gestion AWS pour votre compte hub et créez un VPC en suivant les étapes décrites dans le déploiement de référence Amazon VPC on	Administrateur réseau, administrateur système

Tâche	Description	Compétences requises
	the AWS Cloud Quick Start à partir d'AWS Quick Starts. **Important** Le VPC doit disposer d'une connectivité HTTPS avec l'appliance Infoblox et nous vous recommandons d'utiliser un sous-réseau privé pour cette connexion.	

Tâche	Description	Compétences requises
(Facultatif) Créez les points de terminaison VPC pour les sous-réseaux privés.	Les points de terminaison VPC fournissent une connectivité aux services publics pour vos sous-réseaux privés. Les points de terminaison suivants sont requis : • Un point de terminaison de passerelle pour Amazon Simple Storage Service (Amazon S3) permettant à Lambda de communiquer avec AWS CloudFormation • Un point de terminaison d'interface permettant à Secrets Manager de se connecter à Secrets Manager • Un point de terminaison d'interface pour AWS KMS permettant le chiffrement de la rubrique SNS et du secret Secrets Manager Pour plus d'informations sur la création de points de terminaison pour les sous-réseaux privés, consultez la section Points de terminaison VPC dans la documentation Amazon VPC.	Administrateur réseau, administrateur système

Déployez le hub Infoblox

Tâche	Description	Compétences requises
Créez le modèle AWS SAM.	1. Exécutez la `unzip Infoblox-Hub.zip` commande dans l'environnement qui contient AWS SAM. 2. Exécutez la `cd Hub/` commande pour remplacer votre répertoire par le `Hub` répertoire. 3. Exécutez la `sam build` commande pour traiter le fichier modèle AWS SAM, le code de l'application, ainsi que tous les fichiers et dépendances spécifiques à la langue. La `sam build` commande copie également les artefacts de construction au format et à l'emplacement attendus pour l'histoire suivante.	Développeur, administrateur système
Déployez le modèle AWS SAM.	La `sam deploy` commande prend les paramètres requis et les enregistre dans le `samconfig.toml` fichier, stocke le CloudFormation modèle AWS et les fonctions Lambda dans un compartiment S3, puis déploie le CloudFormation modèle AWS dans votre compte de hub.	Développeur, administrateur système

Tâche	Description	Compétences requises

	L'exemple de code suivant montre comment déployer le modèle AWS SAM :
	
	`$ sam deploy --guided`
	
	`Configuring SAM deploy`
	`==========`
	`==`
	`Looking for config file [samconfig.toml] : Found`
	`Reading default arguments : Success`
	`Setting default arguments for 'sam deploy'`
	`==========`
	`==========`
	`Stack Name [Infoblox-Hub]:`
	`AWS Region [eu-west-1]:`
	`Parameter InfobloxUsername:`
	`Parameter InfobloxPassword:`
	`Parameter InfobloxIPAddress [xxx.xxx.xx.xxx]:`
	`Parameter AWSOrganisationID [o-xxxxxxxxx]:`
	`Parameter VPCID [vpc-xxxxxxxxx]:`
	`Parameter VPCCIDR [xxx.xxx.xxx.xxx/16]:`	

Tâche	Description	Compétences requises
	Parameter VPCSubnetID1 [subnet-xxx]: Parameter VPCSubnetID2 [subnet-xxx]: Parameter VPCSubnetID3 [subnet-xxx]: Parameter VPCSubnetID4 []: #Shows you resources changes to be deployed and require a 'Y' to initiate deploy Confirm changes before deploy [Y/n]: y #SAM needs permission to be able to create roles to connect to the resources in your template Allow SAM CLI IAM role creation [Y/n]: n Capabilities [['CAPABILITY_NAMED_IAM']]: Save arguments to configuration file [Y/n]: y SAM configuration file [samconfig.toml]: SAM configuration environment [default]: **Important** Vous devez utiliser `--guided` cette	

Tâche	Description	Compétences requises
	option à chaque fois car les informations de connexion à Infoblox ne sont pas stockées dans le fichier. `samconfig.toml`	

Ressources connexes

- Commencer à WAPIs utiliser Postman (Infoblox Blog)
- Provisionner des VNIO pour AWS à l'aide du modèle BYOL (documentation Infoblox)
- quickstart-aws-vpc(GitHub dépôt)
- describe_managed_prefix_lists (kit de développement logiciel AWS pour la documentation Python)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Personnalisez les CloudWatch alertes Amazon pour AWS Network Firewall

Créée par Jason Owens (AWS)

Récapitulatif

Le modèle vous permet de personnaliser les CloudWatch alertes Amazon générées par AWS Network Firewall. Vous pouvez utiliser des règles prédéfinies ou créer des règles personnalisées qui déterminent le message, les métadonnées et la gravité des alertes. Vous pouvez ensuite agir en fonction de ces alertes ou automatiser les réponses d'autres services Amazon, tels qu'Amazon EventBridge.

Dans ce modèle, vous générez des règles de pare-feu compatibles avec Suricata. Suricata est un moteur de détection de menaces open source. Vous créez d'abord des règles simples, puis vous les testez pour confirmer que les CloudWatch alertes sont générées et enregistrées. Une fois que vous avez testé les règles avec succès, vous les modifiez pour définir des messages, des métadonnées et des niveaux de sévérité personnalisés, puis vous effectuez un nouveau test pour confirmer les mises à jour.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Command Line Interface (AWS CLI) installé et configuré sur votre poste de travail Linux, macOS ou Windows. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.
- AWS Network Firewall installé et configuré pour utiliser CloudWatch les journaux. Pour plus d'informations, consultez la section Enregistrement du trafic réseau depuis AWS Network Firewall.
- Une instance Amazon Elastic Compute Cloud (Amazon EC2) dans un sous-réseau privé d'un cloud privé virtuel (VPC) protégé par Network Firewall.

Versions du produit

- Pour la version 1 de AWS CLI, utilisez 1.18.180 ou version ultérieure. Pour la version 2 de AWS CLI, utilisez la version 2.1.2 ou ultérieure.
- Le fichier classification.config de Suricata version 5.0.2. Pour obtenir une copie de ce fichier de configuration, consultez la section Informations supplémentaires.

Architecture

Le schéma d'architecture montre le flux de travail suivant :

1. Une EC2 instance Amazon située dans un sous-réseau privé envoie une demande à l'aide de curl ou de Wget.
2. Network Firewall traite le trafic et génère une alerte.
3. Network Firewall envoie les alertes enregistrées à CloudWatch Logs.

Outils

Services AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- AWS Network Firewallest un pare-feu réseau géré et dynamique ainsi qu'un service de détection et de prévention des intrusions pour les clouds privés virtuels (VPCs) dans le AWS Cloud.

Autres outils

- curl est un outil de ligne de commande et une bibliothèque open source.
- GNU Wget est un outil de ligne de commande gratuit.

Épopées

Création des règles de pare-feu et du groupe de règles

Tâche	Description	Compétences requises
Création de règles.	1. Dans un éditeur de texte, créez une liste de règles	Administrateur système AWS, administrateur réseau

Tâche	Description	Compétences requises

	que vous souhaitez ajouter au pare-feu. Chaque règle doit figurer sur une ligne distincte. La valeur du `classtype` paramètre provient du fichier de configuration de classification Suricata par défaut. Pour le contenu complet du fichier de configuration, consultez la section Informations supplémentaires. Voici deux exemples de règles.
	
	`alert http any any -> any any (content:"badstuff"; classtype:misc-activity; sid:3; rev:1;)`
	`alert http any any -> any any (content:"morebadstuff"; classtype:bad-unknown; sid:4; rev:1;)`
	
	2. Enregistrez les règles dans un fichier nommé`custom.rules` .	

Tâche	Description	Compétences requises

Créez le groupe de règles.	Dans le AWS CLI, entrez la commande suivante. Cela crée le groupe de règles.
	
	`# aws network-firewall create-rule-group \ --rule-group-name custom --type STATEFUL \ --capacity 10 --rules file://custom.rules \ --tags Key=environment,Value=development`
	
	Voici un exemple de sortie. Prenez note du`RuleGroup Arn`, dont vous aurez besoin à une étape ultérieure.
	
	`{ "UpdateToken": "4f998d72-973c-490a-bed2-fc3460547e23", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL",`
		Administrateur système AWS

Tâche	Description	Compétences requises

	"Capacity": 10,
	"RuleGrou
	pStatus": "ACTIVE",
	"Tags": [
	{
	"Key":
	"environment",
	"Value":
	"development"
	}
	]
	}	

Mettre à jour la politique de pare-feu

Tâche	Description	Compétences requises
Obtenez l'ARN de la politique de pare-feu.	Dans le AWS CLI, entrez la commande suivante. Cela renvoie le nom de ressource Amazon (ARN) de la politique de pare-feu. Enregistrez l'ARN pour une utilisation ultérieure dans ce modèle. `# aws network-firewall describe-firewall \ --firewall-name aws-network-firewall-anfw \ --query 'Firewall.FirewallPolicyArn'` Voici un exemple d'ARN renvoyé par cette commande.	Administrateur système AWS

Tâche	Description	Compétences requises
	`"arn:aws:network-firewall:us-east-2:1234567890:firewall-policy/firewall-policy-anfw"`	

Tâche	Description	Compétences requises

Mettez à jour la politique de pare-feu.	Dans un éditeur de texte, copiez-collez le code suivant. `<RuleGroupArn>` Remplacez-le par la valeur que vous avez enregistrée dans l'épopée précédente. Enregistrez le fichier sous le nom `firewall-policy-anfw.json` .
	
	`{`
	`  "StatelessDefaultActions": [`
	`  "aws:forward_to_sfe"`
	`  ],`
	`  "StatelessFragmentDefaultActions": [`
	`  "aws:forward_to_sfe"`
	`  ],`
	`  "StatefulRuleGroupReferences": [`
	`  {`
	`  "ResourceArn": "<RuleGroupArn>"`
	`  }`
	`  ]`
	`}`
	
	Entrez la commande suivante dans le AWS CLI. Cette commande nécessite un jeton de mise à jour pour ajouter les nouvelles règles. Le jeton est utilisé pour confirmer que la politique n'a pas changé
		Administrateur système AWS

Tâche	Description	Compétences requises

	depuis que vous l'avez récupérée pour la dernière fois.
	
	`UPDATETOKEN=(`aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --output text --query UpdateToken`)`
	
	`aws network-firewall update-firewall-policy \ --update-token $UPDATETOKEN \ --firewall-policy-name firewall-policy-anfw \ --firewall-policy file://firewall-policy-anfw.json`	

Tâche	Description	Compétences requises

Confirmez les mises à jour des politiques.	(Facultatif) Si vous souhaitez confirmer que les règles ont été ajoutées et consulter le format de la politique, entrez la commande suivante dans le AWS CLI.
	
	`# aws network-firewall describe-firewall-policy \ --firewall-policy-name firewall-policy-anfw \ --query FirewallPolicy`
	
	Voici un exemple de sortie.
	
	`{ "StatelessDefaultActions": [ "aws:forward_to_sfe" ], "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ], "StatefulRuleGroupReferences": [ { "ResourceArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom" }`
		Administrateur système AWS

Tâche	Description	Compétences requises
	<pre>] }</pre>	

Fonctionnalité d'alerte de test

Tâche	Description	Compétences requises

Générez des alertes pour les tests.	1. Connectez-vous à un poste de test dans le sous-réseau du pare-feu.
	2. Entrez les commandes qui devraient générer des alertes. Par exemple, vous pouvez utiliser `wget` ou `curl`.
	<pre>wget -U "badstuff"
	 http://www.amazon.
	com -o /dev/null</pre>
	<pre>curl -A "morebads
	tuff" http://ww
	w.amazon.com -o /
	dev/null</pre>
		Administrateur système AWS

Vérifiez que les alertes sont enregistrées.	1. Ouvrez la CloudWatch console. 2. Accédez au groupe de journaux et au flux appropriés. Pour plus d'informations, voir Afficher les données de journal envoyées à CloudWatch	Administrateur système AWS

Tâche	Description	Compétences requises

	Logs (documentation sur CloudWatch les journaux).
	3. Vérifiez que les événements enregistrés sont similaires aux exemples suivants. Les exemples montrent uniquement la partie pertinente de l'alerte.
	
	Exemple 1
	
	`"alert": { "action": "allowed", "signature_id": 3, "rev": 1, "signature": "", "category": "Misc activity", "severity": 3 }`
	
	Exemple 2
	
	`"alert": { "action": "allowed", "signature_id": 4, "rev": 1, "signature": "", "category": "Potentially Bad Traffic",`	

Tâche	Description	Compétences requises
	<pre>"severity ": 2 }</pre>	

Mettre à jour les règles et le groupe de règles du pare-feu

Tâche	Description	Compétences requises
Mettez à jour les règles du pare-feu.	1. Dans un éditeur de texte, ouvrez le fichier `custom.rules` . 2. Modifiez la première règle pour qu'elle soit similaire à la suivante. Cette règle doit être saisie sur une seule ligne du fichier. <pre>alert http any any -> any any (msg:"Watch out - Bad Stuff!!"; content:"badstuff" ; classtype:misc-activity; priority: 2; sid:3; rev:2; metadata:custom-field-2 Danger!, custom-field More Info;)</pre> Cela apporte les modificat ions suivantes à la règle : • Ajoute une chaîne msg (site Web de Suricata) qui fournit des informations textuelles sur la signature ou l'alerte. Dans l'alerte	Administrateur système AWS

Tâche	Description	Compétences requises
	générée, cela correspond à la signature. • Règle la priorité par défaut (site Web de Suricata) `misc-activity` de 3 à 2. Pour les valeurs par défaut des différents `classtypes`, consultez la section Informations supplémentaires. • Ajoute des métadonnées personnalisées (site Web de Suricata) à l'alerte. Il s'agit d'informations supplémentaires ajoutées à la signature. Il est recommandé d'utiliser des paires clé-valeur. • Modifie le rév (site Web de Suricata) de 1 à 2. Cela représente la version de la signature.	

Tâche	Description	Compétences requises

Mettez à jour le groupe de règles.	Dans le AWS CLI, exécutez les commandes suivantes . Utilisez l'ARN de votre politique de pare-feu. Ces commandes obtiennent un jeton de mise à jour et mettent à jour le groupe de règles en fonction des modifications apportées aux règles.
	`# UPDATETOKEN=(`aws network-firewall \ describe-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:123457890:stateful-rulegroup/custom \ --output text --query UpdateToken`)`
	`# aws network-firewall update-rule-group \ --rule-group-arn arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom \ --rules file://custom.rules \ --update-token $UPDATETOKEN`
	Voici un exemple de sortie.
	`{`
		Administrateur système AWS

Tâche	Description	Compétences requises
	"UpdateToken": "7536939f-6a1d-414c-96d1-bb28110996ed", "RuleGroupResponse": { "RuleGroupArn": "arn:aws:network-firewall:us-east-2:1234567890:stateful-rulegroup/custom", "RuleGroupName": "custom", "RuleGroupId": "238a8259-9eaf-48bb-90af-5e690cf8c48b", "Type": "STATEFUL", "Capacity": 10, "RuleGroupStatus": "ACTIVE", "Tags": [{ "Key": "environment", "Value": "development" }] } }	

Testez la fonctionnalité d'alerte mise à jour

Tâche	Description	Compétences requises
Générez une alerte pour les tests.	1. Connectez-vous à un poste de test dans le sous-réseau du pare-feu.	Administrateur système AWS

Tâche	Description	Compétences requises
	2. Entrez une commande qui doit générer une alerte. Par exemple, vous pouvez utiliser `curl`. `curl -A "badstuff" http://www.amazon.com -o /dev/null`	

Tâche	Description	Compétences requises
Validez l'alerte modifiée.	1. Ouvrez la CloudWatch console. 2. Accédez au groupe de journaux et au flux appropriés. 3. Vérifiez que l'événement enregistré est similaire à l'exemple suivant. L'exemple montre uniquement la partie pertinente de l'alerte. `"alert": { "action": "allowed", "signature_id": 3, "rev": 2, "signature": "Watch out - Bad Stuff!!", "category": "Misc activity", "severity": 2, "metadata": { "custom-field": [ "More Info" ], "custom-field-2": [ "Danger!" ] } }`	Administrateur système AWS

Ressources connexes

Références

- Envoyer des alertes depuis AWS Network Firewall une chaîne Slack (directivesAWS prescriptives)
- Renforcer la prévention des menaces AWS grâce à Suricata (AWS article de blog)
- Modèles de déploiement pour AWS Network Firewall (article de AWS blog)
- Méta-clés Suricata (documentation Suricata)

Tutoriels et vidéos

- AWS Network Firewall atelier

Informations supplémentaires

Voici le fichier de configuration de classification de Suricata 5.0.2. Ces classifications sont utilisées lors de la création des règles de pare-feu.

```
# config classification:shortname,short description,priority

config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1

# NEW CLASSIFICATIONS
config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
```

```
config classification: suspicious-login,An attempted login using a suspicious username
 was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
config classification: unusual-client-port-connection,A client was using an unusual
 port,2
config classification: network-scan,Detection of a Network Scan,3
config classification: denial-of-service,Detection of a Denial of Service Attack,2
config classification: non-standard-protocol,Detection of a non-standard protocol or
 event,2
config classification: protocol-command-decode,Generic Protocol Command Decode,3
config classification: web-application-activity,access to a potentially vulnerable web
 application,2
config classification: web-application-attack,Web Application Attack,1
config classification: misc-activity,Misc activity,3
config classification: misc-attack,Misc Attack,2
config classification: icmp-event,Generic ICMP event,3
config classification: inappropriate-content,Inappropriate Content was Detected,1
config classification: policy-violation,Potential Corporate Privacy Violation,1
config classification: default-login-attempt,Attempt to login by a default username and
 password,2

# Update
config classification: targeted-activity,Targeted Malicious Activity was Detected,1
config classification: exploit-kit,Exploit Kit Activity Detected,1
config classification: external-ip-check,Device Retrieving External IP Address
 Detected,2
config classification: domain-c2,Domain Observed Used for C2 Detected,1
config classification: pup-activity,Possibly Unwanted Program Detected,2
config classification: credential-theft,Successful Credential Theft Detected,1
config classification: social-engineering,Possible Social Engineering Attempted,2
config classification: coin-mining,Crypto Currency Mining Activity Detected,2
config classification: command-and-control,Malware Command and Control Activity
 Detected,1
```

Déployez des ressources dans une AWS Wavelength zone à l'aide de Terraform

Créée par Zahoor Chaudhrey (AWS) et Luca Iannario (AWS)

Récapitulatif

AWS Wavelengthvous aide à créer une infrastructure optimisée pour les applications MEC (Multi-Access Edge Computing). Les zones de longueur d'onde sont des déploiements d' AWS infrastructures qui intègrent des services de AWS calcul et de stockage dans les réseaux 5G des fournisseurs de services de communication (CSP). Le trafic des applications provenant des appareils 5G atteint les serveurs d'applications fonctionnant dans les zones de Wavelength sans quitter le réseau de télécommunications. Les éléments suivants facilitent la connectivité réseau via Wavelength :

- Clouds privés virtuels (VPCs) : ils VPCs Compte AWS peuvent être étendus pour couvrir plusieurs zones de disponibilité, y compris les zones Wavelength. Les instances Amazon Elastic Compute Cloud (Amazon EC2) et les services associés apparaissent dans le cadre de votre VPC régional. VPCs sont créés et gérés dans Amazon Virtual Private Cloud (Amazon VPC).
- Passerelle porteuse : une passerelle porteuse permet la connectivité entre le sous-réseau de la Wavelength Zone et le réseau du CSP, Internet ou Région AWS via le réseau du CSP. La passerelle du transporteur a deux objectifs. Il autorise le trafic entrant depuis un réseau CSP situé à un emplacement spécifique, et le trafic sortant vers le réseau de télécommunications et Internet.

Ce modèle et le code Terraform associé vous aident à lancer des ressources, telles que des EC2 instances Amazon, des volumes Amazon Elastic Block Store (Amazon EBS), des sous-réseaux et une passerelle de support VPCs, dans une zone Wavelength.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un environnement de développement intégré (IDE)
- Optez pour la zone de longueur d'onde cible
- AWS Command Line Interface (AWS CLI), installé et configuré
- Terraform version 1.8.4 ou ultérieure, installée (documentation Terraform)

- Terraform AWS Provider version 5.32.1 ou ultérieure, configurée (documentation Terraform)
- Git, installé (GitHub)
- Autorisations pour créer des ressources Amazon VPC, Wavelength et Amazon EC2

Limites

Tous ne sont pas Régions AWS compatibles avec Wavelength Zones. Pour plus d'informations, consultez Available Wavelength Zones dans la documentation Wavelength.

Architecture

Le schéma suivant montre comment créer un sous-réseau et des AWS ressources dans une Wavelength Zone. VPCs qui contiennent un sous-réseau dans une zone Wavelength peuvent se connecter à une passerelle porteuse. Une passerelle d'opérateur vous permet de vous connecter aux ressources suivantes :

- Appareils 4G/LTE et 5G sur le réseau de l'opérateur de télécommunications.
- Accès sans fil fixe pour certains partenaires de Wavelength Zone. Pour plus d'informations, consultez la section Accès multiple AWS Wavelength.
- Trafic sortant vers les ressources Internet publiques.

Outils

Services AWS

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.
- AWS Wavelengthétend AWS Cloud l'infrastructure aux réseaux 5G des fournisseurs de télécommunications. Cela vous permet de créer des applications qui fournissent des latences extrêmement faibles aux appareils mobiles et aux utilisateurs finaux.

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Creating AWS Wavelength Infrastructure using Terraform. Le code Terraform déploie l'infrastructure et les ressources suivantes :

- Un VPC
- Une zone de longueur d'onde
- Un sous-réseau public dans la Wavelength Zone
- Une passerelle porteuse dans la Wavelength Zone
- Une EC2 instance Amazon dans la Wavelength Zone

Bonnes pratiques

- Avant le déploiement, vérifiez que vous utilisez les dernières versions de Terraform et du. AWS CLI
- Utilisez un pipeline d'intégration et de livraison continues (CI/CD) pour déployer IaC. Pour plus d'informations, consultez Bonnes pratiques pour la gestion des fichiers Terraform State dans AWS CI/CD Pipeline on Blogs. AWS

Épopées

Fournir l'infrastructure

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Entrez la commande suivante pour cloner le référentiel Creating AWS Wavelength Infrastructure using Terraform dans votre environnement. `git clone git@github.com:aws-samples/terraform-waveleng`	DevOps ingénieur

Tâche	Description	Compétences requises
	`th-infrastructure.git`	
Mettez à jour les variables.	1. Accédez au référentiel cloné. `cd terraform-wavelength-infrastructure` 2. À l'aide de n'importe quel éditeur de texte, créez un fichier appelé terraform.tfvars dans le répertoire racine. 3. Créez les variables suivantes et entrez leurs valeurs : • `region = <enter Region name>` • `vpc_cidr = <enter CIDR block used by VPC>` • `wavelength_subnet_cidr = <enter CIDR block for the subnet in the Wavelength Zone>` • `availabilityzone_wavelength = <enter Wavelength Zone name>` 4. Enregistrez le fichier terraform.tfvars.	DevOps ingénieur, Terraform

Tâche	Description	Compétences requises
Initialisez la configuration.	Entrez la commande suivante pour initialiser le répertoire de travail. `terraform init`	DevOps ingénieur, Terraform
Prévisualisez le plan Terraform.	Entrez la commande suivante pour comparer l'état cible à l'état actuel de votre AWS environnement. Cette commande génère un aperçu des ressources qui seront configurées. `terraform plan`	DevOps ingénieur, Terraform

Tâche	Description	Compétences requises
Vérifiez et déployez.	1. Passez en revue les modifications de configuration dans le plan Terraform et confirmez que vous souhaitez implémenter ces modifications. 2. Entrez la commande suivante pour appliquer le plan et créer l'infrastructure. `terraform apply` 3. Entrez `yes` pour continuer. Terraform crée l'architecture déclarée dans les fichiers de configuration. Pour plus d'informations sur l'architecture, consultez la section Architecture cible de ce modèle.	DevOps ingénieur, Terraform

Valider et nettoyer

Tâche	Description	Compétences requises
Vérifiez le déploiement de l'infrastructure.	1. Si vous n'avez pas encore d' EC2 instance Amazon dans un sous-réseau public de votre entreprise Région AWS, créez-en une. Pour obtenir des instructions, consultez Lancer votre instance Linux ou Lancer votre instance	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	Windows. Vous allez utiliser cette instance pour tester la connectivité entre la Wavelength Zone et Région AWS la Wavelength Zone. 2. Testez la connectivité entre l'instance située dans la Région AWS Wavelengt h Zone et l'instance située dans la Wavelength Zone. Pour obtenir des instructi ons, consultez Tester la connectivité dans la documentation Wavelength.	
(Facultatif) Nettoyez l'infrast ructure.	Si vous devez supprimer toutes les ressources fournies par Terraform, procédez comme suit : 1. Entrez la commande suivante. `terraform destroy` 2. Saisissez `yes` pour confirmer.	DevOps ingénieur, Terraform

Résolution des problèmes

Problème	Solution
Connectivité aux EC2 instances Amazon dans le Région AWS.	Consultez Résoudre les problèmes de connexion à votre instance Linux ou Résoudre

Problème	Solution
	les problèmes de connexion à votre instance Windows.
Connectivité aux EC2 instances Amazon dans la Wavelength Zone.	Consultez Résoudre les problèmes de connectivité SSH ou RDP à mes EC2 instances lancées dans une zone Wavelength.
Capacité dans la zone de longueur d'onde.	Voir Quotas et considérations relatives aux zones de longueur d'onde.

Problème	Solution
Connectivité mobile ou opérateur entre le réseau de l'opérateur et le Région AWS.	1. Vérifiez que la passerelle du transporteur est opérationnelle. Procédez comme suit : a. Ouvrez la console VPC Amazon. b. Dans le volet de navigation, sélectionnez Votre VPCs. c. Sélectionnez le VPC qui contient la zone Wavelength. d. Dans le volet Détails, pour Carrier Gateway, vérifiez que la valeur est attachée. 2. Vérifiez que toutes les adresses IP élastiques associées aux instances de la Wavelength Zone sont opérationnelles. Procédez comme suit : a. Ouvrez la EC2 console Amazon. b. Dans le panneau de navigation, choisissez Instances. c. Sélectionnez l'instance dans la Wavelength Zone. d. Choisissez l'onglet Network (Réseau). e. Vérifiez qu'une adresse IP élastique est attachée à l'interface Elastic network. 3. Contactez l'équipe d'assistance du réseau de l'opérateur.

Ressources connexes

- Qu'est-ce que c'est AWS Wavelength ?
- Comment AWS Wavelength fonctionne
- Résilience dans AWS Wavelength

Migrer des enregistrements DNS en masse vers une zone hébergée privée Amazon Route 53

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Les ingénieurs réseau et les administrateurs cloud ont besoin d'un moyen simple et efficace d'ajouter des enregistrements DNS (Domain Name System) aux zones hébergées privées sur Amazon Route 53. L'utilisation d'une approche manuelle pour copier les entrées d'une feuille de calcul Microsoft Excel vers les emplacements appropriés de la console Route 53 est fastidieuse et source d'erreurs. Ce modèle décrit une approche automatisée qui réduit le temps et les efforts nécessaires pour ajouter plusieurs enregistrements. Il fournit également un ensemble d'étapes répétables pour la création de plusieurs zones hébergées.

Ce modèle utilise Amazon Simple Storage Service (Amazon S3) pour stocker les enregistrements. Pour travailler efficacement avec les données, le modèle utilise le format JSON en raison de sa simplicité et de sa capacité à prendre en charge un dictionnaire Python (type de `dict` données).

> **Note**
>
> Si vous pouvez générer un fichier de zone à partir de votre système, pensez plutôt à utiliser la fonctionnalité d'importation Route 53.

Conditions préalables et limitations

Prérequis

- Feuille de calcul Excel contenant des enregistrements de zones hébergées privées
- Connaissance des différents types d'enregistrements DNS tels que l'enregistrement A, l'enregistrement NAPTR (Name Authority Pointer) et l'enregistrement SRV (voir Types d'enregistrements DNS pris en charge)
- Connaissance du langage Python et de ses bibliothèques

Limites

- Le modèle ne fournit pas une couverture étendue pour tous les scénarios d'utilisation. Par exemple, l'appel change_resource_record_sets n'utilise pas toutes les propriétés disponibles de l'API.
- Dans la feuille de calcul Excel, la valeur de chaque ligne est supposée être unique. Plusieurs valeurs pour chaque nom de domaine complet (FQDN) devraient apparaître dans la même ligne. Si ce n'est pas le cas, vous devez modifier le code fourni dans ce modèle pour effectuer la concaténation nécessaire.
- Le modèle utilise le SDK AWS pour Python (Boto3) pour appeler directement le service Route 53. Vous pouvez améliorer le code pour utiliser un CloudFormation wrapper AWS pour les `update_stack` commandes `create_stack` and, et utiliser les valeurs JSON pour renseigner les ressources du modèle.

Architecture

Pile technologique

- Route 53 zones hébergées privées pour acheminer le trafic
- Amazon S3 pour le stockage du fichier JSON de sortie

Le flux de travail comprend les étapes suivantes, comme illustré dans le schéma précédent et décrit dans la section Epics :

1. Téléchargez une feuille de calcul Excel contenant les informations du jeu d'enregistrements dans un compartiment S3.
2. Créez et exécutez un script Python qui convertit les données Excel au format JSON.
3. Lisez les enregistrements du compartiment S3 et nettoyez les données.
4. Créez des ensembles de records dans votre zone hébergée privée.

Outils

- Route 53 — Amazon Route 53 est un service Web DNS hautement disponible et évolutif qui gère l'enregistrement des domaines, le routage DNS et la vérification de l'état de santé.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.

Épopées

Préparer les données pour l'automatisation

Tâche	Description	Compétences requises
Créez un fichier Excel pour vos dossiers.	Utilisez les enregistrements que vous avez exportés depuis votre système actuel pour créer une feuille de calcul Excel contenant les colonnes requises pour un enregistrement, telles que le nom de domaine complet (FQDN), le type d'enregistrement, le temps de vie (TTL) et la valeur. Pour les enregistrements NAPTR et SRV, la valeur est une combinaison de plusieurs propriétés. Utilisez donc la `concat` méthode d'Excel pour combiner ces propriétés. FqdnN Recor Valeur TTL e somet A 1.1.1.1 900 .exem org	Ingénieur de données, compétences Excel

Tâche	Description	Compétences requises

Vérifiez l'environnement de travail.	Dans votre IDE, créez un fichier Python pour convertir la feuille de calcul d'entrée Excel au format JSON. (Au lieu d'un IDE, vous pouvez également utiliser un SageMaker bloc-notes Amazon pour travailler avec du code Python.)
	
	Vérifiez que la version de Python que vous utilisez est la version 3.7 ou ultérieure.
	
	`python3 --version`
	
	Installez le package pandas.
	
	`pip3 install pandas --user`
		AWS général

Convertissez les données de la feuille de calcul Excel en JSON.	Créez un fichier Python contenant le code suivant pour convertir Excel en JSON.
	
	`import pandas as pd`
	`data=pd.read_excel('./Book1.xls')`
	`data.to_json(path_or_buf='my.json', orient='records')`
	
	où `Book1` est le nom de la feuille de calcul Excel et `my.json` le nom du fichier JSON de sortie.
		Ingénieur de données, compétences en Python

Tâche	Description	Compétences requises
Téléchargez le fichier JSON dans un compartiment S3.	Chargez le fichier `my.json` dans un compartiment S3. Pour plus d'informations, consultez la section Création d'un compartiment dans la documentation Amazon S3.	Développeur d'applications

Insérer des enregistrements

Tâche	Description	Compétences requises

Créez une zone hébergée privée.	Utilisez l'API create_hosted_zone et l'exemple de code Python suivant pour créer une zone hébergée privée. Remplacez les paramètres `hostedZoneName` `vpcRegion` , et `vpcId` par vos propres valeurs.
	`import boto3`
	`import random`
	`hostedZoneName ="xxx"`
	`vpcRegion = "us-east-1"`
	`vpcId="vpc-xxxx"`
	`route53_client = boto3.client('route53')`
	`response = route53_client.create_hosted_zone(`
	`Name= hostedZoneName,`
	`VPC={`
		Architecte cloud, administrateur réseau, compétences en Python

Tâche	Description	Compétences requises

	<pre>'VPCRegion': vpcRegion,
	'VPCId': vpcId
	},
	CallerReference=str(random.random()*100000),
	HostedZoneConfig={
	'Comment': : "private hosted zone created by automation",
	'PrivateZone': True
	}
	)
	print(response)</pre>
	Vous pouvez également utiliser un outil d'infrastructure en tant que code (IaC) tel qu'AWS CloudFormation pour remplacer ces étapes par un modèle qui crée une pile dotée des ressources et propriétés appropriées.	

Tâche	Description	Compétences requises
Récupérez les détails sous forme de dictionnaire depuis Amazon S3.	Utilisez le code suivant pour lire le contenu du compartiment S3 et obtenir les valeurs JSON sous forme de dictionnaire Python. `fileobj = s3_client.get_object( Bucket=bucket_name, Key='my.json' ) filedata = fileobj['Body'].read() contents = filedata.decode('utf-8') json_content=json.loads(contents) print(json_content)` où `json_content` contient le dictionnaire Python.	Développeur d'applications, compétences en Python

Tâche	Description	Compétences requises
Nettoyez les valeurs de données pour les espaces et les caractères Unicode.	Par mesure de sécurité afin de garantir l'exactitude des données, utilisez le code suivant pour effectuer une opération de découpage sur les valeurs saisies. `json_content` Ce code supprime les espaces au début et à la fin de chaque chaîne. Il utilise également la `replace` méthode pour supprimer les espaces durs (non cassants) (les `\xa0` caractères). `for item in json_cont ent: fqn_name = unicodeda ta.normalize("NFKD ",item["FqdnName"] .replace("u'", "'").replace('\xa0', '').strip()) rec_type = item["Rec ordType"].replace( '\xa0', '').strip() res_rec = { 'Value': item["Val ue"].replace('\xa0', '').strip() }`	Développeur d'applications, compétences en Python

Tâche	Description	Compétences requises
Insérez des enregistrements.	Utilisez le code suivant dans le cadre de la `for` boucle précédente. `change_response = route53_client.change_resource_record_sets( HostedZoneId="xxxxxxxx", ChangeBatch={ 'Comment': 'Created by automation', 'Changes': [ { 'Action': 'UPSERT', 'ResourceRecordSet': { 'Name': fqn_name, 'Type': rec_type, 'TTL': item["TTL"], 'ResourceRecords': res_rec } } ] } )`	Développeur d'applications, compétences en Python

Tâche	Description	Compétences requises
	Où se xxxxxxx trouve l'identifiant de la zone hébergée dès la première étape de cette épopée.	

Ressources connexes

Références

- Création d'enregistrements en important un fichier de zone (documentation Amazon Route 53)
- méthode create_hosted_zone (documentation Boto3)
- méthode change_resource_record_sets (documentation Boto3)

Tutoriels et vidéos

- Le didacticiel Python (documentation Python)
- Conception du DNS à l'aide d'Amazon Route 53 (YouTube vidéo, AWS Online Tech Talks)

Modifiez les en-têtes HTTP lors de la migration de F5 vers un Application Load Balancer sur AWS

Créée par Sachin Trivedi (AWS)

Récapitulatif

Lorsque vous migrez une application qui utilise un équilibreur de charge F5 vers Amazon Web Services (AWS) et que vous souhaitez utiliser un équilibreur de charge d'application sur AWS, la migration des règles F5 pour les modifications d'en-tête est un problème courant. Un Application Load Balancer ne prend pas en charge les modifications d'en-têtes, mais vous pouvez utiliser Amazon CloudFront comme réseau de diffusion de contenu (CDN) et Lambda @Edge pour modifier les en-têtes.

Ce modèle décrit les intégrations requises et fournit un exemple de code pour la modification des en-têtes à l'aide d'AWS CloudFront et Lambda @Edge.

Conditions préalables et limitations

Prérequis

- Application sur site qui utilise un équilibreur de charge F5 avec une configuration qui remplace la valeur d'en-tête HTTP en utilisant. `if, else` Pour plus d'informations sur cette configuration, consultez HTTP : :header dans la documentation du produit F5.

Limites

- Ce modèle s'applique à la personnalisation de l'en-tête de l'équilibreur de charge F5. Pour les autres équilibreurs de charge tiers, consultez la documentation de l'équilibreur de charge pour obtenir des informations d'assistance.
- Les fonctions Lambda que vous utilisez pour Lambda @Edge doivent se trouver dans la région USA Est (Virginie du Nord).

Architecture

Le schéma suivant montre l'architecture d'AWS, y compris le flux d'intégration entre le CDN et les autres composants AWS.

Outils

Services AWS

- Application Load Balancer – Un Application Load Balancer est un service d'équilibrage de charge entièrement géré par AWS qui fonctionne au niveau de la septième couche du modèle d'interconnexion des systèmes ouverts (OSI). Il équilibre le trafic entre plusieurs cibles et prend en charge les demandes de routage avancées basées sur les en-têtes et les méthodes HTTP, les chaînes de requête et le routage basé sur l'hôte ou le chemin.
- Amazon CloudFront — Amazon CloudFront est un service Web qui accélère la distribution de votre contenu Web statique et dynamique, tel que les fichiers .html, .css, .js et les fichiers image, à vos utilisateurs. CloudFront diffuse votre contenu via un réseau mondial de centres de données appelés emplacements périphériques pour réduire la latence et améliorer les performances.
- Lambda @Edge – Lambda @Edge est une extension d'AWS Lambda qui vous permet d'exécuter des fonctions pour personnaliser le contenu diffusé. CloudFront Vous pouvez créer des fonctions dans la région USA Est (Virginie du Nord), puis associer la fonction à une CloudFront distribution pour répliquer automatiquement votre code dans le monde entier, sans provisionner ni gérer de serveurs. Cela réduit le temps de latence et améliore l'expérience utilisateur.

Code

L'exemple de code suivant fournit un modèle pour modifier les en-têtes de CloudFront réponse. Suivez les instructions de la section Epics pour déployer le code.

```
exports.handler = async (event, context) => {
    const response = event.Records[0].cf.response;
    const headers = response.headers;


    const headerNameSrc = 'content-security-policy';
    const headerNameValue = '*.xyz.com';


    if (headers[headerNameSrc.toLowerCase()]) {
        headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
```

```
        }];
        console.log(`Response header "${headerNameSrc}" was set to ` +
                    `"${headers[headerNameSrc.toLowerCase()][0].value}"`);
    }
    else {
            headers[headerNameSrc.toLowerCase()] = [{
            key: headerNameSrc,
            value: headerNameValue,
            }];
    }
    return response;
};
```

Épopées

Création d'une distribution CDN

Tâche	Description	Compétences requises
Créez une distribution CloudFront Web.	Au cours de cette étape, vous créez une CloudFront distribution indiquant d' CloudFront où vous souhaitez que le contenu soit diffusé, ainsi que les détails sur le suivi et la gestion de la diffusion du contenu. Pour créer une distribution à l'aide de la console, connectez-vous à l'AWS Management Console, ouvrez la CloudFront console, puis suivez les étapes décrites dans la CloudFront documentation.	Administrateur du cloud

Création et déploiement de la fonction Lambda @Edge

Tâche	Description	Compétences requises
Créez et déployez une fonction Lambda @Edge.	Vous pouvez créer une fonction Lambda @Edge en utilisant un plan pour modifier CloudFront les en-têtes de réponse. (D'autres BluePrints sont disponibles pour différents cas d'utilisation ; pour plus d'informations, consultez les exemples de fonctions Lambda @Edge dans CloudFront la documentation.) Pour créer une fonction Lambda @Edge : 1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Lambda à l'adresse. https://console.aws.amazon.com/lambda/ 2. Assurez-vous que vous vous trouvez dans la région USA Est (Virginie du Nord). CloudFront les plans ne sont disponibles que dans cette région. 3. Choisissez Créer une fonction. 4. Choisissez Utiliser un plan, puis saisissez	Administrateur AWS

Tâche	Description	Compétences requises
	cloudfront dans le champ de recherche Blueprints. 5. Choisissez le cloudfron t-modify-response-headerplan, puis sélection nez Configurer. 6. Sur la page Informations de base, entrez les informati ons suivantes : a. Indiquez un nom de fonction. b. Dans la liste déroulant e Execution role (Rôle d'exécution), choisisse z Create a new role from AWS policy templates (Créer un rôle à partir de modèles de stratégie AWS). c. Associez le nom de rôle AWS Identity and Access Management (IAM) requis. 7. Choisissez Créer une fonction. 8. Dans la section Designer de la page, choisissez le nom de votre fonction. 9. Dans la section Code de fonction, remplacez le code du modèle par l'exemple de code fourni précédemm	

Tâche	Description	Compétences requises
	ent dans ce modèle, dans la section Code. 10. Dans l'exemple de code, remplacez-le `xyz.com` par votre nom de domaine. 11. Choisissez Enregistrer.	
Déployez la fonction Lambda @Edge.	Suivez les instructions de l'étape 4 du didacticiel : Création d'une fonction Lambda @Edge simple dans la CloudFront documentation Amazon pour configurer le CloudFront déclencheur et déployer la fonction.	Administrateur AWS

Ressources connexes

CloudFront documentation

- Comportement des demandes et des réponses pour les origines personnalisées
- Utilisation des distributions
- Exemples de fonctions Lambda @Edge
- Personnalisation à la périphérie avec Lambda @Edge
- Tutoriel : Création d'une fonction Lambda @Edge simple

Accédez en privé à un point de terminaison de service AWS central à partir de plusieurs VPCs

Créée par Martin Guenthner (AWS) et Samuel Gordon (AWS)

Récapitulatif

Les exigences de sécurité et de conformité de votre environnement peuvent spécifier que le trafic vers les services ou les points de terminaison Amazon Web Services (AWS) ne doit pas traverser l'Internet public. Ce modèle est une solution conçue pour une hub-and-spoketopologie dans laquelle un VPC central est connecté à plusieurs rayons distribués. VPCs Dans cette solution, vous utilisez AWS PrivateLink pour créer un point de terminaison VPC d'interface pour le service AWS dans le compte du hub. Vous utilisez ensuite des passerelles de transit et une règle de système de noms de domaine (DNS) distribué pour résoudre les demandes adressées à l'adresse IP privée du point de terminaison, sur le réseau connecté VPCs.

Ce modèle décrit comment utiliser AWS Transit Gateway, un point de terminaison Amazon Route 53 Resolver entrant et une règle de transfert Route 53 partagée afin de résoudre les requêtes DNS provenant des ressources connectées. VPCs Vous créez le point de terminaison, la passerelle de transit, le résolveur et la règle de transfert dans le compte du hub. Vous utilisez ensuite AWS Resource Access Manager (AWS RAM) pour partager la passerelle de transit et la règle de transfert avec le rayon VPCs. Les CloudFormation modèles AWS fournis vous aident à déployer et à configurer les ressources dans le hub VPC and Spoke. VPCs

Conditions préalables et limitations

Prérequis

- Un compte hub et un ou plusieurs comptes parlés, gérés dans la même organisation dans AWS Organizations. Pour plus d'informations, consultez la section Création et gestion d'une organisation.
- AWS Resource Access Manager (AWS RAM) est configuré en tant que service fiable dans AWS Organizations. Pour plus d'informations, consultez la section Utilisation d'AWS Organizations avec d'autres services AWS.
- La résolution DNS doit être activée dans le hub and spoke VPCs. Pour plus d'informations, consultez les attributs DNS de votre VPC (documentation Amazon Virtual Private Cloud).

Limites

- Ce modèle connecte les comptes Hub et Spoke dans la même région AWS. Pour les déploiements multirégionaux, vous devez répéter ce modèle pour chaque région.
- Le service AWS doit s'intégrer en PrivateLink tant que point de terminaison VPC d'interface. Pour une liste complète, consultez les services AWS qui s'intègrent à AWS PrivateLink (PrivateLink documentation).
- L'affinité des zones de disponibilité n'est pas garantie. Par exemple, les requêtes provenant de la zone de disponibilité A peuvent répondre par une adresse IP provenant de la zone de disponibilité B.
- L'interface Elastic network associée au point de terminaison VPC est limitée à 10 000 requêtes par seconde.

Architecture

Pile technologique cible

- Un VPC du hub dans le compte AWS du hub
- Un ou plusieurs locuteurs VPCs dans un compte AWS parlé
- Un ou plusieurs points de terminaison VPC d'interface dans le compte du hub
- Résolveurs Route 53 entrants et sortants dans le compte du hub
- Une règle de transfert Route 53 Resolver déployée dans le compte hub et partagée avec le compte Spoke
- Une passerelle de transit déployée dans le compte hub et partagée avec le compte Spoke
- AWS Transit Gateway reliant le hub à Spoke VPCs

Architecture cible

L'image suivante montre un exemple d'architecture pour cette solution. Dans cette architecture, la règle de transfert Route 53 Resolver dans le compte du hub a la relation suivante avec les autres composants de l'architecture :

1. La règle de transfert est partagée avec le VPC Spoke à l'aide de la RAM AWS.
2. La règle de transfert est associée au résolveur sortant dans le VPC du hub.
3. La règle de transfert cible le résolveur entrant dans le VPC du hub.

L'image suivante montre le flux de trafic dans l'exemple d'architecture :

1. Une ressource, telle qu'une instance Amazon Elastic Compute Cloud (Amazon EC2), dans le VPC en étoile envoie une requête DNS à. `<service>.<region>.amazonaws.com` La demande est reçue par le résolveur DNS Amazon Spoke.
2. La règle de transfert Route 53, partagée depuis le compte du hub et associée au VPC en étoile, intercepte la demande.
3. Dans le VPC du hub, le résolveur sortant utilise la règle de transfert pour transférer la demande au résolveur entrant.
4. Le résolveur entrant utilise le résolveur DNS Amazon VPC hub pour convertir l'adresse IP en adresse IP privée d'un point `<service>.<region>.amazonaws.com` de terminaison VPC. Si aucun point de terminaison VPC n'est présent, il est résolu vers l'adresse IP publique.

Outils

Outils et services AWS

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les faire rapidement évoluer vers le haut ou vers le bas.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Resource Access Manager (AWS RAM) vous aide à partager vos ressources en toute sécurité entre les comptes AWS afin de réduire les frais opérationnels et de garantir visibilité et auditabilité.
- Amazon Route 53 est un service web de système de noms de domaine (DNS) hautement disponible et évolutif.
- AWS Systems Manager vous aide à gérer vos applications et votre infrastructure exécutées dans le cloud AWS. Il simplifie la gestion des applications et des ressources, réduit le délai de détection

et de résolution des problèmes opérationnels et vous aide à gérer vos ressources AWS en toute sécurité à grande échelle.

- AWS Transit Gateway est un hub central qui connecte VPCs les réseaux sur site.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Autres outils et services

- nslookup est un outil de ligne de commande utilisé pour interroger les enregistrements DNS. Dans ce modèle, vous utilisez cet outil pour tester la solution.

Référentiel de code

Le code de ce modèle est disponible sur GitHub, dans le vpc-endpoint-sharingréférentiel. Ce modèle fournit deux CloudFormation modèles AWS :

- Un modèle pour déployer les ressources suivantes dans le compte du hub :
  - `rSecurityGroupEndpoints`— Le groupe de sécurité qui contrôle l'accès au point de terminaison du VPC.
  - `rSecurityGroupResolvers`— Le groupe de sécurité qui contrôle l'accès au résolveur Route 53.
  - `rKMSEndpoint`, `rSSMMessagesEndpointrSSMEndpoint`, et `rEC2MessagesEndpoint` — Exemple de points de terminaison VPC d'interface dans le compte du hub. Personnalisez ces points de terminaison en fonction de votre cas d'utilisation.
  - `rInboundResolver`— Un résolveur Route 53 qui résout les requêtes DNS adressées au hub Amazon DNS Resolver.
  - `rOutboundResolver`— Un résolveur de Route 53 sortant qui transmet les requêtes au résolveur entrant.
  - `rAWSApiResolverRule`— La règle de transfert Route 53 Resolver qui est partagée avec tous les intervenants. VPCs
  - `rRamShareAWSResolverRule`— Le partage de RAM AWS qui permet au rayon VPCs d'utiliser la règle `rAWSApiResolverRule` de transfert.
  - * `rVPC` — Le VPC du hub, utilisé pour modéliser les services partagés.

  - * `rSubnet1` — Un sous-réseau privé utilisé pour héberger les ressources du hub.
  - * `rRouteTable1` — La table de routage pour le VPC du hub.
  - * `rRouteTableAssociation1` — Pour la table de `rRouteTable1` routage dans le VPC du hub, l'association pour le sous-réseau privé.
  - * `rRouteSpoke` — L'itinéraire entre le VPC hub et le VPC en étoile.
  - * `rTgw` — La passerelle de transit partagée avec tous les intervenants VPCs.
  - * `rTgwAttach` — La pièce jointe qui permet au VPC du hub d'acheminer le trafic vers la passerelle de `rTgw` transit.
  - * `rTgwShare` — Le partage de RAM AWS qui permet aux comptes Spoke d'utiliser la passerelle de `rTgw` transit.
- Un modèle pour déployer les ressources suivantes dans les comptes Spoke :
  - `rAWSApiResolverRuleAssociation`— Une association qui permet au VPC Spoke d'utiliser la règle de transfert partagée dans le compte du hub.
  - * `rVPC` — Le VPC à rayons.
  - * `rSubnet1, rSubnet2, rSubnet3` — Un sous-réseau pour chaque zone de disponibilité, utilisé pour héberger les ressources privées en étoile.
  - * `rTgwAttach` — La pièce jointe qui permet au VPC en étoile d'acheminer le trafic vers la passerelle de `rTgw` transit.
  - * `rRouteTable1` — La table de routage pour le VPC en rayons.
  - * `rRouteEndpoints` — L'itinéraire entre les ressources du VPC en étoile et la passerelle de transit.
  - * `rRouteTableAssociation1/2/3` — Pour la table de `rRouteTable1` routage dans le VPC en étoile, les associations pour les sous-réseaux privés.
  - * `rInstanceRole` — Le rôle IAM utilisé pour tester la solution.
  - * `rInstancePolicy` — La politique IAM utilisée pour tester la solution.
  - * `rInstanceSg` — Le groupe de sécurité utilisé pour tester la solution.
  - * `rInstanceProfile` — Le profil d'instance IAM utilisé pour tester la solution.
  - * `rInstance` — Une EC2 instance préconfigurée pour un accès via AWS Systems Manager. Utilisez cette instance pour tester la solution.

* Ces ressources prennent en charge l'architecture d'exemple et peuvent ne pas être nécessaires lors de la mise en œuvre de ce modèle dans une zone d'atterrissage existante.

Épopées

Préparez les CloudFormation modèles

Tâche	Description	Compétences requises
Clonez le référentiel de code.	1. Dans une interface de ligne de commande, remplacez votre répertoire de travail par l'emplacement où vous souhaitez stocker les fichiers d'exemple. 2. Entrez la commande suivante : `git clone https://github.com/aws-samples/vpc-endpoint-sharing.git`	Administrateur réseau, architecte cloud
Modifiez les modèles.	1. Dans le référentiel cloné, ouvrez les fichiers hub.yml et spoke.yml. 2. Passez en revue les ressources créées par ces modèles et ajustez-les en fonction des besoins de votre environnement. Pour une liste complète, consultez la section Référentiel de code dans Outils. Si vos comptes disposent déjà de certaines de ces ressources, supprimez-les du CloudFormation modèle. Pour plus d'informations,	Administrateur réseau, architecte cloud

Tâche	Description	Compétences requises
	consultez la section Utilisation des modèles (CloudFormation documentation). 3. Enregistrez et fermez les fichiers hub.yml et spoke.yml.	

Déployez les ressources dans les comptes cibles

Tâche	Description	Compétences requises
Déployez les ressources du hub.	À l'aide du modèle hub.yml, créez une pile. CloudFormation Lorsque vous y êtes invité, fournissez des valeurs pour les paramètres du modèle. Pour plus d'informations, consultez Création d'une pile (CloudFormation documentation).	Architecte cloud, administrateur réseau
Déployez les ressources en rayons.	À l'aide du modèle spoke.yml, créez une pile. CloudFormation Lorsque vous y êtes invité, fournissez des valeurs pour les paramètres du modèle. Pour plus d'informations, consultez Création d'une pile (CloudFormation documentation).	Architecte cloud, administrateur réseau

Tester la solution

Tâche	Description	Compétences requises
Testez les requêtes DNS privées sur le service AWS.	1. Connectez-vous à l'`rInstance` EC2 instance à l'aide du gestionnaire de session, une fonctionnalité d'AWS Systems Manager. Pour plus d'informations, consultez Connect to your Linux instance using Session Manager (EC2 documentation Amazon). 2. Pour un service AWS doté d'un point de terminaison VPC dans le compte du hub, utilisez `nslookup` pour confirmer que les adresses IP privées du résolveur Route 53 entrant sont renvoyées. Voici un exemple d'utilisation `nslookup` pour accéder à un point de terminaison Amazon Systems Manager. `nslookup ssm.<region>.amazonaws.com` 3. Dans l'interface de ligne de commande AWS (AWS CLI), entrez une commande qui peut vous aider à	Administrateur réseau

Tâche	Description	Compétences requises
	confirmer que les modifications n'ont pas affecté les fonctionnalités du service. Pour obtenir la liste des commandes, consultez le manuel de référence des commandes de l'AWS CLI. Par exemple, la commande suivante doit renvoyer une liste de documents Amazon Systems Manager. `aws ssm list-documents`	

Tâche	Description	Compétences requises

Testez les requêtes DNS publiques adressées à un service AWS.	1. Pour un service AWS qui ne possède pas de point de terminaison VPC dans le compte du hub, utilisez `nslookup` pour confirmer que les adresses IP publiques sont renvoyées. Voici un exemple d'utilisation `nslookup` pour atteindre un point de terminaison Amazon Simple Notification Service (Amazon SNS).
	`nslookup sns.<region>.amazonaws.com`
	2. Dans la CLI AWS, entrez une commande qui peut vous aider à confirmer que les modifications n'ont pas affecté les fonctionnalités du service. Pour obtenir la liste des commandes , consultez le manuel de référence des commandes de l'AWS CLI.
	Par exemple, si des sujets Amazon SNS sont présents dans le compte du hub, la commande suivante doit renvoyer une liste de sujets.
	`aws sns list-topics`
		Administrateur réseau

Ressources connexes

- Création d'une infrastructure réseau AWS multi-VPC évolutive et sécurisée (livre blanc AWS)
- Utilisation de ressources partagées (documentation AWS RAM)
- Utilisation des passerelles de transit (documentation AWS Transit Gateway)

Créez un rapport sur les résultats de l'analyseur d'accès réseau pour l'accès Internet entrant en plusieurs Comptes AWS

Créée par Mike Virgilio (AWS)

Récapitulatif

L'accès Internet entrant involontaire aux AWS ressources peut présenter des risques pour le périmètre de données d'une entreprise. Network Access Analyzer est une fonctionnalité d'Amazon Virtual Private Cloud (Amazon VPC) qui vous aide à identifier les accès réseau involontaires à vos ressources sur Amazon Web Services ().AWS Vous pouvez utiliser Network Access Analyzer pour spécifier vos exigences d'accès au réseau et pour identifier les chemins réseau potentiels qui ne répondent pas à vos exigences spécifiées. Vous pouvez utiliser Network Access Analyzer pour effectuer les opérations suivantes :

1. Identifiez les AWS ressources accessibles sur Internet via des passerelles Internet.
2. Vérifiez que vos clouds privés virtuels (VPCs) sont correctement segmentés, par exemple en isolant les environnements de production et de développement et en séparant les charges de travail transactionnelles.

Network Access Analyzer analyse les conditions d' end-to-endaccessibilité du réseau et ne se limite pas à un seul composant. Pour déterminer si une ressource est accessible à Internet, Network Access Analyzer évalue la passerelle Internet, les tables de routage VPC, les listes de contrôle d'accès réseau (ACLs), les adresses IP publiques sur les interfaces réseau élastiques et les groupes de sécurité. Si l'un de ces composants empêche l'accès à Internet, Network Access Analyzer ne génère aucun résultat. Par exemple, si une instance Amazon Elastic Compute Cloud (Amazon EC2) possède un groupe de sécurité ouvert qui autorise le trafic en provenance `0/0` mais que l'instance se trouve dans un sous-réseau privé qui n'est pas routable depuis une passerelle Internet, Network Access Analyzer ne générera aucun résultat. Cela permet d'obtenir des résultats très fidèles afin que vous puissiez identifier les ressources réellement accessibles depuis Internet.

Lorsque vous exécutez Network Access Analyzer, vous utilisez les étendues d'accès réseau pour définir vos exigences en matière d'accès au réseau. Cette solution identifie les chemins réseau entre une passerelle Internet et une interface réseau élastique. Dans ce modèle, vous déployez la solution de manière centralisée Compte AWS au sein de votre organisation, gérée par AWS Organizations, et elle analyse tous les comptes de l'organisation Région AWS, quel qu'il soit.

Cette solution a été conçue avec les éléments suivants à l'esprit :

- Les AWS CloudFormation modèles réduisent l'effort requis pour déployer les AWS ressources selon ce modèle.
- Vous pouvez ajuster les paramètres des CloudFormation modèles et du script naa-script.sh au moment du déploiement afin de les personnaliser en fonction de votre environnement.
- Les scripts Bash provisionnent et analysent automatiquement les étendues d'accès réseau pour plusieurs comptes, en parallèle.
- Un script Python traite les résultats, extrait les données, puis consolide les résultats. Vous pouvez choisir de consulter le rapport consolidé des résultats de l'analyseur d'accès réseau au format CSV ou au AWS Security Hub format. Un exemple de rapport CSV est disponible dans la section Informations supplémentaires de ce modèle.
- Vous pouvez corriger les résultats ou les exclure des analyses futures en les ajoutant au fichier naa-exclusions.csv.

Conditions préalables et limitations

Prérequis

- Et Compte AWS pour héberger des services et outils de sécurité, gérés en tant que compte membre d'une organisation dans AWS Organizations. Dans ce modèle, ce compte est appelé compte de sécurité.
- Dans le compte de sécurité, vous devez disposer d'un sous-réseau privé avec accès Internet sortant. Pour obtenir des instructions, consultez la section Créer un sous-réseau dans la documentation Amazon VPC. Vous pouvez établir un accès à Internet à l'aide d'une passerelle NAT ou d'un point de terminaison VPC d'interface.
- Accès au compte AWS Organizations de gestion ou à un compte doté d'autorisations d'administrateur déléguées pour CloudFormation. Pour obtenir des instructions, voir Enregistrer un administrateur délégué dans la CloudFormation documentation.
- Activez un accès fiable entre AWS Organizations et CloudFormation. Pour obtenir des instructions, consultez la section Activer l'accès sécurisé avec AWS Organizations dans la CloudFormation documentation.
- Si vous téléchargez les résultats sur Security Hub, Security Hub doit être activé sur le compte et sur l' Région AWS endroit où l' EC2 instance Amazon est mise en service. Pour plus d'informations, consultez la section Configuration AWS Security Hub.

Limites

- Les chemins réseau entre comptes ne sont actuellement pas analysés en raison des limites de la fonctionnalité Network Access Analyzer.
- La cible Comptes AWS doit être gérée en tant qu'organisation dans AWS Organizations. Si vous ne l'utilisez pas AWS Organizations, vous pouvez mettre à jour le CloudFormation modèle naa-execrole.yaml et le script naa-script.sh pour votre environnement. Au lieu de cela, vous fournissez une liste Compte AWS IDs des régions dans lesquelles vous souhaitez exécuter le script.
- Le CloudFormation modèle est conçu pour déployer l' EC2 instance Amazon dans un sous-réseau privé doté d'un accès Internet sortant. L' AWS Systems Manager agent (agent SSM) a besoin d'un accès sortant pour atteindre le point de terminaison du service Systems Manager, et vous avez besoin d'un accès sortant pour cloner le référentiel de code et installer les dépendances. Si vous souhaitez utiliser un sous-réseau public, vous devez modifier le modèle naa-resources.yaml pour associer une adresse IP élastique à l'instance Amazon. EC2

Architecture

Architecture cible

Option 1 : accéder aux résultats dans un compartiment Amazon S3

Le schéma montre le processus suivant :

1. Si vous exécutez la solution manuellement, l'utilisateur s'authentifie auprès de l' EC2 instance Amazon à l'aide du gestionnaire de session, puis exécute le script naa-script.sh. Ce script shell exécute les étapes 2 à 7.

   Si vous exécutez automatiquement la solution, le script naa-script.sh démarre automatiquement selon le calendrier que vous avez défini dans l'expression cron. Ce script shell exécute les étapes 2 à 7. Pour plus d'informations, voir Automatisation et mise à l'échelle à la fin de cette section.
2. L' EC2 instance Amazon télécharge le dernier fichier naa-exception.csv depuis le compartiment Amazon S3. Ce fichier est utilisé ultérieurement dans le processus lorsque le script Python traite les exclusions.
3. L' EC2 instance Amazon assume le rôle `NAAEC2Role` AWS Identity and Access Management (IAM), qui accorde les autorisations d'accès au compartiment Amazon S3 et d'assumer les rôles `NAAExecRole` IAM dans les autres comptes de l'organisation.
4. L' EC2 instance Amazon assume le rôle `NAAExecRole` IAM dans le compte de gestion de l'organisation et génère une liste des comptes de l'organisation.

5. L' EC2 instance Amazon assume le rôle `NAAExecRole` IAM dans les comptes membres de l'organisation (appelés comptes de charge de travail dans le schéma d'architecture) et effectue une évaluation de la sécurité de chaque compte. Les résultats sont stockés sous forme de fichiers JSON sur l' EC2 instance Amazon.
6. L' EC2 instance Amazon utilise un script Python pour traiter les fichiers JSON, extraire les champs de données et créer un rapport CSV.
7. L' EC2 instance Amazon télécharge le fichier CSV dans le compartiment Amazon S3.
8. Une EventBridge règle Amazon détecte le téléchargement du fichier et utilise une rubrique Amazon SNS pour envoyer un e-mail informant l'utilisateur que le rapport est complet.
9. L'utilisateur télécharge le fichier CSV depuis le compartiment Amazon S3. L'utilisateur importe les résultats dans le modèle Excel et les examine.

Option 2 : Accédez aux résultats dans AWS Security Hub

Le schéma montre le processus suivant :

1. Si vous exécutez la solution manuellement, l'utilisateur s'authentifie auprès de l' EC2 instance Amazon à l'aide du gestionnaire de session, puis exécute le script naa-script.sh. Ce script shell exécute les étapes 2 à 7.

   Si vous exécutez automatiquement la solution, le script naa-script.sh démarre automatiquement selon le calendrier que vous avez défini dans l'expression cron. Ce script shell exécute les étapes 2 à 7. Pour plus d'informations, voir Automatisation et mise à l'échelle à la fin de cette section.
2. L' EC2 instance Amazon télécharge le dernier fichier naa-exception.csv depuis le compartiment Amazon S3. Ce fichier est utilisé ultérieurement dans le processus lorsque le script Python traite les exclusions.
3. L' EC2 instance Amazon assume le rôle `NAAEC2Role` IAM, qui accorde les autorisations d'accès au compartiment Amazon S3 et d'assumer les rôles `NAAExecRole` IAM dans les autres comptes de l'organisation.
4. L' EC2 instance Amazon assume le rôle `NAAExecRole` IAM dans le compte de gestion de l'organisation et génère une liste des comptes de l'organisation.
5. L' EC2 instance Amazon assume le rôle `NAAExecRole` IAM dans les comptes membres de l'organisation (appelés comptes de charge de travail dans le schéma d'architecture) et effectue une évaluation de la sécurité de chaque compte. Les résultats sont stockés sous forme de fichiers JSON sur l' EC2 instance Amazon.

6. L' EC2 instance Amazon utilise un script Python pour traiter les fichiers JSON et extraire les champs de données à importer dans Security Hub.
7. L' EC2 instance Amazon importe les résultats de l'analyseur d'accès réseau dans Security Hub.
8. Une EventBridge règle Amazon détecte l'importation et utilise une rubrique Amazon SNS pour envoyer un e-mail informant l'utilisateur que le processus est terminé.
9. L'utilisateur consulte les résultats dans Security Hub.

Automatisation et mise à l'échelle

Vous pouvez planifier cette solution pour exécuter le script naa-script.sh automatiquement selon un calendrier personnalisé. Pour définir un calendrier personnalisé, modifiez le paramètre dans le modèle naa-resources.yaml CloudFormation . `CronScheduleExpression` Par exemple, la valeur par défaut de `0 0 * * 0` exécute la solution tous les dimanches à minuit. Une valeur de `0 0 * 1-12 0` exécuterait la solution à minuit le premier dimanche de chaque mois. Pour plus d'informations sur l'utilisation des expressions cron, consultez les expressions Cron et rate dans la documentation de Systems Manager.

Si vous souhaitez ajuster le calendrier une fois la `NAA-Resources` pile déployée, vous pouvez modifier manuellement le calendrier cron dans`/etc/cron.d/naa-schedule`.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, des AWS Lambda fonctions, des points de terminaison d'invocation HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle. Ce modèle utilise le Gestionnaire de session, une fonctionnalité de Systems Manager.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel d'analyse multi-comptes de GitHub Network Access Analyzer. Le référentiel de code contient les fichiers suivants :

- naa-script.sh — Ce script bash est utilisé pour démarrer une analyse de plusieurs fichiers par Network Access Analyzer Comptes AWS, en parallèle. Comme défini dans le CloudFormation modèle naa-resources.yaml, ce script est automatiquement déployé dans le dossier `/usr/local/naa` de l'instance Amazon. EC2
- naa-resources.yaml — Vous utilisez ce CloudFormation modèle pour créer une pile dans le compte de sécurité de l'organisation. Ce modèle déploie toutes les ressources requises pour ce compte afin de prendre en charge la solution. Cette pile doit être déployée avant le modèle naa-execrole.yaml.

> **Note**
>
> Si cette pile est supprimée et redéployée, vous devez reconstruire l'ensemble de `NAAExecRole` piles afin de rétablir les dépendances entre comptes entre les rôles IAM.

- naa-execrole.yaml — Vous utilisez ce CloudFormation modèle pour créer un stack set qui déploie le rôle `NAAExecRole` IAM dans tous les comptes de l'organisation, y compris le compte de gestion.

- naa-processfindings.py — Le script naa-script.sh appelle automatiquement ce script Python pour traiter les sorties JSON de Network Access Analyzer, exclure toute ressource dont le fonctionnement a été vérifié dans le fichier naa-exclusions.csv, puis générer un fichier CSV contenant les résultats consolidés ou importer les résultats dans Security Hub.

Épopées

Préparation au déploiement

Tâche	Description	Compétences requises
Clonez le référentiel de code.	1. Dans une interface de ligne de commande, remplacez votre répertoire de travail par l'emplacement où vous souhaitez stocker les fichiers d'exemple. 2. Entrez la commande suivante : `git clone https://github.com/aws-samples/network-access-analyzer-multi-account-analysis.git`	AWS DevOps
Passez en revue les modèles.	1. Dans le dépôt cloné, ouvrez les fichiers naa-resources.yaml et naa-execrole.yaml. 2. Passez en revue les ressources créées par ces modèles et ajustez-les en fonction des besoins de votre environnement. Pour plus d'informations,	AWS DevOps

Tâche	Description	Compétences requises
	consultez la section Utilisation des modèles dans la CloudFormation documentation. 3. Enregistrez et fermez les fichiers naa-resources.yaml et naa-execrole.yaml.	

Créez les CloudFormation piles

Tâche	Description	Compétences requises
Provisionnez des ressources dans le compte de sécurité.	À l'aide du modèle naa-resources.yaml, vous créez une CloudFormation pile qui déploie toutes les ressources requises dans le compte de sécurité. Pour obtenir des instructions, consultez la section Création d'une pile dans la CloudFormation documentation. Notez les points suivants lors du déploiement de ce modèle : 1. Sur la page Spécifier le modèle, sélectionnez Le modèle est prêt, puis téléchargez le fichier naa-resources.yaml. 2. Sur la page Spécifier les détails de la pile, dans le champ Nom de la pile, entrez`NAA-Resources` .	AWS DevOps

Tâche	Description	Compétences requises
	3. Dans la section Paramètres, entrez les informations suivantes : • `VPCId`— Sélectionnez un VPC dans le compte. • `SubnetId`— Sélectionnez un sous-réseau privé ayant accès à Internet. **Note** Si vous sélectionnez un sous-réseau public, il est possible que l'EC2 instance Amazon ne se voie pas attribuer d'adresse IP publique car le CloudFormation modèle, par défaut, ne fournit ni n'attache d'adresse IP élastique. • `InstanceType` — Conservez le type d'instance par défaut. • `InstanceImageId` — Conservez la valeur par défaut.	

Tâche	Description	Compétences requises
	• `KeyPairName` — Si vous utilisez SSH pour l'accès, spécifiez le nom d'une paire de clés existante. • `PermittedSSHInbound` — Si vous utilisez SSH pour l'accès, spécifiez un bloc CIDR autorisé. Si vous n'utilisez pas SSH, conservez la valeur par défaut de `127.0.0.1` . • `BucketName` — La valeur par défaut est `naa-<accountID>-<region>` . Vous pouvez le modifier selon vos besoins. Si vous spécifiez une valeur personnalisée, l'ID du compte et la région sont automatiquement ajoutés à la valeur spécifiée. • `EmailAddress` — Spécifiez une adresse e-mail pour une notification Amazon SNS lorsque l'analyse est terminée. **Note** La configuration de l'abonnement Amazon	

Tâche	Description	Compétences requises
	SNS doit être confirmée avant la fin de l'analyse , sinon aucune notification ne sera envoyée. • `NAAEC2Role` — Conservez la valeur par défaut, sauf si vos conventions de dénomination exigent un nom différent pour ce rôle IAM. • `NAAExecRole` — Conserve la valeur par défaut à moins qu'un autre nom ne soit utilisé lors du déploiement du fichier naa-execrole.yaml • `Parallelism` — Spécifiez le nombre d'évaluations parallèles à effectuer. • `Regions`— Spécifiez ce que Régions AWS vous souhaitez analyser. • `ScopeNameValue` — Spécifiez le tag qui sera attribué à la portée. Cette balise est utilisée pour déterminer l'étendue de l'accès au réseau.	

Tâche	Description	Compétences requises
	• `ExclusionFile` — Spécifiez le nom du fichier d'exclusion. Les entrées de ce fichier seront exclues des résultats. • `FindingsToCSV` — Spécifiez si les résultats doivent être envoyés au format CSV. Les valeurs acceptées sont `true` et`false`. • `FindingsToSecurityHub` — Spécifiez si les résultats doivent être importés dans Security Hub. Les valeurs acceptées sont `true` et`false`. • `EmailNotificationsForSecurityHub` — Spécifiez si l'importation des résultats dans Security Hub doit générer des notifications par e-mail. Les valeurs acceptées sont `true` et`false`. • `ScheduledAnalysis` — Si vous souhaitez que la solution s'exécute automatiquement selon un calendrier`true`,	

Tâche	Description	Compétences requises
	entrez puis personnalisez le calendrier dans le `CronScheduleExpression` paramètre. Si vous ne souhaitez pas exécuter la solution automatiquement, entrez`false`. • `CronScheduleExpression` — Si vous exécutez la solution automatiquement, entrez une expression cron pour définir le calendrier. Pour plus d'informations, voir Automatisation et mise à l'échelle dans la section Architecture de ce modèle. 1. Sur la page de révision, sélectionnez Les ressources suivantes nécessitent des fonctionnalités : [AWS::IAM::Role], puis choisissez Create Stack. 2. Une fois la pile créée avec succès, dans la CloudFormation console, dans l'onglet Outputs, copiez le `NAAEC2Role` Amazon Resource Name (ARN). Vous utiliserez cet ARN ultérieurement lors du	

Tâche	Description	Compétences requises
	déploiement du fichier naa-execrole.yaml.	

Tâche	Description	Compétences requises
Attribuez le rôle IAM dans les comptes des membres.	Dans le compte AWS Organizations de gestion ou dans un compte doté d'autorisations d'administrateur déléguées pour CloudFormation, utilisez le modèle naa-execrole.yaml pour créer un stack set. CloudFormation Le stack set déploie le rôle `NAAExecRole` IAM dans tous les comptes membres de l'organisation. Pour obtenir des instructions, consultez la section Créer un ensemble de piles avec des autorisations gérées par les services dans la CloudFormation documentation. Notez les points suivants lors du déploiement de ce modèle : 1. Sous Préparer le modèle, sélectionnez Le modèle est prêt, puis téléchargez le fichier naa-execrole.yaml. 2. Sur la page Spécifier StackSet les détails, nommez l'ensemble de pilesNAA-ExecRole . 3. Dans la section Paramètres, entrez les informations suivantes : • `AuthorizedARN` — Entrez l'`NAAEC2Rol`	AWS DevOps

Tâche	Description	Compétences requises
	e ARN que vous avez copié lors de la création de la `NAA-Resources` pile. • `NAARoleName` — Conservez la valeur par défaut, `NAAExecRole` sauf si un autre nom a été utilisé lors du déploiement du fichier naa-resources.yaml. 4. Sous Autorisations, choisissez Autorisations gérées par le service. 5. Sur la page Définir les options de déploiement, sous Cibles de déploiement, choisissez Déployer vers l'organisation et acceptez toutes les valeurs par défaut. **Note** Si vous souhaitez que les piles soient déployées simultanément sur tous les comptes membres, définissez le nombre maximal de comptes simultanés et la tolérance d'échec sur une	

Tâche	Description	Compétences requises
	valeur élevée, telle que `100`. 6. Sous Régions de déploiement, choisissez la région dans laquelle l' EC2 instance Amazon pour Network Access Analyzer est déployée. Les ressources IAM étant mondiales et non régionales, le rôle IAM est déployé dans toutes les régions actives. 7. Sur la page de révision, sélectionnez Je reconnais que des ressources IAM AWS CloudFormation peuvent être créées avec des noms personnalisés, puis choisissez Créer StackSet. 8. Surveillez l'onglet Stack instances (pour le statut des comptes individuels) et l'onglet Opérations (pour le statut général) afin de déterminer quand le déploiement est terminé.	

Tâche	Description	Compétences requises
Attribuez le rôle IAM dans le compte de gestion.	À l'aide du modèle naa-execrole.yaml, vous créez une CloudFormation pile qui déploie le rôle `NAAExecRole` IAM dans le compte de gestion de l'organisation. Le stack set que vous avez créé précédemment ne déploie pas le rôle IAM dans le compte de gestion. Pour obtenir des instructions, consultez la section Création d'une pile dans la CloudFormation documentation. Notez les points suivants lors du déploiement de ce modèle : 1. Sur la page Spécifier le modèle, sélectionnez Le modèle est prêt, puis téléchargez le fichier naa-execrole.yaml. 2. Sur la page Spécifier les détails de la pile, dans le champ Nom de la pile, entrez `NAA-ExecRole` . 3. Dans la section Paramètres, entrez les informations suivantes : • `AuthorizedARN` — Entrez l'`NAAEC2Role` ARN que vous avez copié lors de la création	AWS DevOps

Tâche	Description	Compétences requises
	de la `NAA-Resources` pile. • `NAARoleName` — Conservez la valeur par défaut, `NAAExecRole` sauf si un autre nom a été utilisé lors du déploiement du fichier naa-resources.yaml. 4. Sur la page de révision, sélectionnez Les ressources suivantes nécessitent des fonctionnalités : [AWS::IAM::Role], puis choisissez Create Stack.	

Effectuez l'analyse

Tâche	Description	Compétences requises
Personnalisez le script shell.	1. Connectez-vous au compte de sécurité de l'organisation. 2. À l'aide du gestionnaire de session, connectez-vous à l'EC2 instance Amazon pour Network Access Analyzer que vous avez précédemment mise en service. Pour obtenir des instructions, voir Se connecter à votre instance Linux à l'aide du gestionnaire de session. Si vous ne parvenez pas à	AWS DevOps

Tâche	Description	Compétences requises

	vous connecter, consultez la section Dépannage de ce modèle.
	3. Entrez les commandes suivantes pour ouvrir le fichier naa-script.sh afin de le modifier :
	`sudo -i`
	`cd /usr/local/naa`
	`vi naa-script.sh`
	4. Passez en revue et modifiez les paramètres et variables ajustables de ce script en fonction des besoins de votre environnement. Pour plus d'informations sur les options de personnalisation, consultez les commentaires au début du script.
	Par exemple, au lieu d'obtenir une liste de tous les comptes membres de l'organisation à partir du compte de gestion, vous pouvez modifier le script pour spécifier le Compte AWS IDs ou Régions AWS que vous souhaitez scanner, ou vous pouvez faire référence à un fichier externe contenant ces paramètres.	

Tâche	Description	Compétences requises
	5. Enregistrez et fermez le fichier naa-script.sh.	

Tâche	Description	Compétences requises

Analysez les comptes cibles.	1. Entrez les commandes suivantes : Cela exécute le script naa-script.sh :
	
	`sudo -i`
	`cd /usr/local/naa`
	`screen`
	`./naa-script.sh`
	
	Remarques :
	• La `screen` commande permet au script de continuer à s'exécuter en cas d'expiration de la connexion ou de perte de l'accès à la console.
	• Une fois le scan lancé, vous pouvez forcer le détachement de l'écran en appuyant sur Ctrl+A D. L'écran se détache et vous pouvez fermer la connexion à l'instance pendant que l'analyse se poursuit.
	• Pour reprendre une session détachée, connectez-vous à l'instance, entrez `sudo -i` puis entrez`screen -r`.
	2. Surveillez la sortie pour détecter toute erreur afin de vous assurer que le script fonctionne correctem
		AWS DevOps

Tâche	Description	Compétences requises
	ent. Pour un exemple de sortie, consultez la section Informations supplémentaires de ce modèle. 3. Attendez que l'analyse se termine. Si vous avez configuré les notifications par e-mail, vous recevez un e-mail lorsque les résultats ont été chargés dans le compartiment Amazon S3 ou importés dans Security Hub.	
Option 1 — Récupérez les résultats depuis le compartiment Amazon S3.	1. Téléchargez le fichier CSV depuis le `naa-<accountID>-<region>` bucket. Pour obtenir des instructions, consultez la section Téléchargement d'un objet dans la documentation Amazon S3. 2. Supprimez le fichier CSV du compartiment Amazon S3. Il s'agit d'une bonne pratique en matière d'optimisation des coûts. Pour obtenir des instructions, consultez Supprimer des objets dans la documentation Amazon S3.	AWS DevOps

Tâche	Description	Compétences requises
Option 2 — Vérifiez les résultats dans Security Hub.	1. Ouvrez la console Security Hub. 2. Choisissez Findings dans le volet de navigation. 3. Passez en revue les résultats de l'analyseur d'accès réseau. Pour obtenir des instructions, consultez la section Affichage des listes de résultats et des informations détaillées dans la documentation de Security Hub. **Note** Vous pouvez rechercher des résultats en ajoutant un titre qui commence par un filtre et en saisissant `Network Access Analyzer`.	AWS DevOps

Corriger et exclure les résultats

Tâche	Description	Compétences requises
Corriger les résultats.	Corrigez tous les résultats auxquels vous souhaitez remédier. Pour plus d'informa	AWS DevOps

Tâche	Description	Compétences requises
	tions et pour connaître les meilleures pratiques relatives à la création d'un périmètre autour de vos AWS identités , de vos ressources et de vos réseaux, consultez la section Création d'un périmètre de données sur AWS (AWS livre blanc).	

Tâche	Description	Compétences requises
Excluez les ressources dont les chemins réseau ont été vérifiés.	Si Network Access Analyzer génère des résultats pour des ressources qui devraient être accessibles depuis Internet, vous pouvez ajouter ces ressources à une liste d'exclusion. La prochaine fois que Network Access Analyzer s'exécutera, il ne générera aucun résultat pour cette ressource. 1. Accédez au script naa-script.sh **`/usr/local/naa`** , puis ouvrez-le. Notez la valeur de la `S3_EXCLUSION_FILE` variable. 2. Si la valeur de la `S3_EXCLUSION_FILE` variable est`true`, téléchargez le fichier naa-exclusions.csv depuis le `naa-<accountID>-<region>` bucket. Pour obtenir des instructions, consultez la section Téléchargement d'un objet dans la documentation Amazon S3. Si la valeur de la `S3_EXCLUSION_FILE` variable est`false`, naviguez jusqu'au fichier naa-exclusions.csv, `/usr/`	AWS DevOps

Tâche	Description	Compétences requises
	`local/naa` puis ouvrez-le . **Note** Si la valeur de la `S3_EXCLUSION_FILE` variable est`false`, le script utilise une version locale du fichier d'exclusions. Si vous modifiez ultérieurement la valeur en`true`, le script remplace la version locale par le fichier du compartiment Amazon S3. 3. Dans le fichier naa-exclusions.csv, entrez les ressources que vous souhaitez exclure. Entrez une ressource par ligne et utilisez le format suivant. `<resource_id>,<secgroup_id>,<sgrule_cidr>,<sgrule_portrange>,<sgrule_protocol>` Voici un exemple de ressource.	

Tâche	Description	Compétences requises
	`eni-1111aaaaa2222bbbb,sg-3333ccccc4444dddd,0.0.0.0/0,80 to 80,tcp` 4. Enregistrez et fermez le fichier naa-exclusions.csv. 5. Si vous avez téléchargé le fichier naa-exclusions.csv depuis le compartiment Amazon S3, chargez la nouvelle version. Pour obtenir des instructions, consultez la section Chargement d'objets dans la documentation Amazon S3.	

(Facultatif) Mettez à jour le script naa-script.sh

Tâche	Description	Compétences requises
Mettez à jour le script naa-script.sh.	Si vous souhaitez mettre à jour le script naa-script.sh vers la dernière version du dépôt, procédez comme suit : 1. Connectez-vous à l' EC2 instance Amazon à l'aide du gestionnaire de session. Pour obtenir des instructions, voir Se connecter à votre instance Linux à l'aide du gestionnaire de session.	AWS DevOps

Tâche	Description	Compétences requises

	2. Entrez la commande suivante :
	`sudo -i`
	3. Accédez au répertoire des scripts naa-script.sh :
	`cd /usr/local/naa`
	4. Entrez la commande suivante pour stocker le script local afin de pouvoir fusionner les modifications personnalisées dans la version la plus récente :
	`git stash`
	5. Entrez la commande suivante pour obtenir la dernière version du script :
	`git pull`
	6. Entrez la commande suivante pour fusionner le script personnalisé avec la dernière version du script :
	`git stash pop`	

(Facultatif) Nettoyer

Tâche	Description	Compétences requises
Supprimez toutes les ressources déployées.	Vous pouvez laisser les ressources déployées dans les comptes. Si vous souhaitez déprovisionner toutes les ressources, procédez comme suit : 1. Supprimez la `NAA-ExecRole` pile provisionnée dans le compte de gestion. Pour obtenir des instructions, consultez la section Suppression d'une pile dans la CloudFormation documentation. 2. Supprimez le `NAA-ExecRole` stack set provisionné dans le compte de gestion de l'organisation ou dans le compte d'administrateur délégué. Pour obtenir des instructions, voir Supprimer un ensemble de piles dans la CloudFormation documentation. 3. Supprimez tous les objets du compartiment `naa-<accountID>-<region>` Amazon S3. Pour obtenir des instructions, consultez Supprimer des	AWS DevOps

Tâche	Description	Compétences requises
	objets dans la documentation Amazon S3. 4. Supprimez la `NAA-Resources` pile provisionnée dans le compte de sécurité. Pour obtenir des instructions, consultez la section Suppression d'une pile dans la CloudFormation documentation.	

Résolution des problèmes

Problème	Solution
Impossible de se connecter à l' EC2 instance Amazon à l'aide du gestionnaire de session.	L'agent SSM doit être capable de communiquer avec le point de terminaison Systems Manager. Procédez comme suit : 1. Vérifiez que le sous-réseau sur lequel l' EC2 instance Amazon est déployée dispose d'un accès Internet. 2. Redémarrez l' EC2 instance Amazon.
Lorsque vous déployez le stack set, la CloudFormation console vous invite à`Enable trusted access with AWS Organizations to use service-managed permissions .`	Cela indique que l'accès sécurisé n'a pas été activé entre AWS Organizations et CloudFormation. Un accès sécurisé est requis pour déployer le stack set géré par les services. Cliquez sur le bouton pour activer l'accès sécurisé. Pour plus d'informations, consultez la section Activer l'accès sécurisé dans la CloudFormation documentation.

Ressources connexes

- Nouveau — Analyseur d'accès réseau Amazon VPC (article de blog)AWS
- AWS Re:inForce 2022 - Validez les contrôles d'accès réseau efficaces le AWS (NIS202) (vidéo)
- Démo - Analyse du chemin des données d'entrée Internet à l'échelle de l'organisation à l'aide de l'analyseur d'accès réseau (vidéo)

Informations supplémentaires

Exemple de sortie de console

L'exemple suivant montre le résultat de la génération de la liste des comptes cibles et de l'analyse des comptes cibles.

```
[root@ip-10-10-43-82 naa]# ./naa-script.sh
download: s3://naa-<account ID>-us-east-1/naa-exclusions.csv to ./naa-exclusions.csv

AWS Management Account: <Management account ID>

AWS Accounts being processed...
<Account ID 1> <Account ID 2> <Account ID 3>

Assessing AWS Account: <Account ID 1>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 2>, using Role: NAAExecRole
Assessing AWS Account: <Account ID 3>, using Role: NAAExecRole
Processing account: <Account ID 1> / Region: us-east-1
Account: <Account ID 1> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 2> / Region: us-east-1
Account: <Account ID 2> / Region: us-east-1 - Detecting Network Analyzer scope...
Processing account: <Account ID 3> / Region: us-east-1
Account: <Account ID 3> / Region: us-east-1 - Detecting Network Analyzer scope...
Account: <Account ID 1> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 1> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 2> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 2> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
Account: <Account ID 3> / Region: us-east-1 - Network Access Analyzer scope detected.
Account: <Account ID 3> / Region: us-east-1 - Continuing analyses with Scope ID.
 Accounts with many resources may take up to one hour
```

Exemples de rapports CSV

Les images suivantes sont des exemples de sortie CSV.

Configuration de la résolution DNS pour les réseaux hybrides dans un environnement multi-comptes AWS

Créée par Anvesh Koganti (AWS)

Récapitulatif

Ce modèle fournit une solution complète pour configurer la résolution DNS dans les environnements de réseau hybrides qui incluent plusieurs comptes Amazon Web Services (AWS). Il permet une résolution DNS bidirectionnelle entre les réseaux locaux et l' AWS environnement via Amazon Route 53 Resolver les points de terminaison. Le modèle présente deux solutions pour permettre la résolution DNS dans une architecture centralisée multi-comptes :

- La configuration de base n'utilise pas les profils Route 53. Il permet d'optimiser les coûts pour les petits et moyens déploiements peu complexes.
- La configuration améliorée utilise les profils Route 53 pour simplifier les opérations. Il est préférable pour les déploiements DNS plus importants ou plus complexes.

> **Note**
>
> Consultez la section Limitations pour connaître les limites de service et les quotas avant la mise en œuvre. Tenez compte de facteurs tels que les frais généraux de gestion, les coûts, la complexité opérationnelle et l'expertise de l'équipe lorsque vous prenez votre décision.

Conditions préalables et limitations

Prérequis

- Un environnement AWS multi-comptes avec Amazon Virtual Private Cloud (Amazon VPC) déployé sur des comptes de services partagés et de charge de travail (de préférence configuré via AWS Control Tower en AWS suivant les meilleures pratiques en matière de structure de compte).
- Connectivité hybride existante (AWS Direct Connect ou AWS Site-to-Site VPN) entre votre réseau sur site et l' AWS environnement.
- Amazon VPC peering AWS Transit Gateway, ou AWS Cloud WAN pour la connectivité réseau de couche 3 entre les deux. VPCs (Cette connectivité est requise pour le trafic des applications.

Elle n'est pas requise pour que la résolution DNS fonctionne. La résolution DNS fonctionne indépendamment de la connectivité réseau entre les VPCs.)

- Serveurs DNS exécutés dans l'environnement sur site.

Limites

- Les points de terminaison, les règles et les profils du résolveur Route 53 sont des constructions régionales qui peuvent nécessiter une réplication multiple Régions AWS pour les organisations internationales.
- Pour une liste complète des quotas de service pour Route 53 Resolver, les zones hébergées privées et les profils, consultez la section Quotas dans la documentation Route 53.

Architecture

Pile technologique cible

- Points de terminaison sortants et entrants de Route 53
- Règles du résolveur Route 53 pour le transfert conditionnel
- AWS Resource Access Manager (AWS RAM)
- Zone hébergée privée Route 53

Architecture cible

Points de terminaison sortants et entrants

Le schéma suivant montre le flux de résolution DNS entre AWS et sur site. Il s'agit de la configuration de connectivité pour les résolutions sortantes où le domaine est hébergé sur site. Voici un aperçu général du processus impliqué dans sa mise en place. Pour plus de détails, consultez la section Epics.

1. Déployez les points de terminaison du résolveur Route 53 sortants dans le VPC Shared Services.
2. Créez des règles Route 53 Resolver (règles de transfert) dans le compte Shared Services pour les domaines hébergés sur site.
3. Partagez et associez les règles VPCs à d'autres comptes hébergeant des ressources qui ont besoin de résoudre des domaines hébergés sur site. Cela peut être fait de différentes manières en fonction de votre cas d'utilisation, comme décrit plus loin dans cette section.

Après avoir configuré la connectivité, les étapes nécessaires à la résolution des problèmes sortants sont les suivantes :

1. L'instance Amazon Elastic Compute Cloud (Amazon EC2) envoie une demande de résolution DNS `db.onprem.example.com` au résolveur Route 53 du VPC à l'adresse VPC+2.
2. Route 53 Resolver vérifie les règles du résolveur et transmet la demande au serveur DNS local en IPs utilisant le point de terminaison sortant.
3. Le point de terminaison sortant transmet la demande au DNS local. IPs Le trafic passe par la connectivité réseau hybride établie entre le VPC Shared Services et le centre de données sur site.
4. Le serveur DNS local répond au point de terminaison sortant, qui transmet ensuite la réponse au résolveur Route 53 du VPC. Le résolveur renvoie la réponse à l' EC2 instance.

Le schéma suivant montre le flux de résolution DNS entre l'environnement local et. AWS Il s'agit de la configuration de connectivité pour les résolutions entrantes sur AWS lesquelles le domaine est hébergé. Voici un aperçu général du processus impliqué dans sa mise en place. Pour plus de détails, consultez la section Epics.

1. Déployez les points de terminaison du résolveur entrants dans le VPC Shared Services.
2. Créez des zones hébergées privées dans le compte Shared Services (approche centralisée).
3. Associez les zones hébergées privées au VPC Shared Services. Partagez et associez ces zones à des comptes multiples VPCs pour la résolution VPC-to-VPC DNS. Cela peut être fait de différentes manières en fonction de votre cas d'utilisation, comme décrit plus loin dans cette section.

Après avoir configuré la connectivité, les étapes impliquées dans la résolution entrante sont les suivantes :

1. La ressource locale envoie une demande de résolution DNS `ec2.prod.aws.example.com` au serveur DNS local.
2. Le serveur DNS local transmet la demande au point de terminaison du résolveur entrant dans le VPC Shared Services via la connexion réseau hybride.
3. Le point de terminaison du résolveur entrant recherche la demande dans la zone hébergée privée associée à l'aide du résolveur VPC Route 53 et obtient l'adresse IP appropriée.

4. Ces adresses IP sont renvoyées au serveur DNS local, qui renvoie la réponse à la ressource locale.

Cette configuration permet aux ressources locales de résoudre les noms de domaine AWS privés en acheminant les requêtes via les points de terminaison entrants vers la zone hébergée privée appropriée. Dans cette architecture, les zones hébergées privées sont centralisées dans un VPC Shared Services, ce qui permet à une seule équipe de gérer le DNS de manière centralisée. Ces zones peuvent être associées à de nombreuses zones VPCs pour répondre au cas d'utilisation de la résolution VPC-to-VPC DNS. Vous pouvez également déléguer la propriété et la gestion du domaine DNS à chacun d'entre eux Compte AWS. Dans ce cas, chaque compte gère ses propres zones hébergées privées et associe chaque zone au VPC Shared Services central pour une résolution unifiée avec l'environnement sur site. Cette approche décentralisée n'entre pas dans le cadre de ce modèle. Pour plus d'informations, consultez la section Étendre la gestion du DNS sur plusieurs comptes et VPCs dans le livre blanc sur les options DNS du cloud hybride pour Amazon VPC.

Lorsque vous établissez les flux de résolution DNS fondamentaux à l'aide des points de terminaison du résolveur, vous devez déterminer comment gérer le partage et l'association des règles du résolveur et des zones hébergées privées dans votre environnement. Comptes AWS Vous pouvez aborder cette question de deux manières : par le biais d'un partage autogéré en utilisant AWS RAM pour partager les règles du résolveur et les associations directes de zones hébergées privées, comme indiqué dans la section Configuration de base, ou via les profils Route 53, comme indiqué dans la section Configuration améliorée. Le choix dépend des préférences de gestion du DNS et des exigences opérationnelles de votre organisation. Les diagrammes d'architecture suivants illustrent un environnement évolutif qui inclut plusieurs comptes VPCs différents, ce qui représente un déploiement d'entreprise typique.

Configuration de base

Dans la configuration de base, la mise en œuvre de la résolution DNS hybride dans un AWS environnement multi-comptes consiste AWS RAM à partager les règles de transfert du résolveur et les associations de zones hébergées privées afin de gérer les requêtes DNS entre les sites locaux et les ressources. AWS Cette méthode utilise des points de terminaison Route 53 Resolver centralisés dans un VPC Shared Services connecté à votre réseau local pour gérer efficacement la résolution DNS entrante et sortante.

- Pour la résolution sortante, les règles de transfert du résolveur sont créées dans le compte Shared Services, puis partagées avec d'autres utilisateurs à l'aide Comptes AWS de. AWS RAM Ce partage est limité aux comptes d'une même région. Les comptes cibles peuvent ensuite associer

ces règles à leurs propres règles VPCs et activer les ressources qu'ils contiennent VPCs pour résoudre les noms de domaine locaux.

- Pour la résolution entrante, des zones hébergées privées sont créées dans le compte Shared Services et associées au VPC Shared Services. Ces zones peuvent ensuite être associées VPCs à d'autres comptes à l'aide de l'API Route 53 ou du AWS Command Line Interface (AWS CLI). AWS SDKs Les ressources associées VPCs peuvent ensuite résoudre les enregistrements DNS définis dans les zones hébergées privées, ce qui crée une vue DNS unifiée de votre AWS environnement.

Le schéma suivant montre les flux de résolution DNS dans cette configuration de base.

Cette configuration fonctionne bien lorsque vous travaillez avec une infrastructure DNS à une échelle limitée. Cependant, cela peut devenir difficile à gérer à mesure que votre environnement se développe. La charge opérationnelle liée à la gestion de la manière dont les règles des zones hébergées privées et du résolveur sont partagées et associées VPCs individuellement augmente considérablement avec l'échelle. En outre, les quotas de service tels que la limite d'association de 300 VPC par zone hébergée privée peuvent devenir des facteurs contraignants dans les déploiements à grande échelle. La configuration améliorée permet de relever ces défis.

Configuration améliorée

Les profils Route 53 offrent une solution rationalisée pour gérer la résolution DNS dans les réseaux hybrides sur plusieurs réseaux Comptes AWS. Au lieu de gérer les zones hébergées privées et les règles du résolveur individuellement, vous pouvez regrouper les configurations DNS dans un seul conteneur qui peut être facilement partagé et appliqué à plusieurs VPCs comptes dans une région. Cette configuration maintient l'architecture centralisée du point de terminaison Resolver dans un VPC Shared Services tout en simplifiant considérablement la gestion des configurations DNS.

Le schéma suivant montre les flux de résolution DNS dans une configuration améliorée.

Les profils Route 53 vous permettent de regrouper les associations de zones hébergées privées, les règles de transfert du résolveur et les règles de pare-feu DNS dans une seule unité partageable. Vous pouvez créer des profils dans le compte Shared Services et les partager avec les comptes des membres en utilisant AWS RAM. Lorsqu'un profil est partagé et appliqué à Target VPCs, toutes les associations et configurations nécessaires sont automatiquement gérées par le service. Cela réduit considérablement les frais opérationnels liés à la gestion du DNS et offre une excellente évolutivité pour les environnements en pleine croissance.

Automatisation et mise à l'échelle

Utilisez des outils d'infrastructure en tant que code (IaC) tels que AWS CloudFormation Terraform pour provisionner et gérer automatiquement les points de terminaison, les règles, les zones hébergées privées et les profils du résolveur Route 53. Intégrez la configuration DNS à des pipelines d'intégration continue et de livraison continue (CI/CD) pour garantir la cohérence, la répétabilité et des mises à jour rapides.

Outils

Services AWS

- AWS Resource Access Manager (AWS RAM) vous permet de partager vos ressources en toute sécurité afin Comptes AWS de réduire les frais opérationnels et de garantir visibilité et auditabilité.
- Amazon Route 53 Resolverrépond de manière récursive aux requêtes DNS provenant AWS des ressources et est disponible par défaut dans tous les VPCs domaines. Vous pouvez créer des points de terminaison Resolver et des règles de transfert conditionnel pour résoudre les espaces de noms DNS entre votre centre de données sur site et votre. VPCs
- La zone hébergée privée Amazon Route 53 est un conteneur qui contient des informations sur la manière dont vous souhaitez que Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines.
- Les profils Amazon Route 53 vous permettent d'appliquer et de gérer de manière simplifiée des configurations Route 53 liées au DNS dans de nombreuses VPCs configurations différentes Comptes AWS .

Bonnes pratiques

Cette section fournit certaines des meilleures pratiques pour optimiser Route 53 Resolver. Elles représentent un sous-ensemble des meilleures pratiques de Route 53. Pour obtenir une liste complète, consultez la section Meilleures pratiques pour Amazon Route 53.

Évitez les configurations en boucle avec les points de terminaison du résolveur

- Concevez votre architecture DNS pour empêcher le routage récursif en planifiant soigneusement les associations VPC. Lorsqu'un VPC héberge un point de terminaison entrant, évitez de l'associer à des règles de résolution susceptibles de créer des références circulaires.
- Utilisez-le de AWS RAM manière stratégique lorsque vous partagez des ressources DNS entre des comptes afin de maintenir des chemins de routage propres.

Pour plus d'informations, consultez la section Éviter les configurations de boucle avec les points de terminaison du résolveur dans la documentation Route 53.

Points de terminaison Scale Resolver

- Pour les environnements qui nécessitent un nombre élevé de requêtes par seconde (QPS), sachez qu'il existe une limite de 10 000 QPS par ENI dans un point de terminaison. Il est ENIs possible d'en ajouter d'autres à un point de terminaison pour dimensionner le DNS QPS.
- Amazon CloudWatch fournit `InboundQueryVolume` et fournit `OutboundQueryVolume` des statistiques (voir la CloudWatch documentation). Nous vous recommandons de configurer des règles de surveillance qui vous alertent si le seuil dépasse une certaine valeur (par exemple, 80 % de 10 000 QPS).
- Configurez des règles de groupe de sécurité dynamiques pour les points de terminaison du résolveur afin d'éviter que les limites de suivi des connexions n'entraînent une limitation des requêtes DNS en cas de trafic élevé. Pour en savoir plus sur le fonctionnement du suivi des connexions dans les groupes de sécurité, consultez la section Suivi des connexions des groupes de EC2 sécurité Amazon dans la EC2 documentation Amazon.

Pour plus d'informations, consultez la section Resolver endpoint scaling dans la documentation de Route 53.

Offrez une haute disponibilité aux points de terminaison Resolver

- Créez des points de terminaison entrants avec des adresses IP dans au moins deux zones de disponibilité à des fins de redondance.
- Fournissez des interfaces réseau supplémentaires pour garantir la disponibilité pendant la maintenance ou les pics de trafic.

Pour plus d'informations, consultez la section Haute disponibilité pour les points de terminaison du résolveur dans la documentation Route 53.

Épopées

Déployer les points de terminaison Route 53 Resolver

Tâche	Description	Compétences requises
Déployez un point de terminaison entrant.	Route 53 Resolver utilise le point de terminaison entrant pour recevoir les requêtes DNS des résolveurs DNS locaux. Pour obtenir des instructions, consultez la section Transférer des requêtes DNS entrantes vers votre VPCs adresse dans la documentation de Route 53. Notez l'adresse IP du point de terminaison entrant.	Administrateur AWS, administrateur du cloud
Déployez un point de terminaison sortant.	Route 53 Resolver utilise le point de terminaison sortant pour envoyer des requêtes DNS aux résolveurs DNS locaux. Pour obtenir des instructions, consultez la section Transfert de requêtes DNS sortantes vers votre réseau dans la documentation Route 53. Notez l'ID du point de terminaison de sortie.	Administrateur AWS, administrateur du cloud

Configurer et partager les zones hébergées privées Route 53

Tâche	Description	Compétences requises
Créez une zone hébergée privée pour un domaine hébergé sur AWS.	Cette zone contient les enregistrements DNS pour les ressources d'un domaine AWS hébergé (par exemple,`prod.aws.example.com`) qui doivent être résolues à partir de l'environnement sur site. Pour obtenir des instructions, consultez la section Création d'une zone hébergée privée dans la documentation de Route 53. Lorsque vous créez une zone hébergée privée, vous devez associer un VPC à la zone hébergée appartenant au même compte. Sélectionnez le VPC Shared Services à cette fin.	Administrateur AWS, administrateur du cloud
Configuration de base : associez la zone hébergée privée VPCs à d'autres comptes.	Si vous utilisez une configuration de base (voir la section Architecture) : Pour permettre aux ressources du compte membre de VPCs résoudre les enregistrements DNS dans cette zone hébergée privée, vous devez VPCs associer votre compte à la zone hébergée. Vous devez autoriser l'association,	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
	puis la créer par programmation. Pour obtenir des instructions, consultez la section Association d'un Amazon VPC et d'une zone hébergée privée que vous avez créée avec une méthode différente Comptes AWS dans la documentation de Route 53.	

Tâche	Description	Compétences requises
Configuration améliorée : configurez et partagez les profils Route 53.	Si vous utilisez une configuration améliorée (voir la section Architecture) : 1. Créez un profil Route 53 et associez-y les zones hébergées privées pertinentes. Pour obtenir des instructions, consultez la section Création de profils Route 53 dans la documentation Route 53. 2. AWS RAM À utiliser pour partager le profil avec les comptes des membres, puis associer le profil partagé à Target VPCs. Pour obtenir des instructions, consultez Partager un profil Route 53 et associer un profil Route 53 à VPCs dans la documentation Route 53. **Note** En fonction de la structure de votre organisation et des exigences en matière de DNS, vous devrez peut-être créer et gérer plusieurs profils pour différents	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
	comptes ou charges de travail.	

Configurer et partager les règles de transfert du résolveur Route 53

Tâche	Description	Compétences requises
Créez une règle de transfert pour un domaine hébergé sur site.	Cette règle indiquera à Route 53 Resolver de transférer toutes les requêtes DNS pour les domaines locaux (tels que `onprem.example.com`) aux résolveurs DNS locaux. Pour créer cette règle, vous avez besoin des adresses IP des résolveurs DNS locaux et de l'ID du point de terminaison sortant. Pour obtenir des instructions, consultez la section Création de règles de transfert dans la documentation Route 53.	Administrateur AWS, administrateur du cloud
Configuration de base : partagez et associez la règle de transfert VPCs à vos autres comptes.	Si vous utilisez la configuration de base : Pour que la règle de transfert entre en vigueur, vous devez la partager et l'associer VPCs à vos autres comptes. Route 53 Resolver prend ensuite la règle en considération lorsqu'il résout un domaine. Pour obtenir des instructions,	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
	consultez les sections Partage des règles du résolveur avec d'autres utilisateurs Comptes AWS et utilisation de règles partagées et Associati on de règles de transfert à un VPC dans la documentation de Route 53.	

Tâche	Description	Compétences requises
Configuration améliorée : configurez et partagez les profils Route 53.	Si vous utilisez la configuration améliorée : 1. Si vous avez déjà créé un profil Route 53 lors des étapes précédentes, vous pouvez utiliser le même profil. Sinon, créez un profil Route 53 et associez-y les règles de transfert pertinentes du résolveur. Pour obtenir des instructions, consultez la section Création de profils Route 53 dans la documentation Route 53. 2. AWS RAM À utiliser pour partager le profil avec les comptes des membres, puis associer le profil partagé à Target VPCs. Pour obtenir des instructions, consultez Partager un profil Route 53 et associer un profil Route 53 à VPCs dans la documentation Route 53. **Note** En fonction de la structure de votre organisation et des exigences en matière de DNS, vous devrez	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
	peut-être créer et gérer plusieurs profils pour différents comptes ou charges de travail.	

Configurer des résolveurs DNS locaux pour l'intégration AWS

Tâche	Description	Compétences requises
Configurez le transfert conditionnel dans les résolveurs DNS locaux.	Pour que les requêtes DNS soient envoyées AWS depuis l'environnement local à des fins de résolution, vous devez configurer le transfert conditionnel dans les résolveurs DNS locaux pour qu'il pointe vers l'adresse IP du point de terminaison entrant. Cela indique aux résolveurs DNS de transférer toutes les requêtes DNS pour le domaine AWS hébergé (par exemple, pour`prod.aws.example.com`) à l'adresse IP du point de terminaison entrant pour résolution par Route 53 Resolver.	Administrateur réseau

Vérifier la résolution end-to-end DNS dans un environnement hybride

Tâche	Description	Compétences requises
Testez la résolution DNS depuis AWS l'environnement sur site.	À partir d'une instance d'un VPC à laquelle la règle de transfert est associée, effectuez une requête DNS pour un domaine hébergé sur site (par exemple, pour). `db.onprem.example.com`	Administrateur réseau
Testez la résolution DNS depuis l'environnement sur site vers AWS.	À partir d'un serveur local, effectuez une résolution DNS pour un domaine AWS hébergé (par exemple, pour`ec2.prod.aws.example.com`).	Administrateur réseau

Ressources connexes

- Options DNS dans le cloud hybride pour Amazon VPC (livre blanc)AWS
- Utilisation de zones hébergées privées (documentation Route 53)
- Commencer à utiliser Route 53 Resolver (documentation Route 53)
- Simplifiez la gestion du DNS dans un environnement multi-comptes avec Route 53 Resolver (AWS article de blog)
- Unifiez la gestion du DNS à l'aide de profils Amazon Route 53 avec plusieurs VPCs et Comptes AWS (article de AWS blog)
- Migration de votre environnement DNS multi-comptes vers les profils Amazon Route 53 (AWS article de blog)
- Utilisation des profils Amazon Route 53 pour des AWS environnements multi-comptes évolutifs (article de AWS blog)

Vérifiez que les équilibreurs de charge ELB nécessitent une terminaison TLS

Créée par Priyanka Chaudhary (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), Elastic Load Balancing (ELB) distribue automatiquement le trafic applicatif entrant sur plusieurs cibles, telles que les instances Amazon Elastic Compute Cloud (Amazon EC2), les conteneurs, les adresses IP et les fonctions AWS Lambda. Les équilibreurs de charge utilisent des écouteurs pour définir les ports et les protocoles qu'ils utilisent pour accepter le trafic provenant des utilisateurs. Les équilibreurs de charge d'application prennent les décisions de routage au niveau de la couche application et utilisent leHTTP/HTTPS protocols. Classic Load Balancers make routing decisions at either the transport layer, by using TCP or Secure Sockets Layer (SSL) protocols, or at the application layer, by using HTTP/HTTPS.

Ce modèle fournit un contrôle de sécurité qui examine plusieurs types d'événements pour les équilibreurs de charge d'application et les équilibreurs de charge classiques. Lorsque la fonction est invoquée, AWS Lambda inspecte l'événement et s'assure que l'équilibreur de charge est conforme.

La fonction lance un événement Amazon CloudWatch Events sur les appels d'API suivants : CreateLoadBalancerCreateLoadBalancerListeners, DeleteLoadBalancerListeners, CreateLoadBalancerPolicy, SetLoadBalancerPoliciesOfListener, CreateListenerDeleteListener, et ModifyListener. Lorsque l'événement détecte l'un d'entre eux APIs, il appelle AWS Lambda, qui exécute un script Python. Le script Python évalue si l'écouteur contient un certificat SSL et si la politique appliquée utilise le protocole TLS (Transport Layer Security). S'il est déterminé que la politique SSL est autre chose que TLS, la fonction envoie une notification Amazon Simple Notification Service (Amazon SNS) à l'utilisateur avec les informations pertinentes.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

Limites

- Ce contrôle de sécurité ne vérifie pas les équilibreurs de charge existants, sauf si une mise à jour est apportée aux écouteurs des équilibreurs de charge.

- Ce contrôle de sécurité est régional. Vous devez le déployer dans chaque région AWS que vous souhaitez surveiller.

Architecture

Architecture cible

Automatisation et évolutivité

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Ce modèle inclut les pièces jointes suivantes :

- `ELBRequirestlstermination.zip`— Le code Lambda pour le contrôle de sécurité.
- `ELBRequirestlstermination.yml`— Le CloudFormation modèle qui définit l'événement et la fonction Lambda.

Épopées

Configuration du compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 pour héberger le fichier .zip de code Lambda. Ce compartiment S3 doit se trouver dans la même région AWS que l'équilibreur de charge que vous souhaitez évaluer. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Le nom du compartiment S3 ne peut pas inclure de barres obliques en tête.	Architecte du cloud
Téléchargez le code Lambda.	Téléchargez le code Lambda (`ELBRequirestlstermination.zip` fichier) fourni dans la section Pièces jointes dans le compartiment S3.	Architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle AWS.	Ouvrez la CloudFormation console AWS dans la même région AWS que votre compartiment S3 et déployez le modèle joint `ELBRequirestlstermination.yml`. Pour plus d'informations sur le déploiement de CloudFormation modèles AWS, consultez la section Création d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation.	Architecte du cloud
Complétez les paramètres du modèle.	Lorsque vous lancez le modèle, les informations suivantes vous sont demandées : • Compartiment S3 : Spécifiez le compartiment que vous avez créé ou sélectionné dans le premier épisode épique. C'est ici que vous avez chargé le code Lambda joint (`ELBRequirestlstermination.zip` fichier). • Clé S3 : Spécifiez l'emplacement du fichier Lambda .zip dans votre compartiment S3 (par exemple, `ELBRequir`	Architecte du cloud

Tâche	Description	Compétences requises
	`estlstermination.zip` ou). `controls/ELBRequirestlstermination.zip` N'incluez pas de barres obliques en tête. • E-mail de notification : indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications Amazon SNS. • Niveau de journalisation Lambda : Spécifiez le niveau et la fréquence de journalisation pour la fonction Lambda. Utilisez Info pour consigner des messages d'information détaillés sur la progression, Erreur pour les événements d'erreur susceptibles de permettre la poursuite du déploiement et Avertissement pour les situations potentiellement dangereuses.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail	Architecte du cloud

Tâche	Description	Compétences requises
	d'abonnement à l'adresse e-mail que vous avez fournie. Vous devez confirmer cet abonnement par e-mail pour commencer à recevoir des notifications de violation.	

Ressources connexes

- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Qu'est-ce qu'AWS Lambda ? (documentation AWS Lambda)
- Qu'est-ce qu'un équilibreur de charge Classic Load Balancer ? (documentation de l'ELB)
- Qu’est-ce qu’un équilibreur de charge Application Load Balancer ? (documentation de l'ELB)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Consultez les journaux et les statistiques d'AWS Network Firewall à l'aide de Splunk

Créée par Ivo Pinto

Récapitulatif

De nombreuses organisations utilisent Splunk Enterprise comme outil centralisé d'agrégation et de visualisation pour les journaux et les métriques provenant de différentes sources. Ce modèle vous permet de configurer Splunk pour récupérer les journaux et les métriques d'AWS Network Firewall depuis Amazon CloudWatch Logs à l'aide du module complémentaire Splunk pour AWS.

Pour ce faire, vous créez un rôle AWS Identity and Access Management (IAM) en lecture seule. Le module complémentaire Splunk pour AWS utilise ce rôle pour accéder CloudWatch. Vous configurez le module complémentaire Splunk pour AWS afin de récupérer les métriques et les journaux. CloudWatch Enfin, vous créez des visualisations dans Splunk à partir des données de journal et des métriques récupérées.

Conditions préalables et limitations

Prérequis

- Un compte Splunk
- Une instance Splunk Enterprise, version 8.2.2 ou ultérieure
- Un compte AWS actif
- Network Firewall, configuré et configuré pour envoyer des CloudWatch journaux à Logs

Limites

- Splunk Enterprise doit être déployé sous la forme d'un cluster d'instances Amazon Elastic Compute Cloud (Amazon EC2) dans le cloud AWS.
- La collecte de données à l'aide d'un rôle IAM découvert automatiquement pour Amazon n' EC2 est pas prise en charge dans les régions AWS Chine.

Architecture

Le diagramme illustre les éléments suivants :

1. Network Firewall publie les journaux dans CloudWatch Logs.
2. Splunk Enterprise extrait les métriques et les journaux à partir de. CloudWatch

Pour renseigner des exemples de métriques et de journaux dans cette architecture, une charge de travail génère du trafic qui passe par le point de terminaison Network Firewall pour accéder à Internet. Ceci est réalisé grâce à l'utilisation de tables de routage. Bien que ce modèle utilise une seule EC2 instance Amazon comme charge de travail, il peut s'appliquer à n'importe quelle architecture tant que Network Firewall est configuré pour envoyer des CloudWatch journaux à Logs.

Cette architecture utilise également une instance Splunk Enterprise dans un autre cloud privé virtuel (VPC). Cependant, l'instance Splunk peut se trouver dans un autre emplacement, par exemple dans le même VPC que la charge de travail, à condition qu'elle puisse atteindre le. CloudWatch APIs

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Network Firewall est un pare-feu réseau dynamique et géré, ainsi qu'un service de détection et de prévention des intrusions VPCs destiné au cloud AWS.

Autres outils

- Splunk vous aide à surveiller, à visualiser et à analyser les données des journaux.

Épopées

Créer un rôle IAM

Tâche	Description	Compétences requises
Créez la politique IAM.	Suivez les instructions de la section Création de politique	Administrateur AWS

Tâche	Description	Compétences requises
	s à l'aide de l'éditeur JSON pour créer la politique IAM qui accorde un accès en lecture seule aux données et aux métriques CloudWatch des journaux. CloudWatch Collez le politique suivante dans l'éditeur JSON. `{ "Statement": [ { "Action": [ "cloudwatch:List*", "cloudwatch:Get*", "network-firewall: List*", "logs:Describe*", "logs:Get*", "logs:List*", "logs:StartQuery", "logs:StopQuery", "logs:TestMetricFi lter", "logs:FilterLogEve nts", "network-firewall: Describe*" ],`	

Tâche	Description	Compétences requises
	"Effect": "Allow", "Resource": "*" }], "Version": "2012-10-17" }	
Créez un nouveau rôle IAM.	Suivez les instructions de la section Création d'un rôle pour déléguer des autorisations à un service AWS afin de créer le rôle IAM auquel le module complémentaire Splunk pour AWS utilise pour accéder. CloudWatch Pour les politiques d'autorisations, choisissez la politique que vous avez créée précédemment.	Administrateur AWS

Tâche	Description	Compétences requises
Attribuez le rôle IAM aux EC2 instances du cluster Splunk.	1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/. 2. Dans le panneau de navigation, choisissez Instances. 3. Sélectionnez les EC2 instances du cluster Splunk. 4. Choisissez Actions, Sécurité, puis Modifier le rôle IAM. 5. Sélectionnez le rôle IAM que vous avez créé précédemment, puis choisissez Enregistrer.	Administrateur AWS

Installation du module complémentaire Splunk pour AWS

Tâche	Description	Compétences requises
Installez le module complémentaire.	1. Dans le tableau de bord Splunk, accédez à Splunk Apps. 2. Recherchez le module complémentaire Splunk pour Amazon Web Services. 3. Choisissez Installer. 4. Fournissez vos informations d'identification Splunk.	Administrateur Splunk

Tâche	Description	Compétences requises
Configurez les informations d'identification AWS.	1. Dans le tableau de bord Splunk, accédez au module complémentaire Splunk pour AWS. 2. Choisissez Configuration. 3. Dans la colonne Rôle IAM découvert automatiq uement, sélectionnez le rôle IAM que vous avez créé précédemment. Pour plus d'informations, consultez la section Trouver un rôle IAM au sein de votre instance de plateforme Splunk dans la documentation Splunk.	Administrateur Splunk

Configurez l'accès Splunk à CloudWatch

Tâche	Description	Compétences requises
Configurez la récupération des journaux de Network Firewall à partir de CloudWatch Logs.	1. Dans le tableau de bord Splunk, accédez au module complémentaire Splunk pour AWS. 2. Choisissez Input. 3. Choisissez Créer une nouvelle entrée. 4. Dans la liste, choisissez Type de données personnal isé, puis CloudWatch Logs.	Administrateur Splunk

Tâche	Description	Compétences requises
	5. Indiquez le nom, le compte AWS, la région AWS et le groupe de journaux pour vos journaux Network Firewall. 6. Choisissez Enregistrer. Par défaut, Splunk récupère les données du journal toutes les 10 minutes. Il s'agit d'un paramètre configurable dans les paramètres avancés. Pour plus d'informations, consultez Configurer une entrée de CloudWatch logs à l'aide de Splunk Web dans la documentation Splunk.	

Tâche	Description	Compétences requises
Configurez la récupération des métriques de Network Firewall à partir de CloudWatch.	1. Dans le tableau de bord Splunk, accédez au module complémentaire Splunk pour AWS. 2. Choisissez Input. 3. Choisissez Créer une nouvelle entrée. 4. Dans la liste, choisissez CloudWatch. 5. Indiquez le nom, le compte AWS et la région AWS pour les métriques de votre Network Firewall. 6. À côté de Configuration métrique, choisissez Modifier en mode avancé. 7. (Facultatif) Supprimez tous les espaces de noms préconfigurés. 8. Choisissez Ajouter un espace de noms, puis nommez-le NetworkFirewallAWS/. 9. Dans Dimension Value, ajoutez ce qui suit. `[{"AvailabilityZone":[".*"],"Engine":[".*"],"FirewallName":[".*"]}]` 10. Pour Metrics, sélectionnez All.	Administrateur Splunk

Tâche	Description	Compétences requises
	11. Pour les statistiques métriques, choisissez Sum. 12. Choisissez OK. 13. Choisissez Enregistrer. Par défaut, Splunk récupère les données métriques toutes les 5 minutes. Il s'agit d'un paramètre configurable dans les paramètres avancés. Pour plus d'informations, consultez Configurer une CloudWatch entrée à l'aide de Splunk Web dans la documentation Splunk.	

Créez des visualisations Splunk à l'aide de requêtes

Tâche	Description	Compétences requises
Consultez les principales adresses IP sources.	1. Dans le tableau de bord Splunk, accédez à Search & Reporting. 2. Dans le champ Entrez la recherche ici, entrez ce qui suit. `sourcetype="aws:cloudwatchlogs" | top event.src_ip` Cette requête affiche un tableau des adresses IP sources ayant le plus de trafic, par ordre décroissant.	Administrateur Splunk

Tâche	Description	Compétences requises
	3. Pour une représentation graphique, choisissez Visualization.	
Afficher les statistiques des paquets.	1. Dans le tableau de bord Splunk, accédez à Search & Reporting. 2. Dans le champ Entrez la recherche ici, entrez ce qui suit. `sourcetype="aws:cloudwatch"| timechart sum(Sum) by metric_name` Cette requête affiche un tableau des mesures `DroppedPackets` `PassedPackets`, et `ReceivedPackets` par minute. 3. Pour une représentation graphique, choisissez Visualization.	Administrateur Splunk

Tâche	Description	Compétences requises
Consultez les ports sources les plus utilisés.	1. Dans le tableau de bord Splunk, accédez à Search & Reporting. 2. Dans le champ Entrez la recherche ici, entrez ce qui suit. `sourcetype="aws:cloudwatchlogs" | top event.dest_port` Cette requête affiche un tableau des ports sources ayant le plus de trafic, par ordre décroissant. 3. Pour une représentation graphique, choisissez Visualization.	Administrateur Splunk

Ressources connexes

Documentation AWS

- Création d'un rôle pour déléguer des autorisations à un service AWS (documentation IAM)
- Création de politiques IAM (documentation IAM)
- Journalisation et surveillance dans AWS Network Firewall (documentation Network Firewall)
- Configurations des tables de routage pour AWS Network Firewall (documentation Network Firewall)

Articles de blog AWS

- Modèles de déploiement d'AWS Network Firewall

AWS Marketplace

- Image de machine Amazon (AMI) de Splunk Enterprise

Plus de modèles

- Accédez à un hôte bastion à l'aide du gestionnaire de session et d'Amazon EC2 Instance Connect
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS Fargate, d' PrivateLinkAWS et d'un Network Load Balancer
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Centralisation de la résolution DNS à l'aide AWS Managed Microsoft AD et sur site de Microsoft Active Directory
- Vérifiez les entrées du réseau à hôte unique dans les règles d'entrée du groupe de sécurité pour et IPv4 IPv6
- Créez un portail pour les micro-frontends en utilisant AWS Amplify Angular et Module Federation
- Déployez un pare-feu à l'aide d'AWS Network Firewall et d'AWS Transit Gateway
- Déployez une API Amazon API Gateway sur un site Web interne à l'aide de points de terminaison privés et d'un Application Load Balancer
- Déployez des contrôles d'accès basés sur des attributs de détection pour les sous-réseaux publics en utilisant AWS Config
- Déployez des contrôles d'accès préventifs basés sur les attributs pour les sous-réseaux publics
- Activer les connexions chiffrées pour les instances de base de données PostgreSQL dans Amazon RDS
- Étendez votre accès VRFs à AWS en utilisant AWS Transit Gateway Connect
- Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS
- Migrer les contrôleurs d'entrée NGINX lors de l'activation du mode automatique Amazon EKS
- Préservez l'espace IP routable dans les conceptions VPC multi-comptes pour les sous-réseaux autres que les charges de travail
- Empêchez l'accès à Internet au niveau du compte en utilisant une politique de contrôle des services
- Envoyer des alertes depuis AWS Network Firewall vers un canal Slack
- Diffusez du contenu statique dans un compartiment Amazon S3 via un VPC en utilisant Amazon CloudFront
- Configurer la reprise après sinistre pour Oracle JD Edwards EnterpriseOne avec AWS Elastic Disaster Recovery

- Utilisez les requêtes BMC Discovery pour extraire les données de migration afin de planifier la migration
- Utilisez Network Firewall pour capturer les noms de domaine DNS à partir de l'indication du nom du serveur pour le trafic sortant

Diffusion de contenu

Rubriques

- Envoyez AWS WAF des logs à Splunk à l'aide AWS Firewall Manager d'Amazon Data Firehose
- Diffusez du contenu statique dans un compartiment Amazon S3 via un VPC en utilisant Amazon CloudFront
- Plus de modèles

Envoyez AWS WAF des logs à Splunk à l'aide AWS Firewall Manager d'Amazon Data Firehose

Créée par Michael Friedenthal (AWS), Aman Kaur Gandhi (AWS) et JJ Johnson (AWS)

Récapitulatif

Historiquement, il existait deux méthodes pour transférer des données dans Splunk : une architecture push ou pull. Une architecture d'extraction garantit les données de livraison grâce à de nouvelles tentatives, mais elle nécessite des ressources dédiées dans Splunk pour interroger les données. Les architectures d'extraction ne fonctionnent généralement pas en temps réel en raison du sondage. Une architecture push présente généralement une latence plus faible, est plus évolutive et réduit la complexité opérationnelle et les coûts. Cependant, il ne garantit pas la livraison et nécessite généralement des agents.

L'intégration de Splunk à Amazon Data Firehose fournit des données de streaming en temps réel à Splunk via un collecteur d'événements HTTP (HEC). Cette intégration offre les avantages des architectures push et pull : elle garantit la livraison des données par le biais de nouvelles tentatives, se fait en temps quasi réel et présente une faible latence et une faible complexité. Le HEC envoie rapidement et efficacement des données via HTTP ou HTTPS directement à Splunk. HECs sont basés sur des jetons, ce qui élimine le besoin de coder en dur les informations d'identification dans une application ou dans les fichiers de support.

Dans une AWS Firewall Manager politique, vous pouvez configurer la journalisation de l'ensemble du trafic ACL AWS WAF Web de tous vos comptes, puis utiliser un flux de diffusion Firehose pour envoyer ces données de journal à Splunk à des fins de surveillance, de visualisation et d'analyse. Cette solution offre les avantages suivants :

- Gestion et journalisation centralisées du trafic ACL AWS WAF Web sur tous vos comptes
- Intégration de Splunk avec un seul Compte AWS
- Evolutivité
- Livraison en temps quasi réel des données du journal
- Optimisation des coûts grâce à l'utilisation d'une solution sans serveur, afin que vous n'ayez pas à payer pour les ressources inutilisées.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS qui fait partie d'une organisation dans AWS Organizations.
- Vous devez disposer des autorisations suivantes pour activer la journalisation avec Firehose :
  - `iam:CreateServiceLinkedRole`
  - `firehose:ListDeliveryStreams`
  - `wafv2:PutLoggingConfiguration`
- AWS WAF et son site Web ACLs doit être configuré. Pour obtenir des instructions, voir Commencer avec AWS WAF.
- AWS Firewall Manager doit être configuré. Pour obtenir des instructions, reportez-vous à la section AWS Firewall Manager Conditions préalables.
- Les politiques de sécurité de Firewall Manager pour AWS WAF doivent être configurées. Pour obtenir des instructions, voir Commencer à utiliser AWS Firewall ManagerAWS WAF les politiques.
- Splunk doit être configuré avec un point de terminaison HTTP public accessible par Firehose.

Limites

- Ils Comptes AWS doivent être gérés dans une seule organisation en AWS Organizations.
- L'ACL Web doit se trouver dans la même région que le flux de diffusion. Si vous capturez des logs pour Amazon CloudFront, créez le flux de diffusion Firehose dans la région USA Est (Virginie du Nord),. `us-east-1`
- Le module complémentaire Splunk pour Firehose est disponible pour les déploiements payants de Splunk Cloud, les déploiements distribués de Splunk Enterprise et les déploiements Splunk Enterprise en instance unique. Ce module complémentaire n'est pas pris en charge pour les déploiements d'essai gratuits de Splunk Cloud.

Architecture

Pile technologique cible

- Firewall Manager
- Firehose
- Amazon Simple Storage Service (Amazon S3)

- AWS WAF
- Splunk

Architecture cible

L'image suivante montre comment utiliser Firewall Manager pour enregistrer toutes les AWS WAF données de manière centralisée et les envoyer à Splunk via Firehose.

1. Le AWS WAF Web ACLs envoie les données du journal du pare-feu à Firewall Manager.
2. Firewall Manager envoie les données du journal à Firehose.
3. Le flux de diffusion Firehose transmet les données du journal à Splunk et à un compartiment S3. Le compartiment S3 fait office de sauvegarde en cas d'erreur dans le flux de diffusion Firehose.

Automatisation et évolutivité

Cette solution est conçue pour évoluer et s'adapter à tous les AWS WAF sites ALCs Web de l'organisation. Vous pouvez configurer tous les sites Web ACLs pour utiliser la même instance Firehose. Toutefois, si vous souhaitez configurer et utiliser plusieurs instances de Firehose, vous le pouvez.

Outils

Services AWS

- AWS Firewall Managerest un service de gestion de la sécurité qui vous permet de configurer et de gérer de manière centralisée les règles de pare-feu pour l'ensemble de vos comptes et applications dans AWS Organizations.
- Amazon Data Firehose vous permet de diffuser des données de streaming en temps réel vers d'autres Services AWS points de terminaison HTTP personnalisés et vers des points de terminaison HTTP appartenant à des fournisseurs de services tiers pris en charge, tels que Splunk.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS WAFest un pare-feu d'applications Web qui vous aide à surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources protégées de votre application Web.

Autres outils

- Splunk vous aide à surveiller, visualiser et analyser les données des journaux.

Épopées

Configurer Splunk

Tâche	Description	Compétences requises
Installez l'application Splunk pour AWS.	1. Connectez-vous à votre redirecteur Splunk Heavy. L'URL par défaut est `http://<IP address>:8000` . 2. Dans le menu de navigation de gauche, à côté de Apps, cliquez sur le bouton d'engrenage. 3. Choisissez Parcourir d'autres applications. 4. Recherchez AWS. 5. Pour Splunk App for AWS, choisissez Installer. 6. Entrez vos identifiants de connexion à Splunk.com, acceptez les termes et conditions, puis choisissez Login and Install. 7. Sélectionnez Exécuté.	Administrateur de sécurité, administrateur Splunk
Installez le module complémentaire pour AWS WAF.	Répétez les instructions précédentes pour installer le module complémentaire AWS Web Application Firewall pour Splunk.	Administrateur de sécurité, administrateur Splunk

Tâche	Description	Compétences requises
Installez et configurez le module complémentaire Splunk pour Firehose.	1. Installez et configurez le module complémentaire Splunk pour Firehose. Dans le cadre de l'installation et de la configuration, si nécessaire pour votre plateforme Splunk, vous configurez un collecteur d'événements HTTP et vous préparez l'infrastructure pour envoyer les données du journal à vos indexeurs. Consultez les instructions correspondant à votre déploiement Splunk : • Déploiement de Splunk Cloud (documentation Splunk) • Déploiement distribué de Splunk Enterprise (documentation Splunk) • Déploiement de Splunk Enterprise en instance unique (documentation Splunk) **⚠ Important** Arrêtez cette procédure après avoir installé et configuré le module complémentaire	Administrateur de sécurité, administrateur Splunk

Tâche	Description	Compétences requises
	Splunk. Ne suivez pas les instructions de configuration de Firehose pour envoyer des données à la plateforme Splunk. 2. Notez le jeton du collecteur d'événements HTTP et le point de terminaison HTTP. Vous aurez besoin de cette valeur ultérieurement, lorsque vous configurerez le flux de diffusion.	

Création du flux de diffusion Firehose

Tâche	Description	Compétences requises
Accordez à Firehose l'accès à une destination Splunk.	Configurez la politique d'accès qui permet à Firehose d'accéder à une destination Splunk et de sauvegarder les données du journal dans un compartiment S3. Pour plus d'informations, consultez Accorder à Firehose l'accès à une destination Splunk.	Administrateur de sécurité
Créez un flux de diffusion Firehose.	Dans le compte ACLs pour lequel vous gérez le Web AWS WAF, créez un flux de diffusion dans Firehose. Vous devez disposer d'un rôle IAM	Administrateur de sécurité

Tâche	Description	Compétences requises
	lorsque vous créez un flux de diffusion. Firehose assume ce rôle IAM et accède au compartiment S3 spécifié. Pour obtenir des instructions, consultez la section Création d'un flux de diffusion. Remarques : • Le nom du flux de diffusion doit commencer par `aws-waf-logs-` . • Pour la source, choisissez Direct PUT. • Pour le mode de sauvegarde S3, choisissez Sauvegarder tous les événements, puis choisissez un bucket existant ou créez-en un nouveau. • Pour la destination, suivez les instructions de la section Choisissez Splunk pour votre destination dans la documentation de Firehose. Pour plus d'informations sur les valeurs des points de terminaison et des types de points de terminaison Splunk, consultez la section Configurer Amazon Data Firehose dans la documentation Splunk.	

Tâche	Description	Compétences requises
	Répétez ce processus pour chaque jeton que vous avez configuré dans le collecteur d'événements HTTP.	
Testez le flux de diffusion.	Testez le flux de diffusion pour vérifier qu'il est correctem ent configuré. Pour obtenir des instructions, consultez la section Tester en utilisant Splunk comme destination dans la documentation de Firehose.	Administrateur de sécurité

Configurer Firewall Manager pour enregistrer les données

Tâche	Description	Compétences requises
Configurez les politiques de Firewall Manager.	Les politiques de Firewall Manager doivent être configurées pour activer la journalisation et pour transfére r les journaux vers le flux de diffusion Firehose approprié . Pour plus d'informations et d'instructions, voir Configura tion de la journalisation pour une AWS WAF politique.	Administrateur de sécurité

Ressources connexes

AWS resources

- Journalisation du trafic ACL Web (AWS WAF documentation)

- Configuration de la journalisation pour une AWS WAF politique (AWS WAF documentation)
- Tutoriel : Envoyer des journaux de flux VPC à Splunk à l'aide d'Amazon Data Firehose (documentation Firehose)
- Comment transférer les journaux de flux VPC vers Splunk à l'aide d'Amazon Data Firehose ? (Centre de AWS connaissances)
- Boostez l'ingestion de données dans Splunk à l'aide d'Amazon Data FirehoseAWS (article de blog)

Documentation Splunk

- Module complémentaire Splunk pour Amazon Data Firehose

Diffusez du contenu statique dans un compartiment Amazon S3 via un VPC en utilisant Amazon CloudFront

Créée par Angel Emmanuel Hernandez Cebrian

Récapitulatif

Lorsque vous diffusez du contenu statique hébergé sur Amazon Web Services (AWS), l'approche recommandée consiste à utiliser un bucket Amazon Simple Storage Service (S3) comme origine et à utiliser CloudFront Amazon pour distribuer le contenu. Cette solution présente deux avantages principaux : la commodité de la mise en cache du contenu statique à des emplacements périphériques et la possibilité de définir des listes de contrôle d'accès Web (Web ACLs) pour la CloudFront distribution, ce qui vous permet de sécuriser les demandes relatives au contenu avec un minimum de configuration et de frais administratifs.

Cependant, il existe une limite architecturale commune à l'approche standard recommandée. Dans certains environnements, vous souhaitez déployer des dispositifs de pare-feu virtuels dans un cloud privé virtuel (VPC) pour inspecter l'ensemble du contenu, y compris le contenu statique. L'approche standard n'achemine pas le trafic via le VPC à des fins d'inspection. Ce modèle fournit une solution architecturale alternative. Vous utilisez toujours une CloudFront distribution pour diffuser du contenu statique dans un compartiment S3, mais le trafic est acheminé via le VPC à l'aide d'un Application Load Balancer. Une fonction AWS Lambda récupère et renvoie ensuite le contenu du compartiment S3.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Contenu de site Web statique hébergé dans un compartiment S3.

Limites

- Les ressources de ce modèle doivent se trouver dans une seule région AWS, mais elles peuvent être mises en service dans différents comptes AWS.
- Les limites s'appliquent à la taille maximale des demandes et des réponses que la fonction Lambda peut recevoir et envoyer, respectivement. Pour plus d'informations, consultez la section Limits des fonctions Lambda en tant que cibles (documentation Elastic Load Balancing).

- Il est important de trouver un bon équilibre entre performances, évolutivité, sécurité et rentabilité lors de l'utilisation de cette approche. Malgré la grande évolutivité de Lambda, si le nombre d'appels Lambda simultanés dépasse le quota maximum, certaines demandes sont limitées. Pour plus d'informations, consultez les quotas Lambda (documentation Lambda). Vous devez également tenir compte de la tarification lorsque vous utilisez Lambda. Pour minimiser les appels Lambda, assurez-vous de définir correctement le cache pour la distribution. CloudFront Pour plus d'informations, consultez Optimisation de la mise en cache et de la disponibilité (CloudFront documentation).

Architecture

Pile technologique cible

- CloudFront
- Amazon Virtual Private Cloud (Amazon VPC)
- Application Load Balancer
- Lambda
- Amazon S3

Architecture cible

L'image suivante montre l'architecture suggérée lorsque vous devez l'utiliser pour diffuser du contenu statique CloudFront à partir d'un compartiment S3 via un VPC.

1. Le client demande l'URL de CloudFront distribution pour obtenir un fichier de site Web spécifique dans le compartiment S3.
2. CloudFront envoie la demande à AWS WAF. AWS WAF filtre la demande en utilisant le Web ACLs appliqué à la CloudFront distribution. S'il est déterminé que la demande est valide, le flux continue. S'il est déterminé que la demande n'est pas valide, le client reçoit une erreur 403.
3. CloudFront vérifie son cache interne. Si une clé valide correspond à la demande entrante, la valeur associée est renvoyée au client sous forme de réponse. Dans le cas contraire, le flux continue.
4. CloudFront transmet la demande à l'URL de l'Application Load Balancer spécifié.
5. L'Application Load Balancer possède un écouteur associé à un groupe cible basé sur une fonction Lambda. L'Application Load Balancer appelle la fonction Lambda.

6. La fonction Lambda se connecte au compartiment S3, effectue une `GetObject` opération sur celui-ci et renvoie le contenu sous forme de réponse.

Automatisation et mise à l'échelle

Pour automatiser le déploiement de contenu statique à l'aide de cette approche, créez des pipelines CI/CD pour mettre à jour les compartiments Amazon S3 hébergeant des sites Web.

La fonction Lambda s'adapte automatiquement pour gérer les demandes simultanées, dans les limites des quotas et des limites du service. Pour plus d'informations, consultez la section Dimensionnement des fonctions Lambda et quotas Lambda (documentation Lambda). Pour les autres services et fonctionnalités AWS, tels que CloudFront l'Application Load Balancer, AWS les adapte automatiquement.

Outils

- Amazon CloudFront accélère la diffusion de votre contenu Web en le diffusant via un réseau mondial de centres de données, ce qui réduit le temps de latence et améliore les performances.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Dans ce modèle, vous utilisez un Application Load Balancer provisionné via Elastic Load Balancing pour diriger le trafic vers la fonction Lambda.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Épopées

CloudFront À utiliser pour diffuser du contenu statique depuis Amazon S3 via un VPC

Tâche	Description	Compétences requises
Créez un VPC.	Créez un VPC pour héberger les ressources déployées selon ce modèle, telles que l'Application Load Balancer et la fonction Lambda. Pour obtenir des instructions, consultez Create a VPC (documentation Amazon VPC).	Architecte du cloud
Créez une ACL Web AWS WAF.	Créez une ACL Web AWS WAF. Plus tard dans ce modèle, vous appliquerez cette ACL Web à la CloudFront distribution. Pour obtenir des instructions, consultez Création d'une ACL Web (documentation AWS WAF).	Architecte du cloud
Créez la fonction Lambda.	Créez la fonction Lambda qui diffuse le contenu statique hébergé dans le compartiment S3 sous forme de site Web. Utilisez le code fourni dans la section Informations supplémentaires de ce modèle. Personnalisez le code pour identifier votre compartiment S3 cible.	AWS général
Téléchargez la fonction Lambda.	Entrez la commande suivante pour télécharger le code de	AWS général

Tâche	Description	Compétences requises
	fonction Lambda dans une archive de fichiers .zip dans Lambda. `aws lambda update-function-code \ --function-name \ --zip-file fileb://lambda-alb-s3-website.zip`	
Créez un Application Load Balancer.	Créez un Application Load Balancer connecté à Internet qui pointe vers la fonction Lambda. Pour obtenir des instructions, consultez la section Création d'un groupe cible pour la fonction Lambda (documentation Elastic Load Balancing). Pour une configuration à haute disponibilité, créez l'Application Load Balancer et associez-le à des sous-réseaux privés dans différentes zones de disponibilité.	Architecte du cloud

Tâche	Description	Compétences requises
Créez une CloudFront distribution.	Créez une CloudFront distribution qui pointe vers l'Application Load Balancer que vous avez créé. 1. Connectez-vous à l'AWS Management Console et ouvrez-la sur CloudFront https://console.aws.amazon.com/cloudfront/v3/home. 2. Choisissez Create Distribution. 3. Sur la première page de l'Assistant Assistant Créer une distribution, dans la section Web, choisissez Mise en route. 4. Spécifiez les paramètres de votre distribution. Pour plus d'informations, voir Valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution. Remarques : a. Définissez l'Application Load Balancer comme origine. b. Dans les paramètres de distribution, choisissez le site Web existant ACLs que vous souhaitez appliquer via AWS WAF. Pour plus d'informations,	Architecte du cloud

Tâche	Description	Compétences requises
	consultez l'ACL Web AWS WAF. 5. Enregistrez vos modifications. 6. Après avoir CloudFront créé votre distribution, la valeur de la colonne État de votre distribution passe InProgressde Déployé. Si vous avez choisi d'activer la distribution, elle est prête pour traiter les requêtes une fois que le statut est passé à Déployé.	

Ressources connexes

Documentation AWS

- Optimisation de la mise en cache et de la disponibilité (CloudFront documentation)
- Les fonctions Lambda en tant que cibles (documentation Elastic Load Balancing)
- Quotas Lambda (documentation Lambda)

Sites Web des services AWS

- Application Load Balancer
- Lambda
- CloudFront
- Amazon S3
- AWS WAF
- Amazon VPC

Informations supplémentaires

Code

L'exemple de fonction Lambda suivant est écrit dans Node.js. Cette fonction Lambda agit comme un serveur Web qui exécute une `GetObject` opération sur un compartiment S3 contenant les ressources du site Web.

```
/**

 * This is an AWS Lambda function created for demonstration purposes.

 * It retrieves static assets from a defined Amazon S3 bucket.

 * To make the content available through a URL, use an Application Load Balancer with a
 Lambda integration.
 *
 * Set the S3_BUCKET environment variable in the Lambda function definition.
 */

var AWS = require('aws-sdk');

exports.handler = function(event, context, callback) {

    var bucket = process.env.S3_BUCKET;
    var key = event.path.replace('/', '');

    if (key == '') {
        key = 'index.html';
    }

    // Fetch from S3
    var s3 = new AWS.S3();
    return s3.getObject({Bucket: bucket, Key: key},
       function(err, data) {

            if (err) {
                return err;
            }

            var isBase64Encoded = false;
            var encoding = 'utf8';
```

```
            if (data.ContentType.indexOf('image/') > -1) {
                isBase64Encoded = true;
                encoding = 'base64'
            }

            var resp = {
                statusCode: 200,
                headers: {
                    'Content-Type': data.ContentType,
                },
                body: new Buffer(data.Body).toString(encoding),
                isBase64Encoded: isBase64Encoded
            };

            callback(null, resp);
        }
    );
};
```

Plus de modèles

- Consultez une CloudFront distribution Amazon pour la journalisation des accès, les versions HTTPS et TLS
- Déployez une application basée sur GRPC sur un cluster Amazon EKS et accédez-y à l'aide d'un Application Load Balancer
- Déployez des contrôles d'accès préventifs basés sur les attributs pour les sous-réseaux publics
- Déployez des ressources dans une AWS Wavelength zone à l'aide de Terraform
- Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform
- Configuration d'un routeur cellulaire sans serveur pour une architecture basée sur les cellules
- Utilisez Amazon Q Developer comme assistant de codage pour augmenter votre productivité
- Consultez les journaux et les statistiques d'AWS Network Firewall à l'aide de Splunk

Bases de données et stockage

Rubriques

- Bases de données
- Stockage et sauvegarde

Bases de données

Rubriques

- Accédez aux tables Microsoft SQL Server locales depuis Microsoft SQL Server sur Amazon à EC2 l'aide de serveurs liés
- Ajoutez HA à Oracle PeopleSoft sur Amazon RDS Custom à l'aide d'une réplique en lecture
- Évaluez les performances des requêtes pour la migration des bases de données SQL Server vers MongoDB Atlas sur AWS
- Automatisez les déploiements bleu/vert des bases de données mondiales Amazon Aurora en utilisant les principes de l'IaC
- Automatisez les tâches de base de données dans l'édition SQL Server Express exécutée sur Amazon à EC2 l'aide AWS Lambda d'un planificateur de tâches
- Automatisez le basculement et le retour en arrière entre régions à l'aide de DR Orchestrator Framework
- Automatisez la réplication des instances Amazon RDS sur Comptes AWS
- Sauvegardez automatiquement les bases de données SAP HANA à l'aide de Systems Manager et EventBridge
- Générez automatiquement un modèle PynamoDB et des fonctions CRUD pour Amazon DynamoDB à l'aide d'une application Python
- Bloquez l'accès public à Amazon RDS à l'aide de Cloud Custodian
- Configuration de l'accès intercompte à Amazon DynamoDB
- Configurer le routage en lecture seule dans un groupe de disponibilité Always On dans SQL Server sur AWS
- Connectez-vous en utilisant un tunnel SSH dans pgAdmin
- Convertir les requêtes Oracle JSON en SQL de base de données PostgreSQL
- Copiez les tables Amazon DynamoDB entre les comptes à l'aide de AWS Backup
- Copiez les tables Amazon DynamoDB entre les comptes à l'aide d'une implémentation personnalisée
- Créez des rapports détaillés sur les coûts et l'utilisation pour Amazon RDS et Amazon Aurora
- Déployez des instances de cluster de basculement SQL Server sur Amazon EC2 et Amazon à l'aide FSx de Terraform
- Émuler des charges de travail Oracle RAC à l'aide de points de terminaison personnalisés dans Aurora PostgreSQL

- Activer les connexions chiffrées pour les instances de base de données PostgreSQL dans Amazon RDS
- Chiffrer une instance de base de données Amazon RDS pour PostgreSQL existante
- Appliquer le balisage automatique des bases de données Amazon RDS au lancement
- Estimation du coût d'une table DynamoDB pour une capacité à la demande
- Estimation des coûts de stockage pour une table Amazon DynamoDB
- Estimez la taille du moteur Amazon RDS pour une base de données Oracle à l'aide des rapports AWR
- Exportez les tables Amazon RDS for SQL Server vers un compartiment S3 à l'aide d'AWS DMS
- Gérer les blocs anonymes dans les instructions Dynamic SQL dans Aurora PostgreSQL
- Gérez les fonctions Oracle surchargées dans la compatibilité avec Aurora PostgreSQL
- Aidez à appliquer le balisage DynamoDB
- Mettre en œuvre la reprise après sinistre entre régions avec AWS DMS et Amazon Aurora
- Migrer les fonctions et procédures Oracle comportant plus de 100 arguments vers PostgreSQL
- Migrer les instances de base de données Amazon RDS for Oracle vers d'autres comptes utilisant AMS
- Migrer les variables de liaison Oracle OUT vers une base de données PostgreSQL
- Migrez SAP HANA vers AWS à l'aide de SAP HSR avec le même nom d'hôte
- Migrer SQL Server vers AWS à l'aide de groupes de disponibilité distribués
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for Oracle à l'aide d'AWS DMS SharePlex
- Surveillez Amazon Aurora pour détecter les instances sans chiffrement
- Surveillez GoldenGate les journaux Oracle à l'aide d'Amazon CloudWatch
- Replateformage d'Oracle Database Enterprise Edition vers l'édition Standard 2 sur Amazon RDS for Oracle
- Répliquez des bases de données mainframe sur AWS à l'aide de Precisely Connect
- Planifiez des tâches pour Amazon RDS for PostgreSQL et Aurora PostgreSQL à l'aide de Lambda et Secrets Manager
- Envoyer des notifications pour une instance de base de données Amazon RDS for SQL Server à l'aide d'un serveur SMTP sur site et de Database Mail
- Configuration de la reprise après sinistre pour SAP sur IBM Db2 on AWS
- Configurer un pipeline CI/CD pour la migration de base de données à l'aide de Terraform

- Configuration d'une architecture HA/DR pour Oracle E-Business Suite sur Amazon RDS Custom avec une base de données de secours active
- Configurer la réplication des données entre Amazon RDS for MySQL et MySQL sur EC2 Amazon à l'aide de GTID
- Rôles de transition pour une PeopleSoft application Oracle sur Amazon RDS Custom for Oracle
- Déchargez les données d'un cluster Amazon Redshift entre différents comptes vers Amazon S3
- Modèles de migration de base de données par charge de travail
- Plus de modèles

Accédez aux tables Microsoft SQL Server locales depuis Microsoft SQL Server sur Amazon à EC2 l'aide de serveurs liés

Créée par Tirumala Dasari (AWS) et Eduardo Valentim (AWS)

Récapitulatif

Ce modèle décrit comment accéder aux tables de base de données Microsoft SQL Server locales exécutées sous Microsoft Windows, à partir de bases de données Microsoft SQL Server exécutées ou hébergées sur des instances Windows ou Linux Amazon Elastic Compute Cloud (Amazon EC2) à l'aide de serveurs liés.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Amazon EC2 avec Microsoft SQL Server exécuté sur l'AMI Amazon Linux (Amazon Machine Image)
- AWS Direct Connect entre le serveur Microsoft SQL Server (Windows) sur site et l'instance Windows ou Linux EC2

Versions du produit

- SQL Server 2016 ou version ultérieure

Architecture

Pile technologique source

- Base de données Microsoft SQL Server locale exécutée sous Windows
- Amazon EC2 avec Microsoft SQL Server exécuté sur une AMI Windows ou une AMI Linux

Pile technologique cible

- Amazon EC2 avec Microsoft SQL Server exécuté sur l'AMI Amazon Linux
- Amazon EC2 avec Microsoft SQL Server exécuté sur une AMI Windows

Architecture de base de données source et cible

Outils

- Microsoft SQL Server Management Studio (SSMS) est un environnement intégré permettant de gérer une infrastructure SQL Server. Il fournit une interface utilisateur et un groupe d'outils dotés d'éditeurs de script riches qui interagissent avec SQL Server.

Épopées

Changer le mode d'authentification en Windows pour SQL Server dans Windows SQL Server

Tâche	Description	Compétences requises
Connectez-vous à Windows SQL Server via SSMS.		DBA
Changez le mode d'authentification en Windows dans SQL Server à partir du menu contextuel (clic droit) de l'instance Windows SQL Server.		DBA

Redémarrez le service Windows MSSQL

Tâche	Description	Compétences requises
Redémarrez le service SQL.	1. Dans l'explorateur d'objets SSMS, choisissez l'instance SQL Server. 2. Ouvrez le menu contextuel (clic droit). 3. Choisissez Redémarrer.	DBA

Créez un nouvel identifiant et choisissez les bases de données auxquelles accéder dans Windows SQL Server

Tâche	Description	Compétences requises
Dans l'onglet Sécurité, ouvrez le menu contextuel (clic droit) de Connexion et sélectionnez une nouvelle connexion.		DBA
Dans l'onglet Général, choisissez l'authentification SQL Server, entrez un nom d'utilisateur, entrez le mot de passe, puis confirmez le mot de passe et désactivez l'option permettant de modifier le mot de passe lors de la prochaine connexion.		DBA
Dans l'onglet Rôles du serveur, sélectionnez Public.		DBA
Dans l'onglet User Mapping, choisissez la base de données et le schéma auxquels vous souhaitez accéder, puis surlignez la base de données pour sélectionner les rôles de base de données.	Sélectionnez public et db_datareader pour accéder aux données des tables de base de données.	DBA
Cliquez sur OK pour créer un utilisateur.		DBA

Ajouter l'adresse IP de Windows SQL Server au fichier hôte de Linux SQL Server

Tâche	Description	Compétences requises
Connectez-vous à la boîte Linux SQL Server via la fenêtre du terminal.		DBA
Ouvrez the /etc/hosts le fichier et ajoutez l'adresse IP de la machine Windows avec SQL Server.		DBA
Enregistrez le fichier hosts.		DBA

Créer un serveur lié sur Linux SQL Server

Tâche	Description	Compétences requises
Créez un serveur lié à l'aide des procédures stockées master.sys.sp_addlinkedserver et master.dbo.sp_addlinkedsrvlogin.	Pour plus d'informations sur l'utilisation de ces procédures stockées, consultez la section Informations supplémentaires.	DBA, Développeur

Vérifiez le serveur lié et les bases de données créés dans SSMS

Tâche	Description	Compétences requises
Dans Linux SQL Server in SSMS, accédez à Linked Servers et actualisez.		DBA
Développez les serveurs liés et les catalogues créés dans le volet de gauche.	Vous verrez les bases de données SQL Server sélection	DBA

Tâche	Description	Compétences requises
	nées avec des tables et des vues.	

Vérifiez que vous pouvez accéder aux tables de base de données Windows SQL Server

Tâche	Description	Compétences requises
Dans la fenêtre de requête SSMS, exécutez la requête : « select top 3 * from [sqllin] .dms_sample_win.dbo.mlb_data ».	Notez que la clause FROM utilise une syntaxe en quatre parties : computer. database.schema.table (par exemple, SELECT name « SQL2 databases » FROM [sqllin] .master.sys.databases). Dans notre exemple, nous avons créé un alias pour SQL2 dans le fichier hosts, vous n'avez donc pas besoin de saisir le nom NetBIOS réel entre crochets. Si vous utilisez les noms NetBIOS réels, notez qu'AWS utilise par défaut des noms NetBIOS tels que Win-XXXX, et que SQL Server exige des crochets pour les noms marqués de tirets.	DBA, Développeur

Ressources connexes

- Notes de mise à jour pour SQL Server sous Linux

Informations supplémentaires

Utilisation de procédures stockées pour créer des serveurs liés

SSMS ne prend pas en charge la création de serveurs liés pour Linux SQL Server. Vous devez donc utiliser les procédures stockées suivantes pour les créer :

```
EXEC master.sys.sp_addlinkedserver @server= N'SQLLIN' , @srvproduct= N'SQL Server'
EXEC master.dbo.sp_addlinkedsrvlogin
 @rmtsrvname=N'SQLLIN',@useself=N'False',@locallogin=NULL,@rmtuser=N'username',@rmtpassword='Te
```

Remarque 1 : Entrez les informations de connexion que vous avez créées précédemment dans Windows SQL Server dans la procédure `master.dbo.sp_addlinkedsrvlogin` stockée.

Remarque 2 : `@server` le nom `SQLLIN` et le nom d'entrée du fichier hôte `172.12.12.4 SQLLIN` doivent être identiques.

Vous pouvez utiliser ce processus pour créer des serveurs liés pour les scénarios suivants :

- Linux SQL Server vers Windows SQL Server via un serveur lié (comme spécifié dans ce modèle)
- Windows SQL Server vers Linux SQL Server via un serveur lié
- Linux SQL Server vers un autre Linux SQL Server via un serveur lié

Ajoutez HA à Oracle PeopleSoft sur Amazon RDS Custom à l'aide d'une réplique en lecture

Créée par sampath kathirvel (AWS)

Récapitulatif

Pour exécuter la solution de planification des ressources PeopleSoft d'entreprise (ERP) Oracle sur Amazon Web Services (AWS), vous pouvez utiliser Amazon Relational Database Service (Amazon RDS) ou Amazon RDS Custom pour Oracle, qui prend en charge les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents. Pour connaître les principaux facteurs à prendre en compte lors de la planification d'une migration, consultez les stratégies de migration des bases de données Oracle dans AWS Prescriptive Guidance.

Au moment d'écrire ces lignes, RDS Custom for Oracle ne prend pas en charge l'option multi-AZ, qui est disponible pour Amazon RDS for Oracle en tant que solution HA utilisant la réplication du stockage. Ce modèle permet plutôt d'atteindre la haute disponibilité en utilisant une base de données de secours qui crée et gère une copie physique de la base de données principale. Le modèle se concentre sur les étapes à suivre pour exécuter une base de données d' PeopleSoft applications sur Amazon RDS Custom avec HA en utilisant Oracle Data Guard pour configurer une réplique en lecture.

Ce modèle fait également passer la réplique en lecture seule en mode lecture seule. Le fait d'avoir votre réplique en lecture seule présente des avantages supplémentaires :

- Décharger les charges de travail en lecture seule de la base de données principale
- Activation de la réparation automatique des blocs corrompus en récupérant les blocs sains de la base de données de secours à l'aide de la fonction Oracle Active Data Guard
- Utilisation de la fonctionnalité Far Sync pour maintenir la synchronisation de la base de données de secours distante sans la surcharge de performances associée à la transmission de journaux redo sur de longues distances.

L'utilisation d'une réplique en mode lecture seule nécessite l'option Oracle Active Data Guard, qui entraîne un coût supplémentaire car il s'agit d'une fonctionnalité sous licence séparée d'Oracle Database Enterprise Edition.

Conditions préalables et limitations

Prérequis

- Une PeopleSoft application existante sur Amazon RDS Custom. Si vous n'avez pas d'application, consultez le modèle Migrate Oracle PeopleSoft to Amazon RDS Custom.
- Un seul niveau PeopleSoft d'application. Toutefois, vous pouvez adapter ce modèle pour qu'il fonctionne avec plusieurs niveaux d'application.
- Amazon RDS Custom configuré avec au moins 8 Go d'espace de swap.
- Une licence de base de données Oracle Active Data Guard permettant de convertir la réplique en lecture seule en mode lecture seule et de l'utiliser pour transférer les tâches de reporting vers le mode veille. Pour plus d'informations, consultez la liste des prix commerciaux d'Oracle Technology.

Limites

- Limitations générales et configurations non prises en charge pour RDS Custom pour Oracle
- Limitations associées aux répliques de lecture Amazon RDS Custom for Oracle

Versions du produit

- Pour les versions de base de données Oracle prises en charge par Amazon RDS Custom, consultez RDS Custom pour Oracle.
- Pour les classes d'instance de base de données Oracle prises en charge par Amazon RDS Custom, consultez la section Support des classes d'instance de base de données pour RDS Custom pour Oracle.

Architecture

Pile technologique cible

- Amazon RDS Custom for Oracle
- AWS Secrets Manager
- Oracle Active Data Guard
- PeopleSoft Application Oracle

Architecture cible

Le schéma suivant montre une instance de base de données Amazon RDS Custom et une réplique de lecture Amazon RDS Custom. La réplique en lecture utilise Oracle Active Data Guard pour être répliquée vers une autre zone de disponibilité. Vous pouvez également utiliser la réplique de lecture pour décharger le trafic de lecture sur la base de données principale et à des fins de création de rapports.

Pour une architecture représentative utilisant Oracle PeopleSoft sur AWS, voir Configurer une PeopleSoft architecture hautement disponible sur AWS.

Outils

Services AWS

- Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Dans ce modèle, vous pouvez récupérer les mots de passe des utilisateurs de base de données depuis Secrets Manager pour `RDS_DATAGUARD` lesquels le nom du secret est indiqué`do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Autres outils

- Oracle Data Guard vous aide à créer, maintenir, gérer et surveiller des bases de données de secours.

Bonnes pratiques

Pour atteindre l'objectif de zéro perte de données (RPO=0), utilisez le mode de protection `MaxAvailability` Data Guard, avec le `SYNC+NOAFFIRM` paramètre Redo Transport pour de meilleures performances. Pour plus d'informations sur la sélection du mode de protection de base de données, consultez la section Informations supplémentaires.

Épopées

Création de la réplique lue

Tâche	Description	Compétences requises
Créez la réplique lue.	Pour créer une réplique en lecture de l'instance de base de données personnalisée Amazon RDS, suivez les instructions de la documentation Amazon RDS et utilisez l'instance de base de données personnalisée Amazon RDS que vous avez créée (voir la section Conditions préalables) comme base de données source. Par défaut, la réplique de lecture personnalisée Amazon RDS est créée en tant que support physique et est à l'état monté. Cela est intentionnel pour garantir la conformité avec la licence Oracle Active Data Guard. Ce modèle inclut du code pour configurer une base de données de conteneurs multilocataires (CDB) ou une instance non CDB.	DBA

Changez le mode de protection d'Oracle Data Guard en MaxAvailability

Tâche	Description	Compétences requises
Accédez à la configuration du broker Data Guard sur la base de données principale.	Dans cet exemple, la réplique de lecture personnalisée Amazon RDS est `RDS_CUSTOM_ORCL_D` destinée à l'instance non CDB et `RDS_CUSTOM_RDSCDB_B` à l'instance CDB. Les bases de données pour les bases de données non CDB sont `orcl_a` (principale) et `orcl_d` (de secours). Les noms de base de données pour CDB sont `rdscdb_a` (principal) et `rdscdb_b` (de secours). Vous pouvez vous connecter à la réplique de lecture personnalisée RDS directement ou via la base de données principale. Le nom du service réseau de votre base de données se trouve dans le `tnsnames.ora` fichier situé dans le `$ORACLE_HOME/network/admin` répertoire. RDS Custom for Oracle renseigne automatiquement ces entrées pour votre base de données principale et vos répliques de lecture.	DBA

Tâche	Description	Compétences requises

	Le mot de passe de l'`RDS_DATAGUARD` utilisateur est stocké dans AWS Secrets Manager, avec un nom secret`do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`. Pour plus d'informations sur la façon de se connecter à une instance personnalisée RDS à l'aide de la clé SSH (Secure Shell) extraite de Secrets Manager, consultez Connexion à votre instance de base de données personnalisée RDS à l'aide de SSH.
	
	Pour accéder à la configuration du broker Oracle Data Guard via la ligne de commande Data Guard (`dgmgrl`), utilisez le code suivant.
	
	Non CDB
	
	`$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_D`
	`DGMGRL for Linux:`
	`Release 19.0.0.0.0 -`
	`Production on Fri Sep`
	`30 22:44:49 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982,`
	`2019, Oracle and/or its`	

Tâche	Description	Compétences requises
	affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 11.00 KByte/s Instance(s): ORCL SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 20:24:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its	

Tâche	Description	Compétences requises
	affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG. DGMGRL> DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL>	

Tâche	Description	Compétences requises

Modifiez le paramètre de transport du journal en vous connectant à DGMGRL depuis le nœud principal.	Changez le mode de transport du journal en`FastSync`, correspondant au paramètre `SYNC+NOAFFIRM` de rétablissement du transport. Pour vous assurer que vous disposez de paramètres valides après le changemen t de rôle, modifiez-les à la fois pour la base de données principale et pour la base de données de secours.
	
	Non CDB
	
	`DGMGRL>`
	`DGMGRL> edit database orcl_d set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_d LogXptMode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL> edit database orcl_a set property logxptmode=fastsync;`
	`Property "logxptmode" updated`
	`DGMGRL> show database orcl_a logxptmode;`
	`LogXptMode = 'fastsync'`
	`DGMGRL>`
	
	CDB
		DBA

Tâche	Description	Compétences requises
	`DGMGRL> edit database rdscdb_b set property logxptmode=fastsync;DGMGRL> edit database rdscdb_b set property logxptmode=fastsync;Property "logxptmode" updated DGMGRL> show database rdscdb_b LogXptMode; LogXptMode = 'fastsync' DGMGRL> edit database rdscdb_a set property logxptmode=fastsync;Property "logxptmode" updated DGMGRL> show database rdscdb_a logxptmode; LogXptMode = 'fastsync' DGMGRL>`	

Tâche	Description	Compétences requises

Changez le mode de protection en MaxAvailability.	Changez le mode de protection `MaxAvailability` en vous connectant `DGMGRL` depuis le nœud principal.
	
	Non CDB
	
	`DGMGRL> edit configuration set protection mode as maxavailability;`
	`Succeeded.`
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 38 seconds ago)`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`rdscdb_a - Primary database`
		DBA

Tâche	Description	Compétences requises
	rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL>	

Changez le statut de la réplique de montage à lecture seule et activez Redo Apply

Tâche	Description	Compétences requises
Arrêtez Redo Apply pour la base de données de secours.	La réplique de lecture est créée en MOUNT mode par défaut. Pour l'ouvrir en mode lecture seule, vous devez d'abord désactiver la fonction Redo Apply en vous connectant DGMGRL depuis le nœud principal ou le nœud de secours. Non CDB DGMGRL> show database orcl_dDGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago)	DBA

Tâche	Description	Compétences requises
	Average Apply Rate: 11.00 KByte/s Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL> edit database orcl_d set state=app ly-off; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY- OFF Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 42 seconds (computed 1 second ago) Average Apply Rate: (unknown) Real Time Query: OFF Instance(s): ORCL Database Status: SUCCESS DGMGRL>	
	CDB DGMGRL> show configura tionDGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members:	

Tâche	Description	Compétences requises
	rdscdb_a - Primary database rdscdb_b - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 57 seconds ago) DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 2.00 KByte/s Real Time Query: OFF Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> edit database rdscdb_b set state=apply-off; Succeeded. DGMGRL> show database rdscdb_b; Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-OFF	

Tâche	Description	Compétences requises

	``
	  Transport Lag:
	0 seconds (computed 1
	second ago)
	  Apply Lag:
	0 seconds (computed 1
	second ago)
	  Average Apply Rate:
	(unknown)
	  Real Time Query:
	OFF
	  Instance(s):
	    RDSCDB
	Database Status:
	SUCCESS
	``	

Tâche	Description	Compétences requises
Ouvrez l'instance de réplique en lecture seule.	Connectez-vous à la base de données de secours à l'aide de l'entrée TNS et ouvrez-la en mode lecture seule en vous y connectant depuis le nœud principal ou de secours. Non CDB `$ sqlplus RDS_DATAG UARD@RDS_CUSTOM_OR CL_D as sysdg -bash-4.2$ sqlplus RDS_DATAGUARD@RDS_ CUSTOM_ORCL_D as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Fri Sep 30 23:00:14 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2020, Oracle. All rights reserved. Enter password: Last Successful login time: Fri Sep 30 2022 22:48:27 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.10.0.0.0 SQL> select open_mode from v$database; OPEN_MODE -------------------- MOUNTED SQL> alter database open read only;`	DBA

Tâche	Description	Compétences requises
	Database altered. SQL> select open_mode from v$database; OPEN_MODE -------------------- READ ONLY SQL> CDB -bash-4.2$ sqlplus C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_B as sysdg SQL*Plus: Release 19.0.0.0.0 - Productio n on Wed Jan 11 21:14:07 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2022, Oracle. All rights reserved. Enter password: Last Successful login time: Wed Jan 11 2023 21:12:05 +00:00 Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production Version 19.16.0.0.0 SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- RDSCDB MOUNTED SQL> alter database open read only; Database altered.	

Tâche	Description	Compétences requises
	SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- ---------- ----------- RDSCDB READ ONLY SQL>	

Tâche	Description	Compétences requises
Activez Redo Apply sur l'instance de réplique lue.	Activez Redo Apply sur l'instance de réplique en lecture en utilisant DGMGR L depuis le nœud principal ou de secours. Non CDB `$ dgmgrl RDS_DATAG UARD@RDS_CUSTOM_OR CL_D DGMGRL for Linux: Release 19.0.0.0.0 - Production on Fri Sep 30 23:02:16 2022 Version 19.10.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "ORCL_D" Connected as SYSDG. DGMGRL> edit database orcl_d set state=apply-on; DGMGRL> edit database orcl_d set state=app ly-on; Succeeded. DGMGRL> show database orcl_d Database - orcl_d Role: PHYSICAL STANDBY Intended State: APPLY-ON`	DBA

Tâche	Description	Compétences requises
	Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 496.00 KByte/s Real Time Query: ON Instance(s): ORCL Database Status: SUCCESS DGMGRL> CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B -bash-4.2$ dgmgrl C##RDS_DATAGUARD@RDS_CUSTOM_RDSCDB_B DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 11 21:21:11 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for information. Password: Connected to "RDSCDB_B" Connected as SYSDG.	

Tâche	Description	Compétences requises
	DGMGRL> edit database rdscdb_b set state=apply-on; Succeeded. DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Average Apply Rate: 35.00 KByte/s Real Time Query: ON Instance(s): RDSCDB Database Status: SUCCESS DGMGRL> show database rdscdb_b Database - rdscdb_b Role: PHYSICAL STANDBY Intended State: APPLY-ON Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Average Apply Rate: 16.00 KByte/s Real Time Query: ON Instance(s): RDSCDB	

Tâche	Description	Compétences requises

	`Database Status:`
	`SUCCESS`
	`DGMGRL>`	

Ressources connexes

- Configuration d'Amazon RDS en tant que PeopleSoft base de données Oracle (livre blanc AWS)
- Guide Oracle Data Guard Broker (documentation de référence Oracle)
- Concepts et administration de Data Guard (documentation de référence Oracle)

Informations supplémentaires

Sélectionnez le mode de protection de votre base de données

Oracle Data Guard propose trois modes de protection pour configurer votre environnement Data Guard en fonction de vos exigences en matière de disponibilité, de protection et de performances. Le tableau suivant récapitule ces trois modes.

Mode de protection	Refaire le réglage du transport	Description
PERFORMANCE MAXIMALE	`ASYNC`	Pour les transactions effectuées sur la base de données principale, les données de rétablissement sont transmises de manière asynchrone et écrites dans le journal de rétablissement de la base de données de secours. Par conséquent, l'impact sur les performances est minime. `MaxPerformance` Impossible de fournir RPO=0 en raison

		de l'expédition asynchrone des journaux.
PROTECTION MAXIMALE	`SYNC+AFFIRM`	Pour les transactions sur la base de données principale, les données de rétablissement sont transmises de manière synchrone et écrites dans le journal de rétablissement de la base de données de secours sur disque avant que la transaction ne soit reconnue. Si la base de données de secours devient indisponible, la base de données principal e s'arrête d'elle-même pour garantir la protection des transactions.
DISPONIBILITÉ MAXIMALE	`SYNC+AFFIRM`	Ceci est similaire au `MaxProtection` mode, sauf lorsqu'aucun accusé de réception n'est reçu de la base de données de secours. Dans ce cas, il fonctionne comme s'il était en `MaxPerfor mance` mode permettant de préserver la disponibilité de la base de données principale jusqu'à ce qu'il soit à nouveau en mesure d'écrire son flux de restauration dans une base de données de secours synchroni sée.

SYNC+NOAFFIRM	Pour les transactions sur la base de données principale, le rétablissement est transmis de manière synchrone à la base de données de secours, et la base attend uniquement un accusé de réception indiquant que le rétablissement a été reçu sur le serveur de secours, et non qu'il a été écrit sur le disque de secours. Ce mode, également connu sous le nom de`FastSync`, peut apporter un avantage en termes de performances au détriment de l'exposition potentielle à la perte de données dans un cas particulier de défaillances simultanées multiples.

Les répliques de lecture dans RDS Custom for Oracle sont créées avec le mode de protection maximale des performances, qui est également le mode de protection par défaut pour Oracle Data Guard. Le mode de performance maximale a le plus faible impact sur les performances de la base de données principale, ce qui peut vous aider à atteindre l'objectif de point de restauration (RPO) mesuré en secondes.

Pour atteindre l'objectif de zéro perte de données (RPO=0), vous pouvez personnaliser le mode de protection d'Oracle Data Guard `MaxAvailability` avec le `SYNC+NOAFFIRM` paramètre Redo Transport pour de meilleures performances. Comme les validations sur la base de données principale ne sont reconnues qu'une fois que les vecteurs de rétablissement correspondants ont été transmis avec succès à la base de données de secours, la latence du réseau entre l'instance principale et la réplique peut être cruciale pour les charges de travail sensibles aux validations. Nous vous recommandons d'effectuer des tests de charge pour votre charge de travail afin d'évaluer l'impact sur les performances lorsque la réplique en lecture est personnalisée pour s'exécuter en `MaxAvailability` mode.

Le déploiement de la réplique en lecture dans la même zone de disponibilité que la base de données principale permet de réduire la latence du réseau par rapport au déploiement de la réplique en lecture dans une autre zone de disponibilité. Cependant, le déploiement des répliques principale et en lecture dans la même zone de disponibilité peut ne pas répondre à vos exigences en matière de haute disponibilité car, dans le cas peu probable d'une indisponibilité de la zone de disponibilité, l'instance principale et l'instance de réplique en lecture sont affectées.

Évaluez les performances des requêtes pour la migration des bases de données SQL Server vers MongoDB Atlas sur AWS

Créée par Battulga Purevragchaa (AWS), Krishnakumar PeerIslands Sathyanarayana (US Inc) et Babu Srinivasan (MongoDB)

Récapitulatif

Ce modèle fournit des conseils pour charger MongoDB avec des données quasiment réelles et évaluer les performances des requêtes MongoDB aussi proches que possible du scénario de production. L'évaluation fournit des informations pour vous aider à planifier votre migration vers MongoDB à partir d'une base de données relationnelle. Le modèle utilise le générateur de données de PeerIslands test et l'analyseur de performances pour tester les performances des requêtes.

Ce modèle est particulièrement utile pour la migration de Microsoft SQL Server vers MongoDB, car l'exécution de transformations de schéma et le chargement de données à partir d'instances SQL Server actuelles vers MongoDB peuvent s'avérer très complexes. Au lieu de cela, vous pouvez charger des données quasiment réelles dans MongoDB, comprendre les performances de MongoDB et peaufiner la conception du schéma avant de commencer la migration proprement dite.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Connaissance de MongoDB Atlas
- Schéma MongoDB cible
- Modèles de requête typiques

Limites

- Les temps de chargement des données et les performances seront limités par la taille de l'instance du cluster MongoDB. Nous vous recommandons de choisir des instances recommandées pour une utilisation en production afin de comprendre les performances réelles.
- PeerIslands Le générateur de données de test et l'analyseur de performances ne prennent actuellement en charge que les chargements de données et les requêtes en ligne. Le traitement par lots hors ligne (par exemple, le chargement de données dans MongoDB à l'aide de connecteurs Spark) n'est pas encore pris en charge.

- PeerIslands Le générateur de données de test et l'analyseur de performances prennent en charge les relations de terrain au sein d'une collection. Il ne prend pas en charge les relations entre les collections.

Éditions de produits

- Ce modèle prend en charge MongoDB Atlas et MongoDB Enterprise Advanced.

Architecture

Pile technologique cible

- MongoDB Atlas ou MongoDB Enterprise Advanced

Architecture

PeerIslands Le générateur de données de test et l'analyseur de performances sont conçus à l'aide de Java et d'Angular, et stockent les données générées sur Amazon Elastic Block Store (Amazon EBS). L'outil comprend deux flux de travail : la génération de données de test et les tests de performance.

- Lors de la génération de données de test, vous créez un modèle, qui est la représentation JSON du modèle de données à générer. Après avoir créé le modèle, vous pouvez générer les données dans une collection cible, telle que définie par la configuration de génération de charge.
- Lors des tests de performance, vous créez un profil. Un profil est un scénario de test en plusieurs étapes dans lequel vous pouvez configurer les opérations de création, de lecture, de mise à jour et de suppression (CRUD), les pipelines d'agrégation, le poids de chaque opération et la durée de chaque étape. Après avoir créé le profil, vous pouvez exécuter des tests de performance sur la base de données cible en fonction de la configuration.

PeerIslands Le générateur de données de test et l'analyseur de performances stockent leurs données sur Amazon EBS. Vous pouvez donc connecter Amazon EBS à MongoDB en utilisant n'importe quel mécanisme de connexion pris en charge par MongoDB, notamment le peering, les listes d'autorisation et les points de terminaison privés. Par défaut, l'outil n'inclut pas de composants opérationnels ; toutefois, il peut être configuré avec Amazon Managed Service for Prometheus, Amazon Managed Grafana CloudWatch, Amazon et AWS Secrets Manager si nécessaire.

Outils

- PeerIslands Le générateur de données de test et l'analyseur de performances incluent deux composants. Le composant Test Data Generator vous aide à générer des données réelles très spécifiques au client en fonction de votre schéma MongoDB. L'outil est entièrement piloté par l'interface utilisateur avec une riche bibliothèque de données et peut être utilisé pour générer rapidement des milliards d'enregistrements sur MongoDB. L'outil fournit également des fonctionnalités permettant d'implémenter des relations entre les champs du schéma MongoDB. Le composant Performance Analyzer vous permet de générer des requêtes et des agrégations très spécifiques au client, et de réaliser des tests de performances réalistes sur MongoDB. Vous pouvez utiliser l'analyseur de performances pour tester les performances de MongoDB à l'aide de profils de charge complets et de requêtes paramétrées pour votre cas d'utilisation spécifique.

Bonnes pratiques

Consultez les ressources suivantes :

- Meilleures pratiques de conception de schémas MongoDB (site Web du développeur MongoDB)
- Bonnes pratiques de déploiement de MongoDB Atlas sur AWS (site Web MongoDB)
- Connexion sécurisée d'applications à un plan de données MongoDB Atlas avec AWS (article de blog PrivateLink AWS)
- Guide des meilleures pratiques pour les performances de MongoDB (site Web de MongoDB)

Épopées

Comprenez vos données sources

Tâche	Description	Compétences requises
Comprenez l'encombrement de la base de données de la source SQL Server actuelle.	Comprenez votre empreinte actuelle sur SQL Server. Cela peut être réalisé en exécutant des requêtes sur le `INFORMATION` schéma de la base de données. Déterminez le nombre de tables et la taille	DBA

Tâche	Description	Compétences requises
	de chaque table. Analysez l'index associé à chaque table. Pour plus d'informations sur l'analyse SQL, consultez le billet de blog SQL2Mongo : Data Migration Journey sur le PeerIslands site Web.	
Comprenez le schéma source.	Déterminez le schéma de table et la représentation commerciale des données (par exemple, les codes postaux, les noms et les devises). Utilisez votre diagramme de relation entre entités (ER) existant ou générez le diagramme ER à partir de la base de données existante. Pour plus d'informations, consultez le billet de blog SQL2Mongo : Data Migration Journey sur le PeerIslands site Web.	DBA

Tâche	Description	Compétences requises
Comprenez les modèles de requêtes.	Documentez les 10 principal es requêtes SQL que vous utilisez. Vous pouvez utiliser les tables performan ce_schema.events_statements _summary_by_digest disponibl es dans la base de données pour comprendre les principal es requêtes. Pour plus d'informations, consultez le billet de blog SQL2Mongo : Data Migration Journey sur le PeerIslands site Web.	DBA
Comprenez les engagements en matière de SLA.	Documentez les accords de niveau de service cibles (SLAs) pour les opération s de base de données. Les mesures typiques incluent la latence des requêtes et les requêtes par seconde. Les mesures et leurs cibles sont généralement disponibles dans des documents relatifs aux exigences non fonctionn elles (NFR).	DBA

Définir le schéma MongoDB

Tâche	Description	Compétences requises
Définissez le schéma cible.	Définissez différentes options pour le schéma MongoDB cible. Pour plus d'informa	Ingénieur MongoDB

Tâche	Description	Compétences requises
	tions, consultez la section Schémas dans la documenta tion de l'atlas MongoDB. Tenez compte des meilleure s pratiques et des modèles de conception basés sur les relations entre les tables. Consultez les exemples et modèles de modèles de données dans la documenta tion de MongoDB pour plus de détails.	
Définissez les modèles de requêtes cibles.	Définissez les requêtes MongoDB et les pipelines d'agrégation. Ces requêtes sont l'équivalent des principal es requêtes que vous avez capturées pour votre charge de travail SQL Server. Pour comprendre comment créer des pipelines d'agrégation MongoDB, consultez la documentation MongoDB.	Ingénieur MongoDB
Définissez le type d'instance MongoDB.	Déterminez la taille de l'instance que vous prévoyez d'utiliser pour les tests. Pour obtenir des conseils, consultez la documentation de MongoDB.	Ingénieur MongoDB

Préparation de la base de données cible

Tâche	Description	Compétences requises
Configurez le cluster MongoDB Atlas.	Pour configurer un cluster MongoDB sur AWS, suivez les instructions de la documentation MongoDB.	Ingénieur MongoDB
Créez des utilisateurs dans la base de données cible.	Configurez le cluster MongoDB Atlas pour l'accès et la sécurité du réseau en suivant les instructions de la documentation MongoDB.	Ingénieur MongoDB
Créez des rôles appropriés dans AWS et configurez le contrôle d'accès basé sur les rôles pour Atlas.	Si nécessaire, configurez des utilisateurs supplémentaires en suivant les instructions de la documentation MongoDB. Configurez l'authentification et l'autorisation via les rôles AWS.	Ingénieur MongoDB
Configurez Compass pour accéder à MongoDB Atlas.	Configurez l'utilitaire graphique MongoDB Compass pour faciliter la navigation et l'accès.	Ingénieur MongoDB

Configurer la charge de base à l'aide du générateur de données de test

Tâche	Description	Compétences requises
Installez le générateur de données de test.	Installez PeerIsland Test Data Generator dans votre environnement.	Ingénieur MongoDB

Tâche	Description	Compétences requises
Configurez le générateur de données de test pour générer les données appropriées.	Créez un modèle en utilisant la bibliothèque de données pour générer des données spécifiques pour chaque champ du schéma MongoDB. Pour plus d'informations, consultez le générateur de données et les performances MongoDB. Vidéo de l'analyseur.	Ingénieur MongoDB
Dimensionnez horizontalement le générateur de données de test pour générer la charge requise.	Utilisez le modèle que vous avez créé pour démarrer la génération de charge par rapport à la collection cible en configurant le parallélisme requis. Déterminez les délais et l'échelle nécessaires pour générer les données nécessaires.	Ingénieur MongoDB
Validez le chargement dans MongoDB Atlas.	Vérifiez les données chargées dans MongoDB Atlas.	Ingénieur MongoDB
Générez les index requis sur MongoDB.	Définissez les index selon les besoins, en fonction des modèles de requête. Pour connaître les meilleures pratiques, consultez la documentation de MongoDB.	Ingénieur MongoDB

Procéder à des tests de performance

Tâche	Description	Compétences requises
Configurez les profils de charge dans Performance Analyzer.	Créez un profil de test de performance dans Performance Analyzer en configurant des requêtes spécifiques et leur pondération, la durée du test et les étapes correspondantes. Pour plus d'informations, consultez le générateur de données et les performances MongoDB. Vidéo de l'analyseur.	Ingénieur MongoDB
Effectuez des tests de performance.	Utilisez le profil de test de performance que vous avez créé pour démarrer le test par rapport à la collection cible en configurant le parallélisme requis. Faites évoluer horizontalement l'outil de test de performance pour exécuter des requêtes sur MongoDB Atlas.	Ingénieur MongoDB
Enregistrez les résultats des tests.	Enregistrez les temps de latence P95, P99 pour les requêtes.	Ingénieur MongoDB
Ajustez votre schéma et vos modèles de requêtes.	Modifiez les index et les modèles de requêtes pour résoudre les éventuels problèmes de performances.	Ingénieur MongoDB

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.	Supprimez toutes les ressources temporaires que vous avez utilisées pour Test Data Generator et Performan ce Analyzer.	Administrateur AWS
Mettez à jour les résultats des tests de performance.	Comprenez les performan ces des requêtes MongoDB et comparez-les aux vôtres. SLAs Si nécessaire, affinez le schéma MongoDB et relancez le processus.	Ingénieur MongoDB
Conclure le projet.	Clôturez le projet et faites part de vos commentaires.	Ingénieur MongoDB

Ressources connexes

- GitHub référentiel : S3toAtlas
- Schéma : Conception du schéma MongoDB
- Pipelines d'agrégation : pipelines d'agrégation MongoDB
- Dimensionnement de l'Atlas MongoDB : sélection du niveau de dimensionnement
- Vidéo : Générateur de données MongoDB et Perf. Analyseur
- Références : documentation MongoDB
- Tutoriels : guide du développeur MongoDB, MongoDB Jumpstart
- AWS Marketplace : Atlas MongoDB sur AWS Marketplace
- Solutions pour les partenaires AWS : Atlas MongoDB sur le déploiement de référence AWS

Ressources supplémentaires :

- Analyse SQL

- Forums de la communauté des développeurs MongoDB
- Questions relatives au réglage des performances de MongoDB
- Analyses opérationnelles avec Atlas et Redshift
- Modernisation des applications avec MongoDB Atlas et AWS Elastic Beanstalk

Automatisez les déploiements bleu/vert des bases de données mondiales Amazon Aurora en utilisant les principes de l'IaC

Créée par Ishwar Chauthaiwale (AWS), ANKIT JAIN (AWS) et Ramu Jagini (AWS)

Récapitulatif

La gestion des mises à jour des bases de données, des migrations ou des efforts de dimensionnement peut s'avérer difficile pour les entreprises qui exécutent des charges de travail critiques sur les bases de données mondiales Amazon Aurora. Il est essentiel de veiller à ce que ces opérations soient effectuées de manière fluide, sans interruption de service, pour maintenir la disponibilité des services et éviter les perturbations pour vos utilisateurs.

Une blue/green deployment strategy offers a solution to this challenge by allowing you to run two identical environments concurrently: blue (the current environment) and green (the new environment). A blue/green stratégie vous permet de mettre en œuvre des modifications, d'effectuer des tests et de transférer le trafic entre les environnements avec un minimum de risques et de temps d'arrêt.

Ce modèle vous aide à automatiser le processus de déploiement bleu/vert pour les bases de données globales Aurora en utilisant les principes de l'infrastructure en tant que code (IaC). Il utilise AWS CloudFormationAWS Lambda, et Amazon Route 53 pour simplifier les déploiements bleu/vert. Pour améliorer la fiabilité, il utilise des identificateurs de transaction globaux (GTIDs) pour la réplication. La réplication basée sur le GTID offre une meilleure cohérence des données et des capacités de basculement entre les environnements par rapport à la réplication de journaux binaires (binlog).

> **Note**
>
> Ce modèle suppose que vous utilisez un cluster de base de données global Aurora MySQL Edition compatible. Si vous utilisez plutôt la version compatible avec Aurora PostgreSQL, veuillez utiliser les équivalents PostgreSQL des commandes MySQL.

En suivant les étapes de ce modèle, vous pouvez :

- Fournir une base de données globale Aurora verte : à l'aide de CloudFormation modèles, vous créez un environnement vert qui reflète votre environnement bleu existant.
- Configurer la réplication basée sur le GTID : vous configurez la réplication GTID pour que les environnements bleu et vert restent synchronisés.

- Changez de trafic en toute simplicité : vous utilisez Route 53 et Lambda pour faire passer automatiquement le trafic de l'environnement bleu à l'environnement vert après une synchronisation complète.
- Finalisation du déploiement : vous confirmez que l'environnement écologique est pleinement opérationnel en tant que base de données principale, puis vous arrêtez la réplication et nettoyez toutes les ressources temporaires.

L'approche adoptée dans ce modèle offre les avantages suivants :

- Réduit les temps d'arrêt lors des mises à jour ou des migrations critiques des bases de données : l'automatisation garantit une transition fluide entre les environnements avec une interruption de service minimale.
- Permet des annulations rapides : si un problème survient après le passage du trafic vers l'environnement vert, vous pouvez rapidement revenir à l'environnement bleu et maintenir la continuité du service.
- Améliore les tests et la vérification : l'environnement vert peut être entièrement testé sans affecter l'environnement bleu vif, ce qui réduit le risque d'erreurs de production.
- Garantit la cohérence des données : la réplication basée sur le GTID permet de synchroniser vos environnements bleu et vert, ce qui évite les pertes de données ou les incohérences lors de la migration.
- Maintient la continuité des activités : l'automatisation de vos déploiements bleu/vert permet d'éviter de longues interruptions et des pertes financières en maintenant vos services disponibles pendant les mises à jour ou les migrations.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Un cluster de bases de données global source compatible avec Aurora MySQL (environnement bleu). Les bases de données mondiales fournissent une configuration multirégionale pour une haute disponibilité et une reprise après sinistre. Pour obtenir des instructions sur la configuration d'un cluster de bases de données global, consultez la documentation Aurora.
- La réplication basée sur le GTID est activée sur le cluster source.

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Versions du produit

- Aurora MySQL compatible 8.0 ou version ultérieure

Architecture

Le diagramme illustre les éléments suivants :

- Configuration de base de données globale : un cluster de bases de données global Aurora est déployé stratégiquement sur deux Régions AWS. Cette configuration permet la distribution géographique et la redondance régionale pour améliorer les capacités de reprise après sinistre.
- Réplication de la région principale vers la région secondaire : le mécanisme de réplication logique garantit une synchronisation fluide des données entre la région principale et la région secondaire. Cette réplication assure la cohérence des données avec une latence minimale sur toutes les distances géographiques.
- Réplication basée sur le GTID entre les clusters : la réplication basée sur le GTID préserve la cohérence transactionnelle et le flux de données ordonné entre le cluster principal bleu et le cluster principal vert, et garantit une synchronisation fiable des données.
- Réplication primaire vers secondaire bleue : la réplication logique établit un pipeline de données robuste entre le cluster principal bleu et son cluster secondaire. Cette réplication permet une synchronisation continue des données et une haute disponibilité.
- Configuration DNS Route 53 : les enregistrements de zone hébergée Route 53 gèrent la résolution DNS pour tous les points de terminaison de base de données de clusters bleus et verts. Cette configuration fournit un mappage fluide des terminaux et permet un routage efficace du trafic lors des scénarios de basculement.

Outils

Services AWS

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré conçu pour le cloud et compatible avec MySQL et PostgreSQL.
- AWS CloudFormationvous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur les applications qui s'exécutent sur AWS. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez, et vous vous CloudFormation occupez de leur provisionnement et de leur configuration.
- AWS Lambdaest un service de calcul qui prend en charge l'exécution de code sans provisionnement ni gestion de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.

Bonnes pratiques

Nous vous recommandons de consulter attentivement AWS la documentation afin de mieux comprendre la stratégie de déploiement bleu/vert, la réplication basée sur le GTID et les politiques de routage pondérées de Route 53. Ces connaissances sont cruciales pour mettre en œuvre et gérer efficacement les migrations de vos bases de données, garantir la cohérence des données et optimiser le routage du trafic. En acquérant une compréhension complète de ces AWS fonctionnalités et des meilleures pratiques, vous serez mieux équipé pour gérer les futures mises à jour, minimiser les temps d'arrêt et maintenir un environnement de base de données résilient et sécurisé.

Pour obtenir des instructions d'utilisation du modèle Services AWS pour ce modèle, consultez la AWS documentation suivante :

- Bonnes pratiques avec Amazon Aurora MySQL
- AWS CloudFormation meilleures pratiques
- Bonnes pratiques d'utilisation des AWS Lambda fonctions
- Bonnes pratiques pour Amazon Route 53

Épopées

Créez un environnement vert

Tâche	Description	Compétences requises
Créez une sauvegarde instantanée à partir du cluster bleu.	Dans un déploiement bleu/vert, l'environnement vert représente une nouvelle version identique de votre environnement de base de données actuel (bleu). Vous utilisez l'environnement écologique pour tester les mises à jour en toute sécurité, valider les modifications et garantir la stabilité avant de changer de trafic de productio n. Il sert de point de départ pour la mise en œuvre de modifications de base de données en perturbant le moins possible l'environ nement réel. Pour créer un environne ment écologique, vous devez d'abord créer un instantané du cluster principal (bleu) dans votre base de données globale compatible Aurora MySQL. Cet instantané sert de base à la création d'un environnement vert. Pour créer un instantané, procédez comme suit :	DBA

Tâche	Description	Compétences requises
	1. Connectez-vous à la console Amazon Relational Database Service (Amazon RDS) AWS Management Console et ouvrez-la. 2. Sélectionnez votre cluster principal (bleu). 3. Choisissez Actions, puis Prendre un instantané. 4. Donnez un nom à l'instant ané, par exemple`blue-green-demo` , et lancez le processus de sauvegarde. Vous pouvez également utiliser le AWS Command Line Interface (AWS CLI) pour créer l'instantané : `aws rds create-db-cluster-snapshot --db-cluster-snapshot-identifier blue-green-demo --db-cluster-identifier ex-global-cluster --region eu-west-1` Assurez-vous que le cliché se termine correctement avant de passer à l'étape suivante.	

Tâche	Description	Compétences requises
Générez le CloudFormation modèle pour votre base de données globale et ses ressources.	Le générateur CloudFormation IaC vous aide à générer des CloudFormation modèles à partir de AWS ressources existantes. Utilisez cette fonctionnalité pour créer un CloudFormation modèle pour votre base de données globale compatible Aurora MySQL existante et ses ressources associées. Ce modèle configure les groupes de sous-réseaux, les groupes de sécurité, les groupes de paramètres et d'autres paramètres. 1. Suivez les instructions de la CloudFormation documentation pour accéder à l'outil et le connecter à votre AWS environnement. 2. Sélectionnez votre base de données globale Aurora et les ressources associées pour générer le modèle.	DBA

Tâche	Description	Compétences requises
Modifiez le CloudFormation modèle pour l'environnement vert.	Personnalisez le CloudFormation modèle pour qu'il reflète les paramètres de l'environnement vert. Cela inclut la mise à jour des noms et des identifiants des ressources pour garantir que l'environnement vert fonctionne indépendamment du cluster bleu. 1. Mettez à jour les `DBInstanceIdentifier` propriétés `DBClusterIdentifier` et pour représenter l'environnement vert. 2. Modifiez les autres noms de ressources (par exemple, les groupes de sous-réseaux et les groupes de sécurité) pour éviter les conflits avec l'environnement bleu existant. 3. Activez la réplication basée sur le GTID dans le modèle en configurant les paramètres appropriés, comme décrit dans la documentation Aurora. 4. Modifiez la `SnapshotIdentifier` propriété pour spécifier l' Région AWS identifiant de votre	DBA

Tâche	Description	Compétences requises
	compte et le nom de l'instantané de l'étape précédente : `SnapshotIdentifier: arn:aws:rds:<region>:<account-id>:snapshot:<snapshot-name>` **Note** Si vous utilisez la `SnapshotIdentifier` propriété pour restaurer un cluster de base de données, évitez de spécifier des propriétés telles que `GlobalClusterIdentifier` `MasterUsername` , ou `MasterUserPassword` .	

Tâche	Description	Compétences requises
Déployez la CloudFormation pile pour créer des ressources pour l'environnement vert.	Au cours de cette étape, vous déployez le CloudFormation modèle personnalisé pour créer les ressources pour l'environnement vert. Pour déployer la CloudFormation pile, procédez comme suit : 1. Ouvrez la AWS CloudFormation console. 2. Dans le coin supérieur droit, choisissez Créer une pile, Avec de nouvelles ressources (standard). 3. Téléchargez votre CloudFormation modèle modifié ou spécifiez l'URL du modèle. Choisissez Suivant. 4. Entrez un nom de pile tel que `GreenClusterStack` , et fournissez tous les paramètres nécessaires (par exemple, `GreenClusterIdentifier`). Choisissez Suivant. 5. Configurez des options de pile supplémentaires selon les besoins et cochez la case pour confirmer que cela CloudFormation	DBA

Tâche	Description	Compétences requises
	peut créer des ressources AWS Identity and Access Management (IAM). Choisissez Suivant. 6. Passez en revue les détails de la pile. 7. Sélectionnez Envoyer. CloudFormation lance le processus de création des ressources de l'environnement vert. Ce processus peut prendre plusieurs minutes.	

Tâche	Description	Compétences requises
Validez la CloudFormation pile et les ressources.	Lorsque le déploiement de la CloudFormation pile sera terminé, vous devrez vérifier que l'environnement écologiqu e a été créé avec succès : 1. Dans la section Sorties de la CloudFormation pile, vérifiez les points de terminaison du cluster de base de données et de l'instance de base de données pour vérifier la configuration correcte. 2. Ouvrez la console Amazon RDS et vérifiez que le nouveau cluster de base de données Aurora (environn ement vert) est disponible. 3. Assurez-vous que toutes les ressources associées, telles que les sous-réseaux et les groupes de sécurité, ont été créées et liées à l'environnement vert. Après vérification, votre environnement vert est prêt à être configuré ultérieurement, y compris la réplication à partir de l'environnement bleu.	DBA

Configuration de la réplication basée sur le GTID

Tâche	Description	Compétences requises
Vérifiez les paramètres GTID sur le cluster bleu.	GTIDs fournissent une méthode très fiable pour répliquer les données entre vos environnements bleu et vert. La réplication basée sur le GTID offre une approche résiliente et simplifiée en attribuant un identifiant unique à chaque transaction dans l'environnement bleu. Cette méthode garantit que la synchronisation des données entre les environnements est fluide, cohérente et plus facile à gérer que la réplication binlog traditionnelle. Avant de configurer la réplicati on, vous devez vous assurer que la réplication basée sur le GTID est correctement activée sur le cluster bleu. Cette étape garantit que chaque transacti on dans l'environnement bleu fait l'objet d'un suivi unique et peut être reproduite dans l'environnement vert. Pour vérifier que le GTID est activé, procédez comme suit : 1. Sur la console Amazon RDS, passez en revue	DBA

Tâche	Description	Compétences requises
	le groupe de paramètres attribué au cluster bleu. 2. Vérifiez que les paramètres suivants sont définis : • `gtid-mode = ON` • `enforce_gtid_consistency = ON` Ces paramètres permettent le suivi GTID pour toutes les futures transactions dans l'environnement bleu. Après avoir confirmé ces paramètres, vous pouvez commencer à configurer la réplication.	

Tâche	Description	Compétences requises
Créez un utilisateur de réplication.	Pour répliquer les données de l'environnement bleu vers l'environnement vert, vous devez créer un utilisateur de réplication dédié sur le cluster bleu. Cet utilisateur sera chargé de gérer le processus de réplication. Pour configurer l'utilisateur de réplication : 1. Connectez-vous au cluster bleu à l'aide d'un client MySQL. 2. Exécutez les commandes suivantes pour créer l'utilisateur de réplication : `CREATE USER 'repl_user'@'%' IDENTIFIED BY 'repl_password'; GRANT REPLICATION SLAVE ON . TO 'repl_user'@'%'; FLUSH PRIVILEGES;` Cet utilisateur dispose désormais des autorisations nécessaires pour répliquer les données entre les deux environnements.	DBA

Tâche	Description	Compétences requises
Configurez la réplication basée sur le GTID sur le cluster vert.	L'étape suivante consiste à configurer le cluster vert pour la réplication basée sur le GTID. Cette configuration garantit que l'environnement vert reflétera en permanence toutes les transactions effectuées dans l'environnement bleu. Pour configurer le cluster vert, procédez comme suit : 1. Connectez-vous au cluster vert à l'aide d'un client MySQL. 2. Exécutez la commande suivante pour configurer la réplication : `CHANGE MASTER TO MASTER_HOST='blue-cluster-endpoint', MASTER_USER='repl_user', MASTER_PASSWORD='repl_password', MASTER_AUTO_POSITION=1;` où : • `blue-cluster-endpoint` Remplacez-le par le point de terminaison de votre cluster bleu. • Le `MASTER_AUTO_POSITION=1`	DBA

Tâche	Description	Compétences requises
	paramètre indique à MySQL d'utiliser la réplication basée sur GTID. Il positionne automatiquement le cluster vert pour reproduire les transactions du cluster bleu sans avoir à suivre les journaux et les positions manuellement.	
Démarrez la réplication sur le cluster vert.	Vous pouvez à présent démarrer le processus de réplication. Sur le cluster vert, exécutez la commande : `START SLAVE;` Cela permet à l'environnement vert de commencer à synchroniser les données, ainsi qu'à recevoir et à appliquer des transactions depuis l'environnement bleu.	DBA

Tâche	Description	Compétences requises
Vérifiez le processus de réplication.	Pour vérifier que l'environ nement vert reproduit correctement les données du cluster bleu : 1. Exécutez la commande suivante sur le cluster vert pour vérifier l'état de la réplication : `SHOW SLAVE STATUS\G;` 2. Passez en revue le résultat pour vérifier les points suivants : • `Slave_IO_Running = Yes` • `Slave_SQL_Running = Yes` • Les `Executed_Gtid_Set` valeurs `Retrieved_Gtid_Set` up-to-date et sont synchronisées avec le cluster bleu. • Il n'y a aucune erreur de réplication `Last_Error` sur le terrain. Si tous les indicateurs sont corrects, la réplication basée sur le GTID fonctionne correctement et l'environ nement vert est entièrement	DBA

Tâche	Description	Compétences requises
	synchronisé avec l'environnement bleu.	

Basculer le trafic du cluster bleu au cluster vert

Tâche	Description	Compétences requises
Configurez les politiques de routage pondérées Route 53.	Après avoir vérifié la cohérence des données entre les environnements bleu et vert, vous pouvez transférer le trafic du cluster bleu vers le cluster vert. Cette transition doit se faire en douceur, minimiser les temps d'arrêt et garantir l'intégrité de la base de données de votre application. Pour répondre à ces exigences, vous pouvez utiliser Route 53 pour le routage DNS et Lambda pour automatiser le changement de trafic. De plus, un plan de restauration bien défini vous permet de revenir au cluster bleu en cas de problème. La première étape consiste à configurer le routage pondéré dans Route 53. Le routage pondéré vous permet de contrôler la distribution du trafic entre les clusters bleus et verts, et de déplacer	AWS DevOps

Tâche	Description	Compétences requises
	progressivement le trafic d'un environnement à l'autre. Pour configurer le routage pondéré : 1. Ouvrez la console Route 53 et choisissez votre zone hébergée. 2. Créez deux enregistr ements DNS (CNAMEs) pour la base de données : un enregistrement pour le cluster bleu et un enregistr ement pour le cluster vert. 3. Attribuez des poids initiaux : • Définissez une pondérati on initiale faible (5 %, par exemple) pour le cluster vert afin d'envoyer une petite partie du trafic à des fins de test. • Définissez une pondérati on plus élevée (95 %, par exemple) pour le cluster bleu, afin qu'il conserve la majorité du trafic. Cette configuration vous permet d'effectuer une transition progressive qui réduit les risques et prend en charge les tests en temps réel avant de	

Tâche	Description	Compétences requises
	passer complètement au numérique. Pour plus d'informations sur les politiques de routage pondérées, consultez la documentation Route 53.	

Tâche	Description	Compétences requises

Déployez une fonction Lambda pour surveiller le délai de réplication.	Pour garantir que l'environnement vert est entièrement synchronisé avec l'environnement bleu, déployez une fonction Lambda qui surveille le délai de réplication entre les clusters. Cette fonction peut vérifier l'état de réplication, en particulier la métrique Seconds_Behind_Master, afin de déterminer si le cluster vert est prêt à gérer tout le trafic.
	
	Voici un exemple de fonction Lambda que vous pouvez utiliser :
	
	`import boto3`
	
	`def check_replication_lag(event, context):`
	`  client = boto3.client('rds')`
	`  response = client.describe_db_instances(DBInstanceIdentifier='green-cluster-instance')`
	`  replication_status = response['DBInstances'][0]['ReadReplicaDBInstanceIdentifiers']`
	`  if replication_status:`
	`  lag = replication_status[0]['ReplicationLag']`
		AWS DevOps

Tâche	Description	Compétences requises

	<pre>return lag
	return -1</pre>
	Cette fonction vérifie le délai de réplication et renvoie la valeur. Si le décalage est nul, le cluster vert est entièreme nt synchronisé avec le cluster bleu.	

Tâche	Description	Compétences requises

Automatisez l'ajustement du poids du DNS à l'aide de Lambda.	Lorsque le délai de réplication atteint zéro, il est temps de transférer tout le trafic vers le cluster vert. Vous pouvez automatiser cette transition à l'aide d'une autre fonction Lambda qui ajuste les pondérations DNS dans Route 53 afin de diriger 100 % du trafic vers le cluster vert.
	
	Voici un exemple de fonction Lambda qui automatise le changement de trafic :
	
	`import boto3`
	
	`def switch_traffic(event, context):`
	`route53 = boto3.client('route53')`
	`lag = check_replication_lag(event, context)`
	`if lag == 0:`
	`response = route53.change_resource_record_sets(`
	`HostedZoneId='YOUR_HOSTED_ZONE_ID',`
	`ChangeBatch={`
	`'Changes': [`
	`{`
	`'Action': 'UPSERT',`
		AWS DevOps

Tâche	Description	Compétences requises

	'ResourceRecordSet': {
	'Name': 'db.example.com',
	'Type': 'CNAME',
	'SetIdentifier': 'GreenCluster',
	'Weight': 100,
	'TTL': 60,
	'ResourceRecords': [{'Value': 'green-cluster-endpoint'}]
	}
	},
	{
	'Action': 'UPSERT',
	'ResourceRecordSet': {
	'Name': 'db.example.com',
	'Type': 'CNAME',
	'SetIdentifier': 'BlueCluster',
	'Weight': 0,
	'TTL': 60,
	'ResourceRecords':	

Tâche	Description	Compétences requises

```
 [{'Value': 'blue-clu
ster-endpoint'}]

 }
                    }
                ]
            }
        )
        return response
```

Cette fonction vérifie le délai de réplication et met à jour les pondérations DNS de Route 53 lorsque le décalage est nul afin de transférer complètem ent le trafic vers le cluster vert.

> **Note**
>
> Pendant le processus de transition, si le cluster bleu est confronté à un trafic d'écriture important , envisagez de suspendre temporair ement les opération s d'écriture pendant la transition. Cela garantit que la réplicati on rattrape son retard et évite les incohéren ces de données entre les clusters bleus et verts.

Tâche	Description	Compétences requises
Vérifiez le commutateur de trafic.	Une fois que la fonction Lambda a ajusté les pondérations DNS, vous devez vérifier que tout le trafic est dirigé vers le cluster vert et que le changement a été effectué avec succès. Pour vérifier : 1. Surveillez les enregistrements DNS de Route 53 pour vérifier que le trafic est dirigé vers le cluster vert. Pour plus d'informations, consultez la documentation de Route 53. 2. Vérifiez les performances de l'application en vous assurant que les utilisateurs sont servis dans un environnement écologique. 3. Vérifiez les connexions à la base de données pour confirmer que le cluster vert gère toutes les demandes de base de données. 4. Surveillez CloudWatch les métriques Amazon pour détecter tout signe de latence, de retard de réplication ou de dégradation des performances. Pour plus d'informations,	AWS DevOps

Tâche	Description	Compétences requises
	consultez la documentation d'Aurora. Si tout fonctionne comme prévu, le changement de trafic est terminé.	

Tâche	Description	Compétences requises
Si vous rencontrez des problèmes, annulez les modifications.	Il est essentiel de disposer d'un plan de réduction en cas de problème après le changement de trafic. Voici comment revenir rapidement au cluster bleu si nécessaire : 1. Rétablir les pondérations DNS dans Route 53 : utilisez la même fonction Lambda ou ajustez manuellement les pondérations DNS Route 53 pour rediriger 100 % du trafic vers le cluster bleu. 2. Surveillez les performances des applications : surveillez immédiatement les journaux des applications, CloudWatch les mesures et les performances de la base de données pour confirmer que le retour à l'environnement bleu a résolu les problèmes. 3. Identifier et résoudre les problèmes : étudiez et résolvez tout problème lié au cluster vert avant de tenter un autre changement de trafic. En mettant en œuvre ce plan de restauration, vous	AWS DevOps

Tâche	Description	Compétences requises
	pouvez garantir un minimum de perturbations à vos utilisateurs en cas de problèmes imprévus.	

Valider et arrêter la réplication basée sur le GTID

Tâche	Description	Compétences requises
Arrêtez la réplication basée sur le GTID sur le cluster vert.	Après avoir transféré le trafic de l'environnement bleu à l'environnement vert, vous devez valider le succès de la transition et vous assurer que le cluster vert fonctionne comme prévu. En outre, la réplication basée sur le GTID entre les clusters bleu et vert doit être arrêtée, car l'environnement vert sert désormais de base de données principale. L'exécution de ces tâches garantit que votre environnement est sécurisé, rationalisé et optimisé pour les opérations en cours. Pour arrêter la réplication, procédez comme suit : 1. Utilisez un client MySQL pour vous connecter au cluster vert. 2. Exécutez la commande SQL suivante pour arrêter	DBA

Tâche	Description	Compétences requises

	le processus de réplication sur le cluster vert :
	`STOP SLAVE;`
	3. (Facultatif) Si vous le souhaitez, vous pouvez réinitialiser la configura tion de réplication pour supprimer tous les paramètres de réplication résiduels :
	`RESET SLAVE ALL;`
	Lorsque vous arrêtez la réplication, le cluster vert devient totalement indépenda nt et fonctionne comme environnement de base de données principal pour vos charges de travail.	

Tâche	Description	Compétences requises
Nettoyez les ressources.	Le nettoyage de toutes les ressources temporaires ou inutilisées créées lors de la migration du cluster bleu vers le cluster vert garantit que votre environnement reste optimisé, sécurisé et rentable. Le nettoyage inclut l'ajustement des paramètres de sécurité, la réalisation des sauvegardes finales et la mise hors service des ressources inutiles. Pour nettoyer les ressources, procédez comme suit : 1. Mettre à jour les groupes de sécurité : configurez les groupes de sécurité associés aux clusters bleu et vert pour refléter le nouvel environnement principal (vert). Limitez l'accès à l'environnement bleu s'il n'est plus nécessaire et vérifiez que les paramètres de sécurité du cluster vert respectent les meilleures pratiques. 2. Effectuez une sauvegarde finale du cluster vert : une fois la migration terminée, prenez un dernier instantané du cluster vert pour servir	AWS DevOps

Tâche	Description	Compétences requises

	de sauvegarde. Vous pouvez utiliser cet instantané pour restaurer l'environnement dans le futur si nécessaire.
	
	`aws rds create-db-snapshot --db-instance-identifier green-cluster-instance --db-snapshot-identifier green-cluster-final-snapshot`
	
	3. Vérifiez et supprimez les ressources temporaires : passez en revue toutes les ressources temporaires créées lors de la migration, telles que les groupes de sécurité temporaires, les instantanés ou d'autres configurations. Supprimez les ressources qui ne sont plus nécessaires pour éviter des coûts inutiles. Supprimez par exemple le cluster bleu s'il n'est plus nécessaire :
	
	`aws rds delete-db-cluster --db-cluster-identifier blue-cluster-identifier --skip-final-snapshot`	

Tâche	Description	Compétences requises
	Le nettoyage des ressources permet de maintenir un environnement sécurisé et rationalisé, de réduire les coûts et de garantir que seule l'infrastructure nécessaire reste disponible.	

Ressources connexes

AWS CloudFormation:

- AWS CloudFormation Guide de l'utilisateur
- AWS CloudFormation meilleures pratiques
- Générez des modèles à partir de ressources existantes avec iAc Generator
- Importer des applications entières dans AWS CloudFormation (article de AWS blog)

Amazon Aurora :

- Guide de l'utilisateur Amazon Aurora
- Gestion d'un cluster de base de données Amazon Aurora

Stratégie de déploiement bleu/vert :

- Présentation des déploiements d'Amazon Aurora Blue/Green

Réplication basée sur le GTID :

- Utilisation de la réplication basée sur GTID (documentation Amazon RDS)

AWS Lambda:

- AWS Lambda Manuel du développeur
- Bonnes pratiques d'utilisation des AWS Lambda fonctions

Amazon Route 53 :

- Guide du développeur Amazon Route 53
- Routage pondéré

Outils client MySQL :

- PyMySQL

Automatisez les tâches de base de données dans l'édition SQL Server Express exécutée sur Amazon à EC2 l'aide AWS Lambda d'un planificateur de tâches

Créée par Subhani Shaik (AWS)

Récapitulatif

Ce modèle montre comment planifier et gérer les tâches de base de données dans l'édition SQL Server Express, qui est la version gratuite de SQL Server. Cependant, l'édition SQL Server Express ne dispose pas du service SQL Server Agent qui gère généralement les opérations de base de données automatisées. Ce modèle explique comment vous pouvez utiliser le planificateur de tâches et Lambda comme alternative pour automatiser les tâches de base de données dans l'édition SQL Server Express exécutées sur une instance Amazon Elastic Compute Cloud (Amazon). EC2

Le planificateur de tâches est un utilitaire système Windows intégré qui facilite l'exécution automatique des tâches de routine. Il fournit un mécanisme pour planifier et gérer les opérations automatisées, éliminant ainsi le besoin d'intervention manuelle dans les processus récurrents. AWS Lambdaest un service informatique sans serveur qui exécute automatiquement le code en réponse à des événements, sans que vous ayez à gérer l'infrastructure sous-jacente.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un cloud privé virtuel (VPC) créé avec Amazon Virtual Private Cloud (Amazon VPC)
- Une EC2 instance Amazon avec Windows Server
- Volumes Amazon Elastic Block Store (Amazon EBS) attachés à une instance EC2 Amazon avec Windows Server
- Fichiers binaires de SQL Server Express Edition

Limites

- Pour plus d'informations sur les limites des fonctionnalités de l'édition SQL Server Express, consultez le site Web de Microsoft.

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- SQL Server 2016 ou version ultérieure avec édition SQL Server Express

Architecture

Le schéma suivant montre une EC2 instance Amazon exécutée avec l'édition SQL Server Express installée. L'instance est accessible via le client RDP (Remote Desktop Protocol) ou depuis AWS Systems Manager Session Manager. AWS Key Management Service (AWS KMS) gère le chiffrement des données pour les volumes Amazon EBS afin de garantir data-at-rest la sécurité. L'infrastructure inclut également AWS Identity and Access Management (IAM), qui fournit le contrôle d'accès et gère les autorisations pour l'exécution des fonctions Lambda. Amazon Simple Storage Service (Amazon S3) stocke les fonctions Lambda.

Outils

Services AWS

- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon. EC2
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Systems Manager Session Managerest un AWS Systems Manager outil entièrement géré. Avec Session Manager, vous pouvez gérer vos EC2 instances Amazon, vos appareils périphériques, vos serveurs sur site et vos machines virtuelles (VMs).
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Autres outils

- Microsoft SQL Server Management Studio (SSMS) est un outil de gestion de SQL Server, y compris l'accès, la configuration et l'administration des composants de SQL Server.
- Python est un langage de programmation informatique polyvalent. Vous pouvez l'utiliser pour créer des applications, automatiser des tâches et développer des services sur le AWS Cloud.
- Le planificateur de tâches est un outil Microsoft que vous pouvez utiliser pour planifier automatiquement des tâches de routine sur votre ordinateur.

Bonnes pratiques

- Bonnes pratiques pour Amazon EC2
- Bonnes pratiques pour le déploiement de Microsoft SQL Server sur Amazon EC2
- Bonnes pratiques d'utilisation des AWS Lambda fonctions
- Bonnes pratiques de sécurité dans IAM

Épopées

Créez une EC2 instance Amazon et installez l'édition SQL Server Express

Tâche	Description	Compétences requises
Déployez une EC2 instance Amazon.	Pour créer une EC2 instance Amazon, ouvrez la EC2 console Amazon à l'https://	ADMINISTRATEUR DE BASES DE DONNÉES, AWS DevOps

Tâche	Description	Compétences requises
	console.aws.amazon.com/ec2/adresse et sélectionnez une Amazon Machine Image (AMI) dans la liste des instances disponibles pour Windows Server. Pour plus d'informations, consultez Lancer une EC2 instance Amazon dans la AWS documentation.	

Tâche	Description	Compétences requises
Installez l'édition SQL Server Express.	Pour installer l'édition SQL Server Express, procédez comme suit : 1. Pour vous connecter à votre EC2 instance Amazon, choisissez une option : • Option A — Utiliser le protocole RDP (Remote Desktop Protocol). Pour obtenir des instructions, consultez la section Se connecter à votre instance Windows à l'aide d'un client RDP dans la AWS documentation. • Option B — Utilisez la EC2 console Amazon et AWS Systems Manager Session Manager. Pour obtenir des instructi ons, consultez Connect to your Amazon EC2 instance using Session Manager dans la AWS documentation. 2. Pour télécharger l'édition requise de SQL Server Express, accédez à la section Téléchargements de SQL Server sur le site Web de Microsoft. 3. Pour installer l'édition SQL Server Express, suivez les	ADMINISTRATEUR DE BASES DE DONNÉES, AWS DevOps

Tâche	Description	Compétences requises
	instructions de la section Planifier une installation de SQL Server sur le site Web de Microsoft.	

Créez des tâches de maintenance de base de données automatisées

Tâche	Description	Compétences requises
Identifiez les tâches de routine.	Identifiez les tâches de routine que vous souhaitez automatiser. Par exemple, les tâches suivantes sont éligibles à l'automatisation : • Sauvegardes de base de données (complètes, différentielles et journal des transactions) • Maintenance et réorganisation de l'index • Mises à jour statistiques • Opérations spécifiques à l'application • Nettoyage ou archivage des données	DBA
Préparez des scripts SQL.	Pour préparer des scripts SQL, procédez comme suit : 1. Créez des requêtes SQL pour chaque tâche de maintenance. Voici un exemple de requête T-	DBA

Tâche	Description	Compétences requises
	SQL pour effectuer une sauvegarde de base de données spécifique : `Backup Database <Database_Name> To Disk='C:\Backups\Database_Name.bak'` 2. Enregistrez le fichier de script sous `<File Name>.sql` . Enregistrez ensuite les scripts dans un emplacement accessible sur le disque local du serveur sur l' EC2 instance Amazon ou sur un partage de fichiers réseau.	

Tâche	Description	Compétences requises
Configurez les autorisations d'accès.	Pour configurer les autorisations d'accès, procédez comme suit : 1. Définissez les autorisations de système de fichiers appropriées. Pour obtenir des instructions, voir Configurer les autorisations du système de fichiers pour l'accès au moteur de base de données sur le site Web de Microsoft. 2. Vérifiez que le compte de service SQL Server dispose des accès nécessaires. Pour obtenir des instructions, voir Configurer les comptes de service et les autorisations Windows sur le site Web de Microsoft. 3. Vérifiez la connectivité réseau pour les partages distants. Pour plus d'informations, consultez la section Accès aux données à l'aide de partages de fichiers dans la AWS documentation.	DBA

Automatisez les tâches avec le planificateur de tâches

Tâche	Description	Compétences requises

Créez des fichiers batch.	• Pour créer un fichier batch, utilisez un éditeur de texte pour saisir la commande suivante. Remplacez `username` les paramètres `password` par vos propres valeurs. Enregistrez ensuite le fichier sous`<Name>.bat` .
	
	`sqlcmd -S servername -U username -P password -i <T-SQL query path.sql>`
	
	• Pour créer un fichier batch pour les tâches SQL, utilisez un éditeur de texte et tapez les commandes suivantes. Remplacez les paramètres `ServerName DatabaseName` ,`username`, et `password` par vos propres valeurs. Enregistrez ensuite le fichier sous`<Name>.bat` .
	
	`@echo off`
	`sqlcmd -S [ServerName] -d [DatabaseName] -U username -P password -i "PathToSQLScript\Script.sql"`
		AWS DevOps, ADMINISTRATEUR DE BASE DE DONNÉES

Tâche	Description	Compétences requises
	`-o "PathToOutput\Output.txt"`	

Tâche	Description	Compétences requises
Créez des tâches dans le planificateur de tâches.	Pour créer une tâche dans le planificateur de tâches, procédez comme suit : 1. Pour ouvrir le planificateur de tâches, tapez taskschd.msc dans la recherche Windows. 2. Choisissez le menu Action, puis sélectionnez Créer une tâche de base. 3. Dans Nom, saisissez le nom de la tâche, puis choisissez Next. 4. Pour Trigger, sélectionnez l'option indiquant le moment où vous souhaitez que la tâche commence, puis choisissez Next. 5. Fournissez les informations de début et de récurrence de la tâche, puis choisissez Next. 6. Pour la section Action, sélectionnez Démarrer un programme, puis cliquez sur Suivant. 7. Pour Programme/script, spécifiez le chemin du fichier batch que vous avez créé lors de la tâche précédente, puis choisissez Next.	DBA

Tâche	Description	Compétences requises
	8. Choisissez Finish (Terminer). Pour exécuter la tâche manuellement, cliquez avec le bouton droit sur la tâche nouvellement créée, puis sélectionnez Exécuter.	
Afficher le statut de la tâche.	Pour afficher le statut d'une tâche dans le planificateur de tâches, procédez comme suit : 1. Dans le planificateur de tâches, accédez à la bibliothèque du planificateur de tâches, qui affiche toutes les tâches. 2. Pour voir le statut de la tâche que vous avez créée précédemment, sélectionnez la tâche, puis accédez à l'onglet Historique.	ADMINISTRATEUR DE BASES DE DONNÉES, AWS DevOps

Automatisez les tâches avec AWS Lambda

Tâche	Description	Compétences requises
Implémentez la solution.	Pour implémenter la solution de ce modèle, procédez comme suit : 1. Créez une fonction Lambda. Pour obtenir des instructions, consultez la	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	section Création de votre première fonction Lambda dans la AWS documentation. 2. Planifiez la fonction Lambda. Pour obtenir des instructions, consultez la section Invoquer une fonction Lambda selon un calendrier dans la AWS documentation. 3. Exécutez des requêtes T-SQL. Pour plus d'informations, consultez la section Tutoriel : Utilisation d'une fonction Lambda pour accéder à une base de données Amazon RDS dans la documentation. AWS Le didacticiel explique comment connecter des bases de données Amazon RDS à partir de fonctions Lambda pour exécuter des requêtes SQL.	

Résolution des problèmes

Problème	Solution
Problèmes liés à Lambda	Pour obtenir de l'aide concernant les erreurs et les problèmes que vous pourriez rencontrer lors de l'utilisation AWS Lambda, consultez

Problème	Solution
	la section Résolution des problèmes dans Lambda dans la AWS documentation.

Ressources connexes

- Types d' EC2 instances Amazon
- AWS Lambda documentation
- AWS Lambda tarification
- Planificateur de tâches pour les développeurs (site Web de Microsoft)

Automatisez le basculement et le retour en arrière entre régions à l'aide de DR Orchestrator Framework

Créée par Jitendra Kumar (AWS), Oliver Francis (AWS) et Pavithra Balasubramanian (AWS)

Récapitulatif

Ce modèle décrit comment utiliser DR Orchestrator Framework pour orchestrer et automatiser les étapes manuelles, sujettes aux erreurs, pour effectuer une reprise après sinistre dans les régions Amazon Web Services ().AWS Le modèle couvre les bases de données suivantes :

- Amazon Relational Database Service (Amazon RDS) pour MySQL, Amazon RDS pour PostgreSQL ou Amazon RDS pour MariaDB
- Édition compatible avec Amazon Aurora MySQL ou édition compatible avec Amazon Aurora PostgreSQL (à l'aide d'un fichier centralisé)
- Amazon ElastiCache (Redis OSS)

Pour démontrer les fonctionnalités de DR Orchestrator Framework, vous devez créer deux instances ou clusters de base de données. Le primaire est dans le Région AWS `us-east-1`, et le secondaire est dans`us-west-2`. Pour créer ces ressources, vous devez utiliser les AWS CloudFormation modèles contenus dans le `App-Stack` dossier du GitHub référentiel aws-cross-region-dr-databases.

Conditions préalables et limitations

Prérequis généraux

- Framework DR Orchestrator déployé à la fois dans le primaire et le secondaire Régions AWS
- Deux compartiments Amazon Simple Storage Service
- Un cloud privé virtuel (VPC) avec deux sous-réseaux et un groupe de sécurité AWS

Prérequis spécifiques au moteur

- Amazon Aurora — Au moins une base de données globale Aurora doit être disponible sur deux Régions AWS. Vous pouvez l'utiliser `us-east-1` comme région principale et l'utiliser `us-west-2` comme région secondaire.

- Amazon ElastiCache (Redis OSS) — Une banque de données ElastiCache globale doit être disponible en deux. Régions AWS Vous pouvez le faire `use us-east-1` en tant que région principale et l'utiliser `us-west-2` en tant que région secondaire.

Limitations d'Amazon RDS

- DR Orchestrator Framework ne vérifie pas le délai de réplication avant d'effectuer un basculement ou un retour en arrière. Le délai de réplication doit être vérifié manuellement.
- Cette solution a été testée à l'aide d'une instance de base de données principale avec une réplique en lecture. Si vous souhaitez utiliser plusieurs répliques de lecture, testez soigneusement la solution avant de l'implémenter dans un environnement de production.

Limites d'Aurora

- La disponibilité et le support des fonctionnalités varient en fonction des versions spécifiques de chaque moteur de base de données et d'une version à l'autre Régions AWS. Pour plus d'informations sur la disponibilité des fonctionnalités et des régions pour la réplication entre régions, voir Répliques de lecture entre régions.
- Les bases de données globales Aurora ont des exigences de configuration spécifiques pour les classes d'instances de base de données Aurora prises en charge et le nombre maximum de Régions AWS. Pour plus d'informations, consultez la section Exigences de configuration d'une base de données globale Amazon Aurora.
- Cette solution a été testée à l'aide d'une instance de base de données principale avec une réplique en lecture. Si vous souhaitez utiliser plusieurs répliques de lecture, testez soigneusement la solution avant de l'implémenter dans un environnement de production.

ElastiCache limites

- Pour plus d'informations sur la disponibilité des régions pour Global Datastore et les exigences ElastiCache de configuration, consultez la section Conditions préalables et limites de la ElastiCache documentation.

Versions des produits Amazon RDS

Amazon RDS prend en charge les versions de moteur suivantes :

- MySQL — Amazon RDS prend en charge les instances de base de données exécutant les versions suivantes de MySQL : MySQL 8.0 et MySQL 5.7
- PostgreSQL — Pour plus d'informations sur les versions prises en charge d'Amazon RDS pour PostgreSQL, consultez la section Versions de base de données PostgreSQL disponibles.
- MariaDB — Amazon RDS prend en charge les instances de base de données exécutant les versions suivantes de MariaDB :
  - MariaDB 10.11
  - MariaDB 10.6
  - MariaDB 10.5

Versions des produits Aurora

- Le passage à la base de données globale Amazon Aurora nécessite la compatibilité entre Aurora MySQL et MySQL 5.7, version 2.09.1 et supérieure

  Pour plus d'informations, consultez Limitations des bases de données mondiales Amazon Aurora.

ElastiCache Versions du produit (Redis OSS)

Amazon ElastiCache (Redis OSS) prend en charge les versions Redis suivantes :

- Redis 7.1 (améliorée)
- Redis 7.0 (améliorée)
- Redis 6.2 (améliorée)
- Redis 6.0 (améliorée)
- Redis 5.0.6 (améliorée)

Pour plus d'informations, voir Versions prises en charge ElastiCache (Redis OSS).

Architecture

Architecture Amazon RDS

L'architecture Amazon RDS inclut les ressources suivantes :

- L'instance de base de données Amazon RDS principale créée dans la région principale (`us-east-1`) avec un accès en lecture/écriture pour les clients

- Une réplique en lecture Amazon RDS créée dans la région secondaire (`us-west-2`) avec un accès en lecture seule pour les clients
- Framework DR Orchestrator déployé dans les régions principale et secondaire

Le diagramme décrit les éléments suivants :

1. Réplication asynchrone entre l'instance principale et l'instance secondaire
2. Accès en lecture/écriture pour les clients de la région principale
3. Accès en lecture seule pour les clients de la région secondaire

Architecture Aurora

L'architecture Amazon Aurora inclut les ressources suivantes :

- Le cluster de base de données Aurora principal créé dans la région principale (`us-east-1`) avec un point de terminaison d'écriture active
- Un cluster de base de données Aurora créé dans la région secondaire (`us-west-2`) avec un point de terminaison d'écriture inactif
- Framework DR Orchestrator déployé dans les régions principale et secondaire

Le diagramme décrit les éléments suivants :

1. Réplication asynchrone entre le cluster principal et le cluster secondaire
2. Le cluster de base de données principal avec un point de terminaison d'écriture active
3. Le cluster de base de données secondaire avec un point de terminaison d'écriture inactif

ElastiCache Architecture (Redis OSS)

L'architecture Amazon ElastiCache (Redis OSS) inclut les ressources suivantes :

- Une banque de données globale ElastiCache (Redis OSS) créée avec deux clusters :
  1. Le cluster principal de la région principale (`us-east-1`)

2. Le cluster secondaire de la région secondaire (`us-west-2`)

- Un lien interrégional Amazon avec chiffrement TLS 1.2 entre les deux clusters
- Framework DR Orchestrator déployé dans les régions principale et secondaire

Automatisation et mise à l'échelle

DR Orchestrator Framework est évolutif et prend en charge le basculement ou le repli de plusieurs bases de données AWS en parallèle.

Vous pouvez utiliser le code de charge utile suivant pour basculer entre plusieurs AWS bases de données de votre compte. Dans cet exemple, trois AWS bases de données (deux bases de données globales telles que Aurora MySQL compatible ou Aurora PostgreSQL compatible, et une instance Amazon RDS for MySQL) basculent vers la région DR :

```
{
  "StatePayload": [
    {
      "layer": 1,
      "resources": [
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (MySQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-mysql-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-mysql-cluster-
identifier"
          }
        },
        {
          "resourceType": "PlannedFailoverAurora",
          "resourceName": "Switchover (planned failover) of Amazon Aurora global
 databases (PostgreSQL)",
          "parameters": {
            "GlobalClusterIdentifier": "!Import dr-globaldb-cluster-postgres-global-
identifier",
            "DBClusterIdentifier": "!Import dr-globaldb-cluster-postgres-cluster-
identifier"
```

```
          }
        },
        {
          "resourceType": "PromoteRDSReadReplica",
          "resourceName": "Promote RDS for MySQL Read Replica",
          "parameters": {
            "RDSInstanceIdentifier": "!Import rds-mysql-instance-identifier",
            "TargetClusterIdentifier": "!Import rds-mysql-instance-global-arn"
          }
        }
      ]
    }
  ]
}
```

Outils

AWS services

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré conçu pour le cloud et compatible avec MySQL et PostgreSQL.
- Amazon vous ElastiCache aide à configurer, à gérer et à faire évoluer des environnements de cache en mémoire distribués dans le AWS Cloud. Ce modèle utilise Amazon ElastiCache (Redis OSS).
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez. Dans ce modèle, les fonctions Lambda sont utilisées pour AWS Step Functions effectuer les étapes.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le. AWS Cloud Ce modèle prend en charge Amazon RDS pour MySQL, Amazon RDS pour PostgreSQL et Amazon RDS pour MariaDB.
- AWS SDK pour Python (Boto3)vous permet d'intégrer votre application, bibliothèque ou script Python à Services AWS. Dans ce modèle, les Boto3 APIs sont utilisés pour communiquer avec les instances de base de données ou les bases de données globales.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise. Dans ce modèle, les machines d'état Step Functions sont utilisées pour

orchestrer et exécuter le basculement et le retour en arrière entre régions des instances de base de données ou des bases de données globales.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel aws-cross-region-dr-databases sur GitHub.

Épopées

Installez DR Orchestrator Framework

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Pour cloner le dépôt, exécutez la commande suivante : `git clone https://github.com/aws-samples/aws-cross-region-dr-databases.git`	AWS DevOps, administrateur AWS

Package Lambda utilise le code des fonctions dans une archive de fichier .zip.	Créez les fichiers d'archive pour les fonctions Lambda afin d'inclure les dépendances du DR Orchestrator Framework :
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts`
	
	`bash scripts/deploy-orchestrator-sh.sh`
		Administrateur AWS

Créez des compartiments S3.	Les compartiments S3 sont nécessaires pour stocker le framework DR Orchestrator ainsi que votre dernière configuration. Créez deux compartiments S3, l'un dans la	Administrateur AWS

Tâche	Description	Compétences requises
	région principale (`us-east-1`) et l'autre dans la région secondaire (`us-west-2`) : • `dr-orchestrator-xxxxxx-us-east-1` • `dr-orchestrator-xxxxxx-us-west-2` `xxxxxx`Remplacez-le par une valeur aléatoire pour que les noms des compartiments soient uniques.	
Créez des sous-réseaux et des groupes de sécurité.	Dans la région principale (`us-east-1`) et la région secondaire (`us-west-2`), créez deux sous-réseaux et un groupe de sécurité pour le déploiement de la fonction Lambda dans votre VPC : • `subnet-XXXXXXX` • `subnet-YYYYYYY` • `sg-XXXXXXXXXXX`	Administrateur AWS

Tâche	Description	Compétences requises
Mettez à jour les fichiers de paramètres de DR Orchestrator.	Dans le `<YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation` dossier, mettez à jour les fichiers de paramètres DR Orchestrator suivants : • `Orchestrator-Deployer-parameters-us-east-1.json` • `Orchestrator-Deployer-parameters-us-west-2.json` Utilisez les valeurs de paramètres suivantes, en y remplaçant `x` et par les noms de vos ressources : `[ { "ParameterKey": "TemplateStoreS3BucketName", "ParameterValue": "dr-orchestrator-xxxxxx-us-east-1" }, { "ParameterKey": "TemplateVPCId", "ParameterValue": "vpc-xxxxxx" }, {`	Administrateur AWS

Tâche	Description	Compétences requises
	`"ParameterKey": "TemplateLambdaSubnetID1", "ParameterValue": "subnet-xxxxx" }, { "ParameterKey": "TemplateLambdaSubnetID2", "ParameterValue": "subnet-yyyyy" }, { "ParameterKey": "TemplateLambdaSecurityGroupID", "ParameterValue": "sg-xxxxxxxxxx" } ]`	

Tâche	Description	Compétences requises
Téléchargez le code DR Orchestrator Framework dans le compartiment S3.	Le code sera plus sûr dans un compartiment S3 que dans le répertoire local. Téléchargez le `DR-Orchestration-artifacts` répertoire, y compris tous les fichiers et sous-dossiers, dans les compartiments S3. Pour télécharger le code, procédez comme suit : 1. Connectez-vous au AWS Management Console. 2. Accédez à la console Amazon S3. 3. Sélectionnez la `dr-orchestrator-xxxxxx-us-east-1 bucket` . 4. Choisissez Télécharger, puis Ajouter un dossier. 5. Sélectionnez le `DR-Orchestration-artifacts` dossier. 6. Choisissez Charger. 7. Sélectionnez le `dr-orchestrator-xxxxxx-us-west-2` compartiment. 8. Répétez les étapes 4 à 7.	Administrateur AWS

Tâche	Description	Compétences requises

Déployez DR Orchestrator Framework dans la région principale.	Pour déployer DR Orchestrator Framework dans la région principale (`us-east-1`), exécutez les commandes suivantes :
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		Administrateur AWS

Tâche	Description	Compétences requises

Déployez DR Orchestrator Framework dans la région secondaire.	Dans la région secondaire (`us-west-2`), exécutez les commandes suivantes :
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/DR-Orchestration-artifacts/cloudformation`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name dr-orchestrator \`
	`--template-file Orchestrator-Deployer.yaml \`
	`--parameter-overrides file://Orchestrator-Deployer-parameters-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
		Administrateur AWS

Tâche	Description	Compétences requises
Vérifier le déploiement.	Si la AWS CloudForm ation commande s'exécute correctement, elle renvoie le résultat suivant : `Successfully created/ updated stack - dr-orchestrator` Vous pouvez également accéder à la AWS CloudForm ation console et vérifier l'état de la `dr-orchestrator` pile.	Administrateur AWS

Création des instances ou des clusters de base de données

Tâche	Description	Compétences requises
Créez les sous-réseaux et les groupes de sécurité de la base de données.	Dans votre VPC, créez deux sous-réseaux et un groupe de sécurité pour l'instance de base de données ou la base de données globale dans les régions principale (`us-east-1`) et secondaire (`us-west-2`) : • `subnet-XXXXXX` • `subnet-XXXXXX` • `sg-XXXXXXXXXX`	Administrateur AWS
Mettez à jour le fichier de paramètres pour l'instance ou	Dans le `<YOUR LOCAL GIT FOLDER>/App-Stack`	Administrateur AWS

Tâche	Description	Compétences requises
le cluster de base de données principal.	dossier, mettez à jour le fichier de paramètres de la région principale. Amazon RDS Dans le `RDS-MySQL-parameter-us-east-1.json` fichier, mettez à jour `SubnetIds` et `DBSecurityGroup` avec les noms des ressources que vous avez créées : `{ "Parameters": { "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId" } }` Amazon Aurora	

Tâche	Description	Compétences requises
	Dans le `Aurora-MySQL-parameter-us-east-1.json` fichier, mettez à jour `SubnetIds` et `DBSecurityGroup` avec les noms des ressources que vous avez créées : `{ "Parameters": { "SubnetIds": "subnet1-xxxxxx,subnet2-xxxxxx", "DBSecurityGroup": "sg-xxxxxxxxxx", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql", "DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } }`	

Tâche	Description	Compétences requises
	Amazon ElastiCache (Redis OSS) Dans le `ElastiCache-parameter-us-east-1.json` fichier, mettez à jour `SubnetIds` et `DBSecurityGroup` avec les noms des ressources que vous avez créées. `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-xxxxxxxxxx", "SubnetIds": "subnet-xxxxxx,subnet-xxxxxx", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId",`	

Tâche	Description	Compétences requises
	<pre>"PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" } }</pre>	

Tâche	Description	Compétences requises

Déployez votre instance ou cluster de base de données dans la région principale.	Pour déployer votre instance ou votre cluster dans la région principale (`us-east-1`), exécutez les commandes suivantes en fonction de votre moteur de base de données.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-Primary.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 \`
		Administrateur AWS

Tâche	Description	Compétences requises

	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-Primary.yaml \`
	`--parameter-overrides file://Aurora-MySQL-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`	

	Amazon ElastiCache (Redis OSS)
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-east-1 --stack-name elasticache-ds-app-stack \`
	`--template-file ElastiCache-Primary.yaml \`
	`--parameter-overrides file://ElastiCache-parameter-us-east-1.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`	

Tâche	Description	Compétences requises
	Vérifiez que les AWS CloudFormation ressources ont été déployées avec succès.	

Tâche	Description	Compétences requises
Mettez à jour le fichier de paramètres pour l'instance ou le cluster de base de données secondaire.	Dans le `<YOUR LOCAL GIT FOLDER>/App-Stack` dossier, mettez à jour le fichier de paramètres de la région secondaire. Amazon RDS Dans le `RDS-MySQL-parameter-us-west-2.json` fichier, mettez à jour `SubnetIDs` et `DBSecurityGroup` avec les noms des ressources que vous avez créées. Mettez à jour le `PrimaryRegionKMSKeyArn` avec la valeur `MySQLKmsKeyId` extraite de la section Outputs de la AWS CloudFormation pile pour l'instance de base de données principale : `{ "Parameters": { "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "DBSecurityGroup": "sg-ccccccccc", "MySqlGlobalIdentifier":"rds-mysql-instance", "InitialDatabaseName": "mysqldb", "DBPortNumber": "3789",`	Administrateur AWS

Tâche	Description	Compétences requises
	<pre>"PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/rds-mysql-instance-KmsKeyId", "PrimaryRegionKMSKeyArn":"arn:aws:kms:us-east-1:xxxxxxxxx:key/mrk-xxxxxxxxxxxxxxxxx" } }</pre> Amazon Aurora Dans le `Aurora-MySQL-parameter-us-west-2.json` fichier, mettez à jour `SubnetIDs` et `DBSecurityGroup` avec les noms des ressources que vous avez créées. Mettez à jour le `PrimaryRegionKMSKeyArn` avec la valeur `AuroraKmsKeyId` extraite de la section Outputs de la AWS CloudFormation pile pour l'instance de base de données principale : <pre>{ "Parameters": { "SubnetIds": "subnet1-aaaaaaaaa,subnet2-bbbbbbbbb",</pre>	

Tâche	Description	Compétences requises
	<pre>"DBSecurityGroup": "sg-ccccccccc", "GlobalClusterIdentifier":"dr-globaldb-cluster-mysql", "DBClusterName":"dbcluster-01", "SourceDBClusterName":"dbcluster-02", "DBPortNumber": "3787", "DBInstanceClass": "db.r5.large", "InitialDatabaseName": "sampledb", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2", "KMSKeyAliasName": "rds/dr-globaldb-cluster-mysql-KmsKeyId" } }</pre> Amazon ElastiCache (Redis OSS) Dans le `ElastiCache-parameter-us-west-2.json` fichier, mettez à jour `SubnetIDs` et `DBSecurityGroup` avec les noms des ressources que vous avez créées. Mettez à jour le `PrimaryRegionKMSKeyArn` avec la valeur `ElastiCac`	

Tâche	Description	Compétences requises
	heKmsKeyId extraite de la section Outputs de la AWS CloudFormation pile pour l'instance de base de données principale : `{ "Parameters": { "CacheNodeType": "cache.m5.large", "DBSecurityGroup": "sg-cccccccccc", "SubnetIds": "subnet-aaaaaaaaa, subnet-bbbbbbbbb", "EngineVersion": "5.0.6", "GlobalReplicationGroupIdSuffix": "demo-redis-global-datastore", "NumReplicas": "1", "NumShards": "1", "ReplicationGroupId": "demo-redis-cluster", "DBPortNumber": "3788", "TransitEncryption": "true", "KMSKeyAliasName": "elasticache/demo-redis-global-datastore-KmsKeyId", "PrimaryRegion": "us-east-1", "SecondaryRegion": "us-west-2" } }`	

Tâche	Description	Compétences requises

Déployez votre instance ou cluster de base de données dans la région secondaire.	Exécutez les commandes suivantes, en fonction de votre moteur de base de données.
	
	Amazon RDS
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name rds-mysql-app-stack \`
	`--template-file RDS-MySQL-DR.yaml \`
	`--parameter-overrides file://RDS-MySQL-parameter-us-west-2.json \`
	`--capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \`
	`--disable-rollback`
	
	Amazon Aurora
	
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	
	`aws cloudformation deploy \`
	`--region us-west-2 \`
	`--stack-name aurora-mysql-app-stack \`
	`--template-file Aurora-MySQL-DR.yaml \`
		Administrateur AWS

Tâche	Description	Compétences requises
	`--parameter-overrides file://Aurora-MySQL-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	

	Amazon ElastiCache (Redis OSS)
	`cd <YOUR-LOCAL-GIT-FOLDER>/App-Stack`
	`aws cloudformation deploy \ --region us-west-2 \ --stack-name elasticache-ds-app-stack \ --template-file ElastiCache-DR.yaml \ --parameter-overrides file://ElastiCache-parameter-us-west-2.json \ --capabilities CAPABILITY_AUTO_EXPAND CAPABILITY_NAMED_IAM CAPABILITY_IAM \ --disable-rollback`	

	Vérifiez que les AWS CloudFormation ressources ont été déployées avec succès.	

Ressources connexes

- Stratégie de reprise après sinistre pour les bases de données sur AWS (stratégie d'orientation AWS prescriptive)
- Automatisez votre solution de reprise après sinistre pour les bases de données relationnelles sur AWS (AWS guide prescriptif)
- Utilisation de bases de données globales Amazon Aurora
- Réplication à Régions AWS l'aide de banques de données globales
- Automatisez votre solution de reprise après sinistre pour les bases de données relationnelles sur AWS (AWS guide prescriptif)

Automatisez la réplication des instances Amazon RDS sur Comptes AWS

Créée par Parag Nagwekar (AWS) et Arun Chanapillai (AWS)

Récapitulatif

Ce modèle vous montre comment automatiser le processus de réplication, de suivi et de restauration de vos instances de base de données Amazon Relational Database Service (Amazon RDS) sur Comptes AWS différentes instances en utilisant et. AWS Step Functions AWS Lambda Vous pouvez utiliser cette automatisation pour effectuer une réplication à grande échelle d'instances de base de données RDS sans impact sur les performances ni surcharge opérationnelle, quelle que soit la taille de votre organisation. Vous pouvez également utiliser ce modèle pour aider votre entreprise à se conformer aux stratégies obligatoires de gouvernance des données ou aux exigences de conformité qui exigent que vos données soient répliquées et redondantes entre différents Comptes AWS et. Régions AWS La réplication multicompte des données Amazon RDS à grande échelle est un processus manuel inefficace et sujet aux erreurs qui peut être coûteux et chronophage, mais l'automatisation selon ce modèle peut vous aider à réaliser une réplication entre comptes de manière sûre, efficace et efficiente.

Conditions préalables et limitations

Prérequis

- Deux Comptes AWS
- Une instance de base de données RDS, opérationnelle dans la source Compte AWS
- Un groupe de sous-réseaux pour l'instance de base de données RDS dans la destination Compte AWS
- Une clé AWS Key Management Service (AWS KMS) créée dans la source Compte AWS et partagée avec le compte de destination (pour plus d'informations sur les détails de la politique, consultez la section Informations supplémentaires de ce modèle.)
- Un AWS KMS key dans la destination Compte AWS pour chiffrer la base de données dans le compte de destination

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Versions du produit

- Python 3.9 (en utilisant AWS Lambda)
- PostgreSQL 11.3, 13.x et 14.x

Architecture

Pile technologique

- Amazon Relational Database Service (Amazon RDS)
- Amazon Simple Notification Service (Amazon SNS)
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- AWS Secrets Manager
- AWS Step Functions

Architecture cible

Le schéma suivant montre une architecture permettant d'utiliser Step Functions pour orchestrer la réplication planifiée et à la demande d'instances de base de données RDS d'un compte source (compte A) vers un compte de destination (compte B).

Dans le compte source (compte A dans le schéma), la machine d'état Step Functions effectue les opérations suivantes :

1. Crée un instantané à partir de l'instance de base de données RDS dans le compte A.
2. Copie et chiffre le cliché avec un compte AWS KMS key de provenance A. Pour garantir le chiffrement pendant le transfert, le cliché est chiffré, que l'instance de base de données soit chiffrée ou non.
3. Partage l'instantané de base de données avec le compte B en donnant au compte B l'accès à l'instantané.
4. Envoie une notification à la rubrique SNS, puis la rubrique SNS invoque la fonction Lambda dans le compte B.

Dans le compte de destination (compte B dans le schéma), la fonction Lambda exécute la machine d'état Step Functions pour orchestrer les opérations suivantes :

1. Copie l'instantané partagé du compte A vers le compte B, tout en utilisant le AWS KMS key compte A pour déchiffrer les données, puis les chiffrer AWS KMS key à l'aide du compte B intégré.
2. Lit le secret depuis Secrets Manager pour capturer le nom de l'instance de base de données actuelle.
3. Restaure l'instance de base de données à partir du snapshot avec un nouveau nom et un nouveau nom par défaut AWS KMS key pour Amazon RDS.
4. Lit le point de terminaison de la nouvelle base de données et met à jour le secret dans Secrets Manager avec le nouveau point de terminaison de base de données, puis étiquette l'instance de base de données précédente afin qu'elle puisse être supprimée ultérieurement.
5. Conserve les N dernières instances des bases de données et supprime toutes les autres instances.

Outils

Services AWS

- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le. AWS Cloud
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des fonctions Lambda et d'autres fonctions pour créer des applications critiques Services AWS pour l'entreprise.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Crossaccount RDS Replication.

Épopées

Automatisez la réplication des instances de base de données RDS Comptes AWS en un seul clic

Tâche	Description	Compétences requises
Déployez la CloudFormation pile dans le compte source.	1. Connectez-vous au AWS Management Console compte source (compte A) et ouvrez la CloudFormation console. 2. Dans le volet de navigation, choisissez Stack (Piles). 3. Choisissez Créer une pile, puis sélectionnez Avec les ressources existantes (ressources d'importation). 4. Sur la page Identifier les ressources, choisissez Next. 5. Sur la page Spécifier un modèle, sélectionnez Charger un modèle. 6. Choisissez Choisir un fichier, sélectionnez le	Administrateur cloud, architecte cloud

Tâche	Description	Compétences requises
	`Cloudformation-SourceAccountRDS.yaml` fichier dans le référentiel de réplication GitHub Crossaccount RDS, puis choisissez Next. 7. Dans Nom de la pile, entrez le nom de votre pile. 8. Dans la section Paramètres, spécifiez les paramètres définis dans le modèle de pile : • Pour DestinationAccountNumber, entrez le numéro de compte de votre instance de base de données RDS de destination. • Pour KeyName, entrez votre AWS KMS key. • Pour ScheduleExpression, entrez une expression cron (la valeur par défaut est minuit tous les jours). • Dans Source DBIdentifier, entrez le nom de la base de données source. • Dans le champ DBSnapshot Nom de la source, entrez le nom du cliché ou acceptez le nom par défaut. 9. Choisissez Suivant.	

Tâche	Description	Compétences requises
	10. Sur la page Configurer les options de pile, conservez les valeurs par défaut, puis choisissez Next. 11. Passez en revue la configuration de votre pile, puis choisissez Soumettre. 12. Choisissez l'onglet Resources correspondant à votre stack, puis notez le nom de ressource Amazon (ARN) de la rubrique SNS.	

Tâche	Description	Compétences requises
Déployez la CloudFormation pile dans le compte de destination.	1. Connectez-vous au compte AWS Management Console de destination (compte B) et ouvrez la CloudFormation console. 2. Dans le volet de navigation, choisissez Stack (Piles). 3. Choisissez Créer une pile, puis sélectionnez Avec les ressources existantes (ressources d'importation). 4. Sur la page Identifier les ressources, choisissez Next. 5. Sur la page Spécifier un modèle, sélectionnez Charger un modèle. 6. Choisissez un fichier, sélectionnez le **`Cloudformation-DestinationAccountRDS.yaml`** fichier dans le référentiel GitHub Crossaccount RDS Replication, puis choisissez Next. 7. Dans Nom de la pile, entrez le nom de votre pile. 8. Dans la section Paramètres, spécifiez les paramètres définis dans le modèle de pile :	Architecte cloud, DevOps ingénieur, administrateur cloud

Tâche	Description	Compétences requises
	• Pour DatabaseName, entrez un nom pour votre base de données. • Pour Engine, entrez le type de moteur de base de données correspon dant à la base de données source. • Pour DBInstanceClass, entrez le type d'instanc e de base de données préféré ou acceptez le type par défaut. • Pour les groupes de sous-réseaux, entrez le groupe de sous-rése aux VPC existant. Pour obtenir des instructi ons sur la création d'un groupe de sous-rése aux, consultez Étape 2 : Création d'un groupe de sous-réseaux de base de données dans la documentation Amazon RDS. • Pour SecretName, entrez le chemin et le nom du secret, ou acceptez le nom par défaut. • Pour SGID, entrez l'ID du groupe de sécurité de votre cluster de destinati on.	

Tâche	Description	Compétences requises
	• Pour KMSKey, entrez l'ARN de la clé KMS dans votre compte de destination. • Pour NoOfOlderInstances, entrez le nombre d'anciennes copies des instances de base de données RDS que vous souhaitez conserver pour la restauration. 9. Choisissez Suivant. 10. Sur la page Configurer les options de pile, conservez les valeurs par défaut, puis choisissez Next. 11. Passez en revue la configuration de votre pile, puis choisissez Soumettre. 12. Choisissez l'onglet Ressources pour votre pile, puis notez l'ID physique et l'ARN de `InvokeStepFunction`.	

Tâche	Description	Compétences requises
Vérifiez la création de l'instance de base de données RDS dans le compte de destination.	1. Connectez-vous à la console Amazon RDS AWS Management Console et ouvrez-la. 2. Dans le volet de navigation, choisissez Databases, puis vérifiez que la nouvelle instance de base de données RDS apparaît sous le nouveau cluster.	Administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises

Abonnez la fonction Lambda à la rubrique SNS.	Vous devez exécuter les commandes suivantes AWS Command Line Interface (AWS CLI) pour abonner la fonction Lambda du compte de destination (compte B) à la rubrique SNS du compte source (compte A).
	
	Dans le compte A, exécutez la commande suivante :
	
	`aws sns add-permission \ --label lambda-access --aws-account-id <DestinationAccount> \ --topic-arn <Arn of SNSTopic > \ --action-name Subscribe ListSubscriptionsB yTopic`
	
	Dans le compte B, exécutez la commande suivante :
	
	`aws lambda add-permi ssion \ --function-name <Name of InvokeStepFunction > \ --source-arn <Arn of SNSTopic > \ --statement-id function-with-sns \ --action lambda:In vokeFunction \`
		Administrateur cloud, architect e cloud, DBA

Tâche	Description	Compétences requises

	`--principal sns.amazonaws.com`
	
	Dans le compte B, exécutez la commande suivante :
	
	`aws sns subscribe \ --protocol "lambda" \ --topic-arn <Arn of SNSTopic> \ --notification-endpoint <Arn of InvokeStepFunction>`	

Tâche	Description	Compétences requises
Synchronisez l'instance de base de données RDS depuis le compte source avec le compte de destination.	Lancez la réplication de base de données à la demande en démarrant la machine d'état Step Functions dans le compte source. 1. Ouvrez la console Step Functions. 2. Dans le volet de navigation, sélectionnez State machines. 3. Choisissez votre machine à états. 4. Dans l'onglet Exécutions, sélectionnez votre fonction, puis choisissez Démarrer l'exécution pour démarrer le flux de travail. **Note** Un planificateur est en place pour vous aider à exécuter la réplication automatiquement comme prévu, mais il est désactivé par défaut. Vous trouverez le nom de la CloudWatch règle Amazon pour le planificateur dans l'onglet Ressources de la CloudFormation pile	Architecte cloud, DevOps ingénieur, administrateur cloud

Tâche	Description	Compétences requises
	du compte de destination. Pour savoir comment modifier la règle CloudWatch des événements, consultez la section Supprimer ou désactiver une règle d' CloudWatch événements dans la CloudWatch documentation.	
Restaurez votre base de données à l'une des copies précédentes si nécessaire.	1. Ouvrez la console Secrets Manager. 2. Dans la liste des secrets, choisissez le secret que vous avez créé à l'aide du CloudFormation modèle précédent. Votre application utilise le secret pour accéder à la base de données du cluster de destination. 3. Pour mettre à jour la valeur secrète depuis la page de détails, dans la section Valeur secrète, choisissez Récupérer la valeur secrète, puis Modifier. 4. Entrez les détails du point de terminaison de la base de données.	Administrateur cloud, DBA, ingénieur DevOps

Ressources connexes

- Répliques de lecture entre régions (documentation Amazon RDS)
- Déploiements bleu/vert (documentation Amazon RDS)

Informations supplémentaires

Vous pouvez utiliser l'exemple de politique suivant pour partager AWS KMS key le vôtre Comptes AWS.

```
{
    "Version": "2012-10-17",
    "Id": "cross-account-rds-kms-key",
    "Statement": [
        {
            "Sid": "Enable user permissions",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<SourceAccount>:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow administration of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<DestinationAccount>:root"
            },
            "Action": [
                "kms:Create*",
                "kms:Describe*",
                "kms:Enable*",
                "kms:List*",
                "kms:Put*",
                "kms:Update*",
                "kms:Revoke*",
                "kms:Disable*",
                "kms:Get*",
                "kms:Delete*",
                "kms:ScheduleKeyDeletion",
                "kms:CancelKeyDeletion"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::<DestinationAccount>:root",
                    "arn:aws:iam::<SourceAccount>:root"
                ]
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:CreateGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

Sauvegardez automatiquement les bases de données SAP HANA à l'aide de Systems Manager et EventBridge

Créée par Ambarish Satarkar (AWS) et Gaurav Rath (AWS)

Récapitulatif

Ce modèle décrit comment automatiser les sauvegardes de bases de données SAP HANA à l'aide d'AWS Systems Manager, d'Amazon EventBridge, d'Amazon Simple Storage Service (Amazon S3) et d'AWS Backint Agent pour SAP HANA.

Ce modèle fournit une approche basée sur un script shell utilisant la `BACKUP DATA` commande et élimine le besoin de gérer des scripts et des configurations de travail pour chaque instance de système d'exploitation (OS) sur de nombreux systèmes.

> **Note**
>
> En avril 2023, AWS Backup a annoncé la prise en charge des bases de données SAP HANA sur Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez la section Bases de données SAP HANA sur la sauvegarde EC2 des instances Amazon.

Selon les besoins de votre organisation, vous pouvez utiliser le service AWS Backup pour sauvegarder automatiquement vos bases de données SAP HANA ou vous pouvez utiliser ce modèle.

Conditions préalables et limitations

Prérequis

- Une instance SAP HANA existante avec une version prise en charge en cours d'exécution sur une instance Amazon Elastic Compute Cloud (Amazon EC2) gérée et configurée pour Systems Manager
- Systems Manager Agent (SSM Agent) 2.3.274.0 ou version ultérieure installé
- Un compartiment S3 dont l'accès public n'est pas activé

- Une `hdbuserstore` clé nommée `SYSTEM`
- Un rôle AWS Identity and Access Management (IAM) pour que le runbook d'automatisation s'exécute dans les délais
- `AmazonSSMManagedInstanceCore`et `ssm:StartAutomationExecution` les politiques sont associées au rôle de service Systems Manager Automation.

Limites

- AWS Backint Agent pour SAP HANA ne prend pas en charge la déduplication.
- AWS Backint Agent pour SAP HANA ne prend pas en charge la compression des données.

Versions du produit

AWS Backint Agent est pris en charge sur les systèmes d'exploitation suivants :

- SUSE Linux Enterprise Server
- Serveur SUSE Linux Enterprise pour SAP
- Red Hat Enterprise Linux pour SAP

AWS Backint Agent prend en charge les bases de données suivantes :

- SAP HANA 1.0 SP12 (nœud unique et nœuds multiples)
- SAP HANA 2.0 et versions ultérieures (nœud unique et nœuds multiples)

Architecture

Pile technologique cible

- Agent de backint AWS
- Amazon S3
- AWS Systems Manager
- Amazon EventBridge
- SAP HANA

Architecture cible

Le schéma suivant montre les scripts d'installation qui installent AWS Backint Agent, le compartiment S3 et Systems Manager EventBridge et qui utilisent un document de commande pour planifier des sauvegardes régulières.

Automatisation et mise à l'échelle

- Plusieurs agents AWS Backint peuvent être installés à l'aide d'un runbook d'automatisation de Systems Manager.
- Chaque exécution du runbook Systems Manager peut être étendue à un certain nombre d'instances SAP HANA, en fonction de la sélection des cibles.
- EventBridge peut automatiser les sauvegardes SAP HANA.

Outils

- AWS Backint Agent pour SAP HANA est une application autonome qui s'intègre à vos flux de travail existants pour sauvegarder votre base de données SAP HANA dans un compartiment S3 que vous spécifiez dans le fichier de configuration. AWS Backint Agent prend en charge les sauvegardes complètes, incrémentielles et différentielles des bases de données SAP HANA. Il s'exécute sur un serveur de base de données SAP HANA, où les sauvegardes et les catalogues sont transférés de la base de données SAP HANA vers l'agent AWS Backint.
- Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel provenant de vos applications, de vos applications SaaS et des services AWS à des cibles telles que les fonctions AWS Lambda, les points de terminaison d'invocation HTTP utilisant des destinations d'API ou les bus d'événements d'autres comptes.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- AWS Systems Manager vous aide à visualiser et à contrôler votre infrastructure sur AWS. À l'aide de la console Systems Manager, vous pouvez consulter les données opérationnelles de plusieurs services AWS et automatiser les tâches opérationnelles sur l'ensemble de vos ressources AWS.

Code

Le code de ce modèle est disponible dans le aws-backint-automated-backup GitHub référentiel.

Épopées

Créez un système de clés hdbuserstore

Tâche	Description	Compétences requises

Créez une clé hdbuserstore.	1. Accédez à `/usr/sap/<SID>/HDB<InstNo>/exe`.
	2. Exécutez la commande suivante, en indiquant `XX` comme numéro d'instance de base de données SAP HANA.
	`hdbuserstore -i set SYSTEM <hostname>:3XX13@SYSTEMDB SYSTEM`
	Par exemple, pour un hôte SAP HANA `saphanadb` avec un numéro d'instance`00`, exécutez la commande suivante.
	`hdbuserstore -i set SYSTEM saphanadb:30013@SYSTEMDB SYSTEM`
		Administrateur AWS, administrateur SAP HANA

Installation de l'agent AWS Backint

Tâche	Description	Compétences requises
Installez AWS Backint Agent.	Suivez les instructions de la section Installation et	Administrateur AWS, administrateur SAP HANA

Tâche	Description	Compétences requises
	configuration d'AWS Backint Agent pour SAP HANA dans la documentation d'AWS Backint Agent.	

Création du document de commande de Systems Manager

Tâche	Description	Compétences requises
Créez le document de commande de Systems Manager.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Systems Manager. 2. Choisissez Documents, puis Owned by me. 3. Vérifiez que vous vous trouvez dans la même région AWS que votre base de données SAP HANA. 4. Choisissez Créer un document, une commande ou une session pour créer votre document. 5. Utilisez un nom unique et descriptif, sans espaces (par exemple, SAP HANA-Backup). 6. Assurez-vous que le type de document est défini sur Document de commande. 7. Sous l'en-tête Content, vous trouverez un exemple de code. Assurez-vous	Administrateur AWS, administrateur SAP HANA

Tâche	Description	Compétences requises
	de choisir le type de code JSON et de remplacer le code par le code du `HDB_Backup_SSM_Document.json` fichier du GitHub référentiel. 8. Sélectionnez Créer un document. 9. Vérifiez votre document dans la section Possédé par moi.	

Planifiez des sauvegardes à une fréquence régulière

Tâche	Description	Compétences requises
Planifiez des sauvegardes régulières à l'aide d'Amazon EventBridge.	1. Ouvrez la EventBridge console Amazon, choisissez Rules, puis Create rule. 2. Sur l'écran Définir les détails de la règle, entrez un nom et une description uniques pour votre règle, puis utilisez le bus d'événements par défaut. 3. Sous Type de règle, sélectionnez Planifier, puis Suivant. 4. Sur l'écran Définir le calendrier, choisissez le modèle de planification approprié et l'expression	Administrateur AWS, administrateur SAP HANA

Tâche	Description	Compétences requises
	cron ou rate en fonction de la fréquence requise. 5. Sur l'écran Sélectionner les cibles, pour Type de cible, choisissez le service AWS. Sous Sélectionnez une cible, choisissez Systems Manager Run Command. 6. Choisissez le document que vous avez créé précédemment. 7. Sous Clé cible et valeur cible, indiquez l'ID de l'instance. Vous pouvez utiliser les noms et les valeurs des balises pour ajouter plusieurs instances. 8. Sous Configurer les paramètres d'automatisation, choisissez Constant pour les sauvegardes incrémentielles ou différentielles. Si vous souhaitez une sauvegarde complète, sélectionnez Aucun paramètre. 9. Choisissez de créer un nouveau rôle ou d'utiliser un rôle existant. Si vous utilisez un rôle existant, assurez-vous qu'il dispose des politiques requises pour appeler la cible.	

Tâche	Description	Compétences requises
	10. Conservez les paramètres supplémentaires par défaut, puis choisissez Next. 11. L'écran Configurer les balises est facultatif. Choisissez « Suivant ». 12. Sur l'écran Révision et création, passez en revue les paramètres des règles, puis choisissez Créer. La règle doit être créée avec succès. Vous pouvez vérifier le succès de la sauvegarde à partir du chemin du compartiment S3. `s3:/<your_bucket_name>/<target folder>/<SID>/usr/sap/<SID>/SYS/global/hdb/backint/DB_<SID>/` Vous pouvez également vérifier les sauvegardes à partir du catalogue de sauvegarde SAP HANA.	

Ressources connexes

- Agent de backint AWS pour SAP HANA
- Installation et configuration d'AWS Backint Agent pour SAP HANA

Générez automatiquement un modèle PynamoDB et des fonctions CRUD pour Amazon DynamoDB à l'aide d'une application Python

Créée par Vijit Vashishtha (AWS), Dheeraj Alimchandani (AWS) et Dhananjay Karanjkar (AWS)

Récapitulatif

Il est courant d'avoir besoin d'entités et de fonctions d'opérations de création, de lecture, de mise à jour et de suppression (CRUD) pour exécuter efficacement les opérations de base de données Amazon DynamoDB. PynamoDB est une interface basée sur Python qui supporte Python 3. Il fournit également des fonctionnalités telles que la prise en charge des transactions Amazon DynamoDB, la sérialisation et la désérialisation automatiques des valeurs d'attributs, ainsi que la compatibilité avec les frameworks Python courants, tels que Flask et Django. Ce modèle aide les développeurs travaillant avec Python et DynamoDB en fournissant une bibliothèque qui rationalise la création automatique de modèles Pynamodb et de fonctions d'opération CRUD. Bien qu'il génère des fonctions CRUD essentielles pour les tables de base de données, il peut également rétroconcevoir des modèles Pynamodb et des fonctions CRUD à partir de tables Amazon DynamoDB. Ce modèle est conçu pour simplifier les opérations de base de données en utilisant une application basée sur Python.

Les principales caractéristiques de cette solution sont les suivantes :

- Schéma JSON vers modèle Pynamodb — Générez automatiquement des modèles Pynamodb en Python en important un fichier de schéma JSON.
- Génération de fonctions CRUD — Génère automatiquement des fonctions pour effectuer des opérations CRUD sur des tables DynamoDB.
- Rétro-ingénierie à partir de DynamoDB : utilisez le mappage relationnel objet (ORM) PynamoDB pour rétroconcevoir les modèles PynamoDB et les fonctions CRUD pour les tables Amazon DynamoDB existantes.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Python version 3.8 ou ultérieure, téléchargée et installée
- Jinja2 version 3.1.2 ou ultérieure, téléchargée et installée

- Tables Amazon DynamoDB pour lesquelles vous souhaitez générer un ORM
- AWS Command Line Interface (AWS CLI), installé et configuré
- Pynamodb version 5.4.1 ou ultérieure, installée

Architecture

Pile technologique cible

- Script JSON
- Application Python
- Modèle PynamoDB
- Instance de base de données Amazon DynamoDB

Architecture cible

1. Vous créez un fichier de schéma JSON d'entrée. Ce fichier de schéma JSON représente les attributs des tables DynamoDB respectives à partir desquelles vous souhaitez créer des modèles Pynamodb et des fonctions CRUD pour lesquelles vous souhaitez créer des fonctions CRUD. Il contient les trois clés importantes suivantes :
   - `name`: nom de la table DynamoDB cible.
   - `region`— L' Région AWS endroit où la table est hébergée
   - `attributes`— Les attributs qui font partie de la table cible, tels que la clé de partition (également appelée attribut de hachage), la clé de tri, les index secondaires locaux, les indexsecondaires globaux et tout attribut non clé. Cet outil s'attend à ce que le schéma d'entrée fournisse uniquement les attributs non clés, car l'application extrait les attributs clés directement depuis la table cible. Pour un exemple de la manière de spécifier des attributs dans le fichier de schéma JSON, consultez la section Informations supplémentaires de ce modèle.
2. Exécutez l'application Python et fournissez le fichier de schéma JSON en entrée.
3. L'application Python lit le fichier de schéma JSON.
4. L'application Python se connecte aux tables DynamoDB pour dériver le schéma et les types de données. L'application exécute l'opération describe_table et récupère les attributs de clé et d'index de la table.

5. L'application Python combine les attributs du fichier de schéma JSON et de la table DynamoDB. Il utilise le moteur de modèles Jinja pour générer un modèle Pynamodb et les fonctions CRUD correspondantes.
6. Vous accédez au modèle PynamoDB pour effectuer des opérations CRUD sur la table DynamoDB.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.

Autres outils

- Jinja est un moteur de création de modèles extensible qui compile des modèles dans du code Python optimisé. Ce modèle utilise Jinja pour générer du contenu dynamique en intégrant des espaces réservés et de la logique dans les modèles.
- PynamoDB est une interface basée sur Python pour Amazon DynamoDB.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel de modèles Pynamodb et de fonctions CRUD à GitHub générer automatiquement. Le référentiel est divisé en deux parties principales : le package du contrôleur et les modèles.

Package de contrôleur

Le package Python du contrôleur contient la logique d'application principale qui permet de générer le modèle Pynamodb et les fonctions CRUD. Il contient les éléments suivants :

- `input_json_validator.py`— Ce script Python valide le fichier de schéma JSON d'entrée et crée les objets Python contenant la liste des tables DynamoDB cibles et les attributs requis pour chacune d'elles.

- `dynamo_connection.py`— Ce script établit une connexion à la table DynamoDB et utilise `describe_table` l'opération pour extraire les attributs nécessaires à la création du modèle PynamoDB.
- `generate_model.py`— Ce script contient une classe Python `GenerateModel` qui crée le modèle Pynamodb en fonction du fichier de schéma JSON d'entrée et de l'opération. `describe_table`
- `generate_crud.py`— Pour les tables DynamoDB définies dans le fichier de schéma JSON, ce script utilise `GenerateCrud` l'opération de création des classes Python.

Modèles

Ce répertoire Python contient les modèles Jinja suivants :

- `model.jinja`— Ce modèle Jinja contient l'expression du modèle permettant de générer le script du modèle Pynamodb.
- `crud.jinja`— Ce modèle Jinja contient l'expression du modèle permettant de générer le script des fonctions CRUD.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Entrez la commande suivante pour cloner le référentiel de modèles Pynamodb et de fonctions CRUD générés automatiquement. `git clone https://github.com/aws-samples/amazon-reverse-engineer-dynamodb.git`	Développeur d’applications

Tâche	Description	Compétences requises

Configurez l'environnement Python.	1. Accédez au répertoire de premier niveau du référenti el cloné.
	`cd amazon-reverse-eng ineer-dynamodb`
	2. Entrez la commande suivante pour installer les bibliothèques et les packages requis.
	`pip install -r requirements.txt`
		Développeur d’applications

Génération du modèle Pynamodb et des fonctions CRUD

Tâche	Description	Compétences requises
Modifiez le fichier de schéma JSON.	1. Accédez au répertoire de premier niveau du référenti el cloné. `cd amazon-reverse-eng ineer-dynamodb` 2. Ouvrez le `test.json` fichier dans votre éditeur préféré. Vous pouvez utiliser ce fichier comme référence pour créer votre propre fichier de schéma JSON, ou vous pouvez mettre à jour les valeurs	Développeur d’applications

Tâche	Description	Compétences requises
	de ce fichier en fonction de votre environnement. 3. Modifiez le nom et Région AWS les valeurs des attributs de vos tables DynamoDB cibles. **Note** Si vous définissez une table qui n'existe pas dans le fichier de schéma JSON, cette solution ne génère pas de modèles ni de fonctions CRUD pour cette table. 4. Enregistrez et fermez le fichier `test.json` . Nous vous recommandons d'enregistrer ce fichier sous un nouveau nom.	
Exécutez l'application Python.	Entrez la commande suivante pour générer les modèles Pynamodb et les fonctions CRUD, `<input_schema.json>` où est le nom de votre fichier de schéma JSON. `python main.py --file <input_schema.json>`	Développeur d’applications

Vérifiez le modèle Pynamodb et les fonctions CRUD

Tâche	Description	Compétences requises
Vérifiez le modèle Pynamodb généré.	1. Dans le répertoire de premier niveau du référentiel cloné, entrez la commande suivante pour accéder au `models` référentiel. `cd models` 2. Par défaut, cette solution nomme le fichier de modèle Pynamodb. `demo_model.py` Vérifiez que ce fichier est présent.	Développeur d'applications
Vérifiez les fonctions CRUD générées.	1. Dans le répertoire de premier niveau du référentiel cloné, entrez la commande suivante pour accéder au `crud` référentiel. `cd crud` 2. Par défaut, cette solution nomme le script`demo_crud.py` . Vérifiez que ce fichier est présent. 3. Utilisez les classes Python du `demo_crud.py` fichier pour effectuer une opération CRUD sur la table DynamoDB cible.	Développeur d'applications

Tâche	Description	Compétences requises
	Vérifiez que l'opération s'est terminée correctement.	

Ressources connexes

- Composants principaux d'Amazon DynamoDB (documentation DynamoDB)
- Améliorer l'accès aux données grâce aux index secondaires (documentation DynamoDB)

Informations supplémentaires

Exemples d'attributs pour le fichier de schéma JSON

```
[
{
"name": "test_table",
"region": "ap-south-1",
"attributes": [
{
"name": "id",
"type": "UnicodeAttribute"
},
{
"name": "name",
"type": "UnicodeAttribute"
},
{
"name": "age",
"type": "NumberAttribute"
}
]
}
]
```

Bloquez l'accès public à Amazon RDS à l'aide de Cloud Custodian

Créée par Abhay Kumar (AWS) et Dwarika Patra (AWS)

Récapitulatif

De nombreuses entreprises exécutent leurs charges de travail et leurs services auprès de plusieurs fournisseurs de cloud. Dans ces environnements de cloud hybride, l'infrastructure cloud a besoin d'une gouvernance cloud stricte, en plus de la sécurité fournie par les différents fournisseurs de cloud. Une base de données cloud telle qu'Amazon Relational Database Service (Amazon RDS) est un service important qui doit être surveillé pour détecter toute vulnérabilité en matière d'accès et d'autorisation. Bien que vous puissiez restreindre l'accès à la base de données Amazon RDS en configurant un groupe de sécurité, vous pouvez ajouter une deuxième couche de protection pour interdire des actions telles que l'accès public. Le blocage de l'accès public vous aide à respecter le règlement général sur la protection des données (RGPD), la loi HIPAA (Health Insurance Portability and Accountability Act), le National Institute of Standards and Technology (NIST) et la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS).

Cloud Custodian est un moteur de règles open source que vous pouvez utiliser pour appliquer des restrictions d'accès aux ressources Amazon Web Services (AWS) telles qu'Amazon RDS. Avec Cloud Custodian, vous pouvez définir des règles qui valident l'environnement par rapport aux normes de sécurité et de conformité définies. Vous pouvez utiliser Cloud Custodian pour gérer vos environnements cloud en garantissant le respect des politiques de sécurité, des politiques en matière de balises, la collecte des ressources inutilisées et la gestion des coûts. Avec Cloud Custodian, vous pouvez utiliser une interface unique pour mettre en œuvre la gouvernance dans un environnement cloud hybride. Par exemple, vous pouvez utiliser l'interface Cloud Custodian pour interagir avec Microsoft Azure AWS et ainsi réduire les efforts liés à l'utilisation de mécanismes tels que AWS Config les groupes AWS de sécurité et les politiques Azure.

Ce modèle fournit des instructions pour utiliser Cloud Custodian AWS afin de restreindre l'accessibilité publique aux instances Amazon RDS.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une paire de clés

- AWS Lambda installé

Architecture

Le schéma suivant montre le déploiement de la politique par Cloud Custodian AWS Lambda, le AWS CloudTrail lancement de l'`CreateDBInstance`événement et le `PubliclyAccessible` paramétrage de la fonction Lambda sur false sur Amazon RDS.

Outils

Services AWS

- AWS CloudTrailvous aide à auditer la gouvernance, la conformité et le risque opérationnel de votre Compte AWS
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS via des commandes dans votre interface de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le. AWS Cloud

Autres outils

- Cloud Custodian unifie les outils et les scripts utilisés par de nombreuses entreprises pour gérer leurs comptes de cloud public en un seul outil open source. Il utilise un moteur de règles sans état pour la définition et l'application des politiques, avec des métriques, des résultats structurés et des rapports détaillés pour l'infrastructure cloud. Il s'intègre étroitement à un environnement d'exécution sans serveur pour fournir une correction et une réponse en temps réel avec une faible charge opérationnelle.

Épopées

Configurez le AWS CLI

Tâche	Description	Compétences requises
Installez le AWS CLI.	Pour l'installer AWS CLI, suivez les instructions de la AWS documentation.	Administrateur AWS

Configurez les AWS informations d'identification.	Configurez les paramètres avec lesquels les AWS CLI utilisateurs doivent interagir AWS, y compris le Région AWS format de sortie que vous souhaitez utiliser.
	`$>aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]:`
	`Default output format [None]:`
	Pour plus d'informations, consultez la documentation AWS.
		Administrateur AWS

Créez un rôle IAM.	Pour créer un rôle IAM avec le rôle d'exécution Lambda, exécutez la commande suivante. `aws iam create-role --role-name lambda-ex --`	AWS DevOps

Tâche	Description	Compétences requises
	`assume-role-policy-document '{"Version": "2012-10-17","Statement": [{ "Effect": "Allow", "Principal": {"Service": "lambda.amazonaws.com"}, "Action": "sts:AssumeRole"}]}`	

Configurer Cloud Custodian

Tâche	Description	Compétences requises
Installez Cloud Custodian.	Pour installer Cloud Custodian pour votre système d'exploitation et votre environnement, suivez les instructions de la documentation Cloud Custodian.	DevOps ingénieur
Vérifiez le schéma Cloud Custodian.	Pour consulter la liste complète des ressources Amazon RDS sur lesquelles vous pouvez exécuter des politiques, utilisez la commande suivante. `custodian schema aws.rds`	DevOps ingénieur
Créez la politique Cloud Custodian.	Enregistrez le code qui se trouve sous le fichier de politique Cloud Custodian dans la section Informations	DevOps ingénieur

Tâche	Description	Compétences requises
	supplémentaires à l'aide d'une extension YAML.	
Définissez les actions du Cloud Custodian pour modifier le drapeau accessible au public.	1. Localisez le code du dépositaire (par exemple,`/Users/abcd/custodian/lib/python3.9/site-packages/c7n/resources/rds.py`). 2. Localisez la `RDSSetPublicAvailability` classe et modifiez-la en `rds.py` utilisant le code qui se trouve sous le fichier c7n resources rds.py dans la section Informations supplémentaires.	DevOps ingénieur
Effectuez un essai à sec.	(Facultatif) Pour vérifier quelles ressources sont identifiées par la politique sans exécuter aucune action sur les ressources, utilisez la commande suivante. `custodian run -dryrun <policy_name>.yaml -s <output_directory>`	DevOps ingénieur

Déployer la politique

Tâche	Description	Compétences requises
Déployez la politique à l'aide de Lambda.	Pour créer la fonction Lambda qui exécutera la politique, utilisez la commande suivante. `custodian run -s policy.yaml` Cette politique sera ensuite initiée par l' AWS CloudTrail `CreateDBInstance` événement. Par conséquent, le drapeau accessible au public AWS Lambda sera défini sur `false` les instances qui répondent aux critères.	DevOps ingénieur

Ressources connexes

- AWS Lambda website
- Site Web Amazon RDS
- Documentation Cloud Custodian

Informations supplémentaires

Fichier YAML de politique Cloud Custodian

```
policies:
  - name: "block-public-access"
    resource: rds
    description: |
      This Enforcement blocks public access for RDS instances.
```

```
    mode:
      type: cloudtrail
      events:
        - event: CreateDBInstance # Create RDS instance cloudtrail event
          source: rds.amazonaws.com
          ids: requestParameters.dBInstanceIdentifier
      role: arn:aws:iam::1234567890:role/Custodian-compliance-role
    filters:
      - type: event
        key: 'detail.requestParameters.publiclyAccessible'
        value: true
    actions:
      - type: set-public-access
        state: false
```

fichier rds.py de ressources c7n

```
@actions.register('set-public-access')
 class RDSSetPublicAvailability(BaseAction):

     schema = type_schema(
         "set-public-access",
         state={'type': 'boolean'})
     permissions = ('rds:ModifyDBInstance',)

     def set_accessibility(self, r):
         client = local_session(self.manager.session_factory).client('rds')
         waiter = client.get_waiter('db_instance_available')
         waiter.wait(DBInstanceIdentifier=r['DBInstanceIdentifier'])
         client.modify_db_instance(
             DBInstanceIdentifier=r['DBInstanceIdentifier'],
             PubliclyAccessible=self.data.get('state', False))


     def process(self, rds):
         with self.executor_factory(max_workers=2) as w:
             futures = {w.submit(self.set_accessibility, r): r for r in rds}
             for f in as_completed(futures):
                 if f.exception():
                     self.log.error(
                         "Exception setting public access on %s  \n %s",
                         futures[f]['DBInstanceIdentifier'], f.exception())
         return rds
```

Intégration au Security Hub

Cloud Custodian peut être intégré AWS Security Hubpour envoyer des résultats de sécurité et tenter de prendre des mesures correctives. Pour plus d'informations, consultez Annonce de l'intégration de Cloud Custodian avec AWS Security Hub.

Configuration de l'accès intercompte à Amazon DynamoDB

Créée par Shashi Dalmia (AWS), Esteban Serna Parra (AWS) et Imhoertha Ojior (AWS)

Récapitulatif

Ce modèle explique les étapes de configuration de l'accès entre comptes à Amazon DynamoDB à l'aide de politiques basées sur les ressources. Pour les charges de travail qui utilisent DynamoDB, il est de plus en plus courant d'utiliser des stratégies d'isolation des charges de travail afin de minimiser les menaces de sécurité et de répondre aux exigences de conformité. La mise en œuvre de stratégies d'isolation des charges de travail nécessite souvent un accès entre comptes et entre régions aux ressources DynamoDB à l'aide AWS Identity and Access Management de politiques basées sur l'identité (IAM). Cela implique de définir des autorisations IAM et d'établir une relation de confiance entre les Comptes AWS.

Les politiques basées sur les ressources pour DynamoDB simplifient considérablement le dispositif de sécurité pour les charges de travail entre comptes. Ce modèle fournit des étapes et un exemple de code pour montrer comment configurer les AWS Lambda fonctions d'un compte Compte AWS pour écrire des données dans une table de base de données DynamoDB d'un autre compte.

Conditions préalables et limitations

Prérequis

- Deux actifs Comptes AWS. Dans ce schéma, ces comptes sont appelés compte A et compte B.
- AWS Command Line Interface (AWS CLI) installé et configuré pour accéder au compte A, afin de créer la table DynamoDB. Les autres étapes de ce modèle fournissent des instructions d'utilisation des consoles IAM, DynamoDB et Lambda. Si vous prévoyez de l'utiliser à la AWS CLI place, configurez-le pour accéder aux deux comptes.

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Le schéma suivant montre une architecture à compte unique. AWS Lambda, Amazon Elastic Compute Cloud (Amazon EC2) et DynamoDB appartiennent tous au même compte. Dans ce scénario, les fonctions Lambda et les EC2 instances Amazon peuvent accéder à DynamoDB. Pour accorder l'accès à la table DynamoDB, vous pouvez créer une stratégie basée sur l'identité dans IAM ou une stratégie basée sur les ressources dans DynamoDB.

Le schéma suivant montre une architecture multi-comptes. Si les ressources d'un compte Compte AWS nécessitent l'accès à une table DynamoDB dans un autre compte, vous devez configurer une politique basée sur les ressources dans DynamoDB pour accorder l'accès requis. Par exemple, dans le schéma suivant, l'accès à la table DynamoDB du compte A est accordé à une fonction Lambda du compte B à l'aide d'une politique basée sur les ressources.

Ce modèle décrit l'accès entre comptes entre Lambda et DynamoDB. Vous pouvez suivre des étapes similaires pour les autres comptes Services AWS si les autorisations appropriées sont configurées sur les deux comptes. Par exemple, si vous souhaitez fournir à une fonction Lambda un accès à un bucket Amazon Simple Storage Service (Amazon S3) dans le compte A, vous pouvez créer une politique basée sur les ressources dans Amazon S3 et ajouter les autorisations au rôle d'exécution Lambda dans le compte B.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Code

Ce modèle inclut un exemple de code dans la section Informations supplémentaires pour montrer comment configurer une fonction Lambda dans le compte B pour écrire dans la table DynamoDB du

compte A. Le code est fourni uniquement à des fins d'illustration et de test. Si vous implémentez ce modèle dans un environnement de production, utilisez le code comme référence et personnalisez-le pour votre propre environnement.

Bonnes pratiques

- Suivez les meilleures pratiques relatives aux politiques basées sur les ressources dans la documentation DynamoDB.
- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Création d'une politique et d'un rôle IAM pour la fonction Lambda dans le compte B

Tâche	Description	Compétences requises
Créez une politique dans le compte B.	Cette politique IAM autorise l'PutItemaction pour une table DynamoDB dans le compte A. 1. Connectez-vous au compte B dans le AWS Management Console. 2. Ouvrez la console IAM. 3. Dans le volet de navigation, sélectionnez Politiques, puis Créer une politique. 4. Sur la page Spécifier les autorisations, pour l'éditeur de politiques, sélectionnez JSON. 5. Saisissez la politique suivante. `{`	AWS général

Tâche	Description	Compétences requises

	<pre>{
	  "Version":
	 "2012-10-17",
	  "Statement": [
	  {
	  "Sid": "Statemen
	t1",
	  "Effect":
	 "Allow",
	  "Action":
	 "dynamodb:PutItem",
	  "Resource":
	 "arn:aws:dynamodb:
	<Region>:<Account-
	A-ID>:table/Table-
	Account-A"
	  }
	  ]
	}</pre>
	6. Remplacez <Region> et <Account-A-ID> par vos valeurs, puis choisissez Next.
	7. Dans Nom de la politique, entrez un nom unique pour votre politique, tel queDynamoDB-PutItem-Policy .
	8. (Facultatif) Ajoutez une description de la politique.
	9. Choisissez Create Policy (Créer une politique).	

Tâche	Description	Compétences requises
Créez un rôle dans le compte B.	La fonction Lambda du compte B utilise ce rôle IAM pour accéder à la table DynamoDB du compte A. 1. Ouvrez la console IAM. 2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle. 3. Pour Select trusted entity (Sélectionner une entité de confiance), choisissez Service AWS. 4. Dans la section Cas d'utilisation, choisissez Lambda. 5. Choisissez Suivant : Autorisations. 6. Dans la zone Politiques de filtrage, entrez DynamoDB. 7. Dans la liste des politiques DynamoDB, sélectionnez. `DynamoDB-PutItem-Policy` 8. Décochez la case Politiques de filtrage, puis entrez Lambda. 9. Dans la liste des politiques Lambda, choisissez AWSLambda Execute. 10. Choisissez Suivant : Nom, révision et création. 11. Pour Role name (Nom de rôle), saisissez un nom	AWS général

Tâche	Description	Compétences requises
	unique pour votre rôle, par exemple, `DynamoDB-PutItemAccess` . 12. (Facultatif) Ajoutez une description du rôle. 13. (Facultatif) Ajoutez des métadonnées au rôle en associant les identifications sous forme de paires clé-valeur. 14. Choisissez Créer un rôle. Pour plus d'informations sur la création de rôles, consultez la documentation IAM.	
Notez l'ARN du rôle.	1. Ouvrez la console IAM. 2. Dans le panneau de navigation, choisissez Roles (Rôles). 3. Dans la zone de recherche `DynamoDB-PutItemAccess` , entrez, puis choisissez le rôle. 4. Sur la page de résumé du rôle, copiez le nom de ressource Amazon (ARN). Vous utilisez l'ARN lorsque vous configurez la fonction Lambda.	AWS général

Création d'une table DynamoDB dans le compte A

Tâche	Description	Compétences requises

Créez une table DynamoDB.	Utilisez la AWS CLI commande suivante pour créer une table DynamoDB.
	
	`aws dynamodb create-table \`
	`--table-name Table-Account-A \`
	`--attribute-definitions \`
	`Attribute Name=category,AttributeType=S \`
	`Attribute Name=item,AttributeType=S \`
	`--key-schema \`
	`Attribute Name=category,KeyType=HASH \`
	`Attribute Name=item,KeyType=RANGE \`
	`--provisioned-throughput \`
	`ReadCapacityUnits=5,WriteCapacityUnits=5 \`
	`--resource-policy \`
	`'{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Statement1",`
		AWS général

Tâche	Description	Compétences requises

	<pre>"Effect": "Allow",
	"Principal": {
	"AWS": "arn:aws:iam::<Account-B-ID>:role/<Role-Name>"
	},
	"Action": "dynamodb:PutItem",
	"Resource": "arn:aws:dynamodb:<Region>:<Account-A-ID>:table/Table-Account-A"
	}
	
	]
	}'</pre>
	Remplacez le code suivant dans cet exemple de code :
	• `<Account-B-ID>` est l'identifiant du compte B.
	• `<Role-Name>` est le nom du rôle IAM que vous avez créé, par exemple`DynamoDB-PutItemAccess` .
	• `<Region>`est l' Région AWS endroit où vous créez la table DynamoDB.
	• `<Account-A-ID>` est l'identifiant du compte A.	

Tâche	Description	Compétences requises
	Note Vous spécifiez la configuration de la politique basée sur les ressources dans l'`create-table` instruction à l'aide de l'`--resource-policy` indicateur. Cette politique fait référence à l'ARN de la table DynamoDB dans le compte A. Pour plus d'informations sur la création de tables, consultez la documentation DynamoDB.	

Création d'une fonction Lambda dans le compte B

Tâche	Description	Compétences requises
Créez une fonction Lambda pour écrire des données dans DynamoDB.	1. Connectez-vous au compte B dans le AWS Management Console. 2. Ouvrez la console Lambda. 3. Dans le volet de navigation, choisissez Functions, puis Create function. 4. Pour Nom, saisissez `lambda_write_function` .	AWS général

Tâche	Description	Compétences requises
	5. Pour Runtime, choisissez Python 3.8 ou version ultérieure. 6. Sous Modifier le rôle d'exécution par défaut, choisissez Utiliser un rôle existant. 7. Pour Rôle existant, choisissez le rôle IAM que vous avez créé, tel que`DynamoDB-PutItemAccess` . 8. Choisissez Créer une fonction. 9. Dans l'onglet Code, collez l'exemple de code fourni dans la section Informations supplémentaires de ce modèle. Remplacez le code suivant dans cet exemple de code : • `<Account-A-ID>` est l'identifiant du compte A. • `<Region>`est l' Région AWS endroit où vous avez créé la table DynamoDB. 10. Sélectionnez Deploy (Déployer). 11. Sélectionnez Test. Cela vous invite à configurer un événement de test. Créez un nouvel événement	

Tâche	Description	Compétences requises
	avec votre nom préféré, par exemple`MyTestEvent ForWrite` , puis enregistrez la configuration. 12. Choisissez Test à nouveau. Cela exécute la fonction Lambda avec le nom d'événement que vous avez fourni. 13. Vérifiez le résultat de la fonction. Cela doit indiquer que la fonction a accédé à la table DynamoDB dans le compte A et a pu y écrire des données. Pour plus d'informations sur la création de fonctions Lambda, consultez la documentation Lambda.	

Nettoyage

Tâche	Description	Compétences requises
Supprimez des ressources.	Pour éviter les coûts associés aux ressources créées selon ce modèle, procédez comme suit pour supprimer ces ressources : 1. Dans le compte B, supprimez la fonction Lambda que vous avez	AWS général

Tâche	Description	Compétences requises
	créée pour vous connecter à DynamoDB. Pour obtenir des instructions, consultez la documentation Lambda. 2. Dans le compte A, supprimez la table DynamoDB que vous avez créée. Pour obtenir des instructions, consultez la documentation DynamoDB. 3. Pour respecter les meilleures pratiques en matière de sécurité, supprimez la politique IAM (`DynamoDB-PutItem-Policy`) lorsqu'elle n'est plus nécessaire. Pour de plus amples informations, veuillez consulter la documentation IAM. 4. Pour respecter les meilleures pratiques en matière de sécurité, supprimez le rôle IAM (`DynamoDB-PutItemAccess`) lorsqu'il n'est plus nécessaire. Pour de plus amples informations, veuillez consulter la documentation IAM.	

Résolution des problèmes

Problème	Solution
Lors de la création de la fonction Lambda, vous recevez un `ResourceNotFoundException` message d'erreur.	Vérifiez que vous avez correctement saisi le Région AWS et l'ID du compte A. Ils font partie de l'ARN de la table DynamoDB.

Ressources connexes

- Démarrage avec DynamoDB (documentation DynamoDB)
- Commencer à utiliser Lambda (documentation Lambda)
- Utilisation de politiques basées sur les ressources pour DynamoDB (documentation DynamoDB)
- Création de politiques IAM (documentation IAM)
- Logique d'évaluation des politiques entre comptes (documentation IAM)
- Référence des éléments de politique JSON IAM (documentation IAM)

Informations supplémentaires

Exemple de code

```
import boto3
from datetime import datetime

dynamodb_client = boto3.client('dynamodb')

def lambda_handler(event, context):
     now = datetime.now().isoformat()
     data = dynamodb_client.put_item(TableName='arn:aws:dynamodb:<Region>:<Account-
A-ID>:table/Table-Account-A', Item={"category": {"S": "Fruit"},"item": {"S":
 "Apple"},"time": {"S": now}})
     return data
```

> **Note**
>
> Lorsque le client DynamoDB est instancié, l'ARN de la table DynamoDB est fourni à la place du nom de la table. Cela est nécessaire pour que la fonction Lambda se connecte à la bonne table DynamoDB lors de son exécution.

Configurer le routage en lecture seule dans un groupe de disponibilité Always On dans SQL Server sur AWS

Créée par Subhani Shaik (AWS)

Récapitulatif

Ce modèle explique comment utiliser le réplica secondaire de secours dans SQL Server Always On en déchargeant les charges de travail en lecture seule du réplica principal vers le réplica secondaire.

La mise en miroir de bases de données comporte un one-to-one mappage. Comme vous ne pouvez pas lire directement la base de données secondaire, vous devez créer des instantanés. La fonctionnalité de groupe de disponibilité Always On a été introduite dans Microsoft SQL Server 2012. Dans les versions ultérieures, des fonctionnalités majeures ont été introduites, notamment le routage en lecture seule. Dans les groupes de disponibilité Always On, vous pouvez lire les données directement à partir du réplica secondaire en passant le mode de réplication en lecture seule.

La solution de groupes de disponibilité Always On prend en charge la haute disponibilité (HA), la reprise après sinistre (DR) et constitue une alternative à la mise en miroir de bases de données. Les groupes de disponibilité Always On fonctionnent au niveau de la base de données et optimisent la disponibilité d'un ensemble de bases de données utilisateur.

SQL Server utilise le mécanisme de routage en lecture seule pour rediriger les connexions en lecture seule entrantes vers le réplica en lecture secondaire. Pour ce faire, vous devez ajouter les paramètres et valeurs suivants dans la chaîne de connexion :

- `ApplicationIntent=ReadOnly`
- `Initial Catalog=<database name>`

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec un cloud privé virtuel (VPC), deux zones de disponibilité, des sous-réseaux privés et un groupe de sécurité
- Deux machines Amazon Elastic Compute Cloud (Amazon EC2) avec SQL Server 2019 Enterprise Edition Amazon Machine Image avec Windows Server Failover Clustering (WSFC) configuré au niveau de l'instance et un groupe de disponibilité Always On configuré au niveau SQL Server entre

le nœud principal (`WSFCNODE1`) et le nœud secondaire (`WSFCNODE2`), qui font partie du répertoire AWS Directory Service pour Microsoft Active Directory nommé `tagechtalk.com`

- Un ou plusieurs nœuds configurés pour être acceptés `read-only` dans la réplique secondaire
- Un écouteur nommé d'après `SQLAG1` le groupe de disponibilité Always On
- Moteur de base de données SQL Server exécuté avec le même compte de service sur deux nœuds
- Studio de gestion SQL Server (SSMS)
- Une base de données de test nommée `test`

Versions du produit

- SQL Server 2014 et versions ultérieures

Architecture

Pile technologique cible

- Amazon EC2
- AWS Managed Microsoft AD
- Amazon FSx

Architecture cible

Le schéma suivant montre comment l'écouteur du groupe de disponibilité Always On (AG) redirige les requêtes contenant le `ApplicationIntent` paramètre dans la connexion vers le nœud secondaire approprié.

1. Une demande est envoyée à l'écouteur du groupe de disponibilité Always On.
2. Si la chaîne de connexion ne contient pas le `ApplicationIntent` paramètre, la demande est envoyée à l'instance principale.
3. Si la chaîne de connexion contient`ApplicationIntent=ReadOnly`, la demande est envoyée à l'instance secondaire avec une configuration de routage en lecture seule, qui est WSFC avec un groupe de disponibilité Always On.

Outils

Services AWS

- AWS Directory Service pour Microsoft Active Directory permet à vos charges de travail sensibles aux annuaires et à vos ressources AWS d'utiliser Microsoft Active Directory dans le cloud AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon FSx fournit des systèmes de fichiers qui prennent en charge les protocoles de connectivité standard du secteur et offrent une disponibilité et une réplication élevées dans les régions AWS.

Autres services

- SQL Server Management Studio (SSMS) est un outil permettant de connecter, de gérer et d'administrer les instances de SQL Server.
- sqlcmd est un utilitaire de ligne de commande.

Bonnes pratiques

Pour plus d'informations sur les groupes de disponibilité Always On, consultez la documentation de SQL Server.

Épopées

Configurer le routage en lecture seule

Tâche	Description	Compétences requises
Mettez à jour les répliques en lecture seule.	Pour mettre à jour le réplica principal et le réplica secondaire en lecture seule, connectez-vous au réplica principal depuis SSMS et exécutez le code de l'étape 1 dans la section Informations supplémentaires.	DBA

Tâche	Description	Compétences requises
Créez l'URL de routage.	Pour créer une URL de routage pour les deux répliques, exécutez le code de l'étape 2 dans la section Informations supplémentaires. Dans ce code, `tagechtalk.com` se trouve le nom du répertoire Microsoft AD géré par AWS.	DBA
Créez la liste de routage.	Pour créer la liste de routage pour les deux répliques, exécutez le code de l'étape 3 dans la section Informations supplémentaires.	DBA
Validez la liste de routage.	Connectez-vous à l'instance principale depuis SQL Server Management Studio et exécutez le code de l'étape 4 de la section Informations supplémentaires pour valider la liste de routage.	DBA

Tester le routage en lecture seule

Tâche	Description	Compétences requises
Connectez-vous à l'aide du ApplicationIntent paramètre.	1. À partir de SSMS, connectez-vous au nom de l'écouteur du groupe de disponibilité Always On avec. `ApplicationIntent=ReadOnly;`	DBA

Tâche	Description	Compétences requises

	`Initial Catalog=test`
	2. La connexion est établie avec la réplique secondaire. Pour tester cela, exécutez la commande suivante pour afficher le nom du serveur connecté.
	`SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')`
	La sortie indiquera le nom de la réplique secondaire actuelle (`WSFCNODE2`).	

Tâche	Description	Compétences requises
Effectuez un basculement.	1. À partir de SSMS, connectez-vous au nom du récepteur du groupe de disponibilité Always On. 2. Vérifiez que les bases de données principale et secondaire sont synchronisées, sans perte de données. 3. Effectuez un basculement afin que le réplica principal actuel devienne le réplica secondaire et que le réplica secondaire devienne le réplica principal. 4. À partir de SSMS, connectez-vous au nom de l'écouteur du groupe de disponibilité Always On avec. `ApplicationIntent=ReadOnly; Initial Catalog=test` 5. La connexion est établie avec la réplique secondaire. Pour tester cela, affichez le nom du serveur connecté en exécutant la commande suivante. `SELECT SERVERPROPERTY('ComputerNamePhysicalNetBios')`	DBA

Tâche	Description	Compétences requises
	Il affichera le nom de la réplique secondaire actuelle (`WSFCNODE1`).	

Connectez-vous à l'aide de l'utilitaire de ligne de commande sqlcmd

Tâche	Description	Compétences requises
Connectez-vous à l'aide de sqlcmd.	Pour vous connecter à partir de sqlcmd, exécutez le code de l'étape 5 dans la section Informations supplémentaires à l'invite de commande. Une fois connecté, exécutez la commande suivante pour afficher le nom du serveur connecté. `SELECT SERVERPRO PERTY('Computernam ePhysicalNetBios') .` La sortie affichera le nom de la réplique secondaire actuelle (`WSFCNODE1`).	DBA

Résolution des problèmes

Problème	Solution
La création de l'écouteur échoue avec le message « Le cluster WSFC n'a pas pu mettre la ressource de nom de réseau en ligne ».	Pour plus d'informations, consultez le billet de blog Microsoft Create Listener Fails with

Problème	Solution
	Message « The WSFC cluster could not bring the Network Name resource online ».
Problèmes potentiels, notamment d'autres problèmes liés à l'écouteur ou à l'accès au réseau.	Consultez la section Résolution des problèmes de configuration des groupes de disponibilité Always On (SQL Server) dans la documentation Microsoft.

Ressources connexes

- Configurer le routage en lecture seule pour un groupe de disponibilité Always On
- Résolution des problèmes de configuration des groupes de disponibilité Always On (SQL Server)

Informations supplémentaires

Étape 1. Mettre à jour les répliques en lecture seule

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (ALLOW_CONNECTIONS = READ_ONLY))
GO
```

Étape 2. Création de l'URL de routage

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode1.tagechtalk.com:1433'))
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (SECONDARY_ROLE
 (READ_ONLY_ROUTING_URL = N'TCP://WSFCNode2.tagechtalk.com:1433'))
GO
```

Étape 3. Création de la liste de routage

```
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE1' WITH
 (PRIMARY_ROLE(READ_ONLY_ROUTING_LIST=('WSFCNODE2','WSFCNODE1')));
```

```
GO
ALTER AVAILABILITY GROUP [SQLAG1] MODIFY REPLICA ON N'WSFCNODE2' WITH (PRIMARY_ROLE
 (READ_ONLY_ROUTING_LIST=('WSFCNODE1','WSFCNODE2')));
GO
```

Étape 4. Valider la liste de routage

```
SELECT AGSrc.replica_server_name AS PrimaryReplica, AGRepl.replica_server_name AS
 ReadOnlyReplica, AGRepl.read_only_routing_url AS RoutingURL , AGRL.routing_priority
 AS RoutingPriority FROM sys.availability_read_only_routing_lists AGRL INNER JOIN
 sys.availability_replicas AGSrc ON AGRL.replica_id = AGSrc.replica_id INNER JOIN
 sys.availability_replicas AGRepl ON AGRL.read_only_replica_id = AGRepl.replica_id
 INNER JOIN sys.availability_groups AV ON AV.group_id = AGSrc.group_id ORDER BY
 PrimaryReplica
```

Étape 5. Utilitaire de commande SQL

```
sqlcmd -S SQLAG1,1433 -E -d test -K ReadOnly
```

Connectez-vous en utilisant un tunnel SSH dans pgAdmin

Créée par Jeevan Shetty (AWS) et Bhanu Ganesh Gudivada (AWS)

Récapitulatif

Pour des raisons de sécurité, il est toujours préférable de placer les bases de données dans un sous-réseau privé. Les requêtes sur la base de données peuvent être exécutées en se connectant via un hôte bastion Amazon Elastic Compute Cloud (Amazon EC2) dans un sous-réseau public du cloud Amazon Web Services (AWS). Cela nécessite l'installation de logiciels tels que pgAdmin DBeaver ou, couramment utilisés par les développeurs ou les administrateurs de bases de données, sur l'hôte Amazon. EC2

L'exécution de pgAdmin sur un serveur Linux et l'accès à celui-ci via un navigateur Web nécessitent l'installation de dépendances, d'autorisations et de configurations supplémentaires.

Comme solution alternative, les développeurs ou les administrateurs de base de données peuvent se connecter à une base de données PostgreSQL en utilisant pgAdmin pour activer un tunnel SSH depuis leur système local. Dans cette approche, pgAdmin utilise l'hôte EC2 Amazon du sous-réseau public comme hôte intermédiaire avant de se connecter à la base de données. Le schéma de la section Architecture montre la configuration.

> **Note**
>
> Assurez-vous que le groupe de sécurité attaché à la base de données PostgreSQL autorise la connexion sur le port 5432 depuis l'hôte Amazon. EC2

Conditions préalables et limitations

Prérequis

- Un compte AWS existant
- Un cloud privé virtuel (VPC) avec un sous-réseau public et un sous-réseau privé
- Une EC2 instance associée à un groupe de sécurité
- Une base de données Amazon Aurora PostgreSQL Edition associée à un groupe de sécurité
- Une paire de clés Secure Shell (SSH) pour configurer le tunnel

Versions du produit

- Version 6.2+ de pgAdmin
- Édition compatible avec Amazon Aurora PostgreSQL version 12.7+

Architecture

Pile technologique cible

- Amazon EC2
- Compatible avec Amazon Aurora PostgreSQL

Architecture cible

Le schéma suivant montre l'utilisation de pgAdmin avec un tunnel SSH pour se connecter via une passerelle Internet à l'instance, qui se connecte à EC2 la base de données.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.

Autres services

- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Épopées

Créez la connexion

Tâche	Description	Compétences requises
Créez un serveur.	Dans pgAdmin, choisisse z Create, puis Server. Pour obtenir de l'aide supplémen taire sur la configuration de pgAdmin afin d'enregistrer un serveur, de configurer une connexion et de se connecter via le tunneling SSH à l'aide de la boîte de dialogue du serveur, consultez les liens dans la section Ressources connexes.	DBA
Donnez un nom au serveur.	Dans l'onglet Général, entrez un nom.	DBA
Entrez les détails de la base de données.	Dans l'onglet Connexion, entrez les valeurs suivantes : • Nom/adresse de l'hôte • Port • Base de données de maintenance • Username • Mot de passe :	DBA
Entrez les détails EC2 du serveur Amazon.	Dans l'onglet Tunnel SSH, fournissez les détails de l' EC2 instance Amazon qui se trouve dans le sous-réseau public.	DBA

Tâche	Description	Compétences requises
	• Définissez Use SSH tunneling sur Yes pour spécifier que pgAdmin doit utiliser un tunnel SSH lors de la connexion au serveur spécifié. • Dans le champ Hôte du tunnel, spécifiez le nom ou l'adresse IP de l'hôte SSH (par exemple, 10.x.x.x). • Dans le champ Port du tunnel, spécifiez le port de l'hôte SSH (par exemple, 22). • Dans le champ Nom d'utilisateur, spécifiez le nom d'un utilisateur disposant de privilèges de connexion pour l'hôte SSH (par exemple, ec2-user). • Spécifiez le type d'authentification sous forme de fichier d'identité afin que pgAdmin utilise un fichier de clé privée lors de la connexion. • Indiquez l'emplacement du fichier PEM (Privacy Enhanced Mail) dans le champ Fichier d'identité. Le fichier .pem est la paire de EC2 clés Amazon.	

Tâche	Description	Compétences requises
Enregistrez et connectez-vous.	Choisissez Enregistrer pour terminer la configuration et vous connecter à la base de données compatible Aurora PostgreSQL à l'aide du tunnel SSH.	DBA

Ressources connexes

- Boîte de dialogue du serveur
- Se connecter au serveur

Convertir les requêtes Oracle JSON en SQL de base de données PostgreSQL

Créée par Pinesh Singal (AWS) et Lokesh Gurram (AWS)

Récapitulatif

Ce processus de migration pour passer d'une solution sur site au cloud Amazon Web Services (AWS) utilise l'outil AWS Schema Conversion Tool (AWS SCT) pour convertir le code d'une base de données Oracle en une base de données PostgreSQL. La majeure partie du code est automatiquement convertie par AWS SCT. Toutefois, les requêtes Oracle liées à JSON ne sont pas automatiquement converties.

À partir de la version Oracle 12.2, Oracle Database prend en charge diverses fonctions JSON qui aident à convertir les données JSON en données basées sur les lignes. Cependant, AWS SCT ne convertit pas automatiquement les données basées sur JSON dans un langage pris en charge par PostgreSQL.

Ce modèle de migration se concentre principalement sur la conversion manuelle des requêtes Oracle liées au JSON avec des fonctions telles que `JSON_OBJECT`, `JSON_ARRAYAGG`, et d'une base `JSON_TABLE` de données Oracle vers une base de données PostgreSQL.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance de base de données Oracle sur site (opérationnelle)
- Une instance de base de données Amazon Relational Database Service (Amazon RDS) pour PostgreSQL ou Amazon Aurora PostgreSQL Edition compatible (opérationnelle)

Limites

- Les requêtes liées au JSON nécessitent un format fixe `KEY` et un format. `VALUE` Le fait de ne pas utiliser ce format renvoie un résultat erroné.
- Si une modification de la structure JSON ajoute de nouvelles `VALUE` paires `KEY` et de nouvelles paires dans la section des résultats, la procédure ou la fonction correspondante doit être modifiée dans la requête SQL.

- Certaines fonctions liées au JSON sont prises en charge dans les versions antérieures d'Oracle et de PostgreSQL, mais avec moins de fonctionnalités.

Versions du produit

- Oracle Database version 12.2 et versions ultérieures
- Version 9.5 et ultérieure compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL
- Dernière version d'AWS SCT (testée à l'aide de la version 1.0.664)

Architecture

Pile technologique source

- Une instance de base de données Oracle avec la version 19c

Pile technologique cible

- Une instance de base de données compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL avec la version 13

Architecture cible

1. Utilisez AWS SCT avec le code de fonction JSON pour convertir le code source d'Oracle vers PostgreSQL.
2. La conversion produit des fichiers .sql migrés compatibles avec PostgreSQL.
3. Convertissez manuellement les codes de fonction Oracle JSON non convertis en codes de fonction JSON PostgreSQL.
4. Exécutez les fichiers .sql sur l'instance de base de données cible compatible Aurora PostgreSQL.

Outils

Services AWS

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré conçu pour le cloud et compatible avec MySQL et PostgreSQL.

- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Autres services

- Oracle SQL Developer est un environnement de développement intégré qui simplifie le développement et la gestion des bases de données Oracle dans les déploiements traditionnels et basés sur le cloud.
- pgAdmin ou. DBeaver pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données. DBeaverest un outil de base de données universel.

Bonnes pratiques

La requête Oracle utilise `CAST` le type par défaut lors de l'utilisation de la `JSON_TABLE` fonction. Il est recommandé de l'utiliser également `CAST` dans PostgreSQL, en utilisant deux fois plus de caractères (). >>

Pour plus d'informations, consultez Postgres_SQL_Read_JSON dans la section Informations supplémentaires.

Épopées

Générez les données JSON dans les bases de données Oracle et PostgreSQL

Tâche	Description	Compétences requises
Stockez les données JSON dans la base de données Oracle.	Créez une table dans la base de données Oracle et stockez les données JSON dans la `CLOB` colonne. Utilisez le script Oracle_Table_Creation_Insert_Script qui se trouve	Ingénieur en migration

Tâche	Description	Compétences requises
	dans la section Informations supplémentaires.	
Stockez les données JSON dans la base de données PostgreSQL.	Créez une table dans la base de données PostgreSQL et stockez les données JSON dans la colonne. `TEXT` Utilisez le Postgres_Table_Creation_Insert_Script qui se trouve dans la section Informations supplémentaires.	Ingénieur en migration

Convertissez le JSON au format ROW

Tâche	Description	Compétences requises
Convertissez les données JSON dans la base de données Oracle.	Rédigez une requête Oracle SQL pour lire les données JSON au format ROW. Pour plus de détails et des exemples de syntaxe, consultez Oracle_SQL_Read_JSON dans la section Informations supplémentaires.	Ingénieur en migration
Convertissez les données JSON dans la base de données PostgreSQL.	Rédigez une requête PostgreSQL pour lire les données JSON au format ROW. Pour plus de détails et des exemples de syntaxe, consultez Postgres_SQL_Read_JSON dans la section Informations supplémentaires.	Ingénieur en migration

Convertissez manuellement les données JSON à l'aide de la requête SQL et rapportez le résultat au format JSON

Tâche	Description	Compétences requises
Effectuez des agrégations et des validations sur la requête SQL Oracle.	Pour convertir manuellement les données JSON, effectuez une jointure, une agrégation et une validation sur la requête SQL Oracle, puis rapportez le résultat au format JSON. Utilisez le code sous Oracle_SQL_JSON_Aggregation_Join dans la section Informations supplémentaires. 1. JOIN — Les données au format JSON sont transmises en tant que paramètre d'entrée à la requête. Un JOIN interne est créé entre ces données statiques et les données JSON de la table de base de données Oracle`aws_test_table` . 2. Agrégation avec validation — Les données JSON `KEY` contiennent des `VALUE` paramètres contenant des valeurs telles que `accountNumber parentAccountNumber` , `businessUnitId` et`positionId` , qui sont	Ingénieur en migration

Tâche	Description	Compétences requises
	utilisés pour les `SUM` `COUNT` agrégations. 3. Format JSON — Après la jointure et l'agrégat ion, les données sont rapportées au format JSON à l'aide de `JSON_OBJECT` et`JSON_ARRAYAGG` .	

Tâche	Description	Compétences requises
Effectuez des agrégations et des validations sur la requête SQL Postgres.	Pour convertir manuellement les données JSON, effectuez une jointure, une agrégation et une validation sur la requête PostgreSQL, puis rapportez le résultat au format JSON. Utilisez le code situé sous Postgres_SQL_JSON_Aggregation_Join dans la section Informations supplémentaires. 1. JOIN — Les données au format JSON (`tab1`) sont transmises en tant que paramètre d'entrée à la `WITH` requête de clause. Un JOIN est créé entre ces données statiques et les données JSON, qui se trouvent dans le `tab` tableau. Un JOIN est également créé avec la `WITH` clause, qui contient des données JSON dans la `aws_test_pg_table` table. 2. Agrégation — Les données JSON `KEY` contiennent des `VALUE` paramètres avec des valeurs telles que `accountNumber parentAccountNumbe`	Ingénieur en migration

Tâche	Description	Compétences requises
	`r` ,`businessUnitId` , et`positionId` , qui sont utilisés pour les `COUNT` agrégations `SUM` et. 3. Format JSON — Après la jointure et l'agrégation, les données sont rapportées au format JSON à l'aide de `JSON_BUILD_OBJECT` et`JSON_AGG`.	

Convertir la procédure Oracle en une fonction PostgreSQL contenant des requêtes JSON

Tâche	Description	Compétences requises
Convertissez les requêtes JSON de la procédure Oracle en lignes.	Pour l'exemple de procédure Oracle, utilisez la requête Oracle précédente et le code situé sous Oracle_Procedure_with_JSON_Query dans la section Informations supplémentaires.	Ingénieur en migration
Convertissez les fonctions PostgreSQL qui comportent des requêtes JSON en données basées sur des lignes.	Pour les exemples de fonctions PostgreSQL, utilisez la requête PostgreSQL précédente et le code qui se trouve sous Postgres_Function_with_JSON_Query dans la section Informations supplémentaires.	Ingénieur en migration

Ressources connexes

- Fonctions Oracle JSON
- Fonctions JSON de PostgreSQL
- Exemples de fonctions Oracle JSON
- Exemples de fonctions JSON PostgreSQL
- Outil de conversion de schéma AWS

Informations supplémentaires

Pour convertir le code JSON de la base de données Oracle vers la base de données PostgreSQL, utilisez les scripts suivants, dans l'ordre.

1. Oracle_Table_Creation_Insert_Script

```
create table aws_test_table(id number,created_on date default sysdate,modified_on
 date,json_doc clob);

REM INSERTING into EXPORT_TABLE
SET DEFINE OFF;
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc)
values (1,to_date('02-AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022
 12:30:14','DD-MON-YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
    "arrayPattern" : " -'",
    "a]')
|| TO_CLOB(q'[ccount" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
```

```
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
]')
|| TO_CLOB(q'[        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));
Insert into aws_test_table (ID,CREATED_ON,MODIFIED_ON,json_doc) values (2,to_date('02-
AUG-2022 12:30:14','DD-MON-YYYY HH24:MI:SS'),to_date('02-AUG-2022 12:30:14','DD-MON-
YYYY HH24:MI:SS'),TO_CLOB(q'[{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "pqr@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -'",
    "account" : {
      "companyId" : "CARS",
      "busin]')
|| TO_CLOB(q'[essUnitId" : 6,
      "accountNumber" : 42001,
```

```
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
      ]')
|| TO_CLOB(q'[  "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}]'));

commit;
```

2. Postgres_Table_Creation_Insert_Script

```
create table aws_test_pg_table(id int,created_on date ,modified_on date,json_doc text);
insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(1,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0100",
```

```
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
      "businessUnitId" : 7,
      "accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');


insert into aws_test_pg_table(id,created_on,modified_on,json_doc)
values(2,now(),now(),'{
  "metadata" : {
    "upperLastNameFirstName" : "PQR XYZ",
    "upperEmailAddress" : "pqr@gmail.com",
    "profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "54534343",
    "displayName" : "Xyz, pqr",
    "firstName" : "pqr",
    "lastName" : "Xyz",
    "emailAddress" : "a*b**@h**.k**",
    "productRegistrationStatus" : "Not registered",
    "positionId" : "0090",
    "arrayPattern" : " -",
    "account" : {
```

```
      "companyId" : "CARS",
      "businessUnitId" : 6,
      "accountNumber" : 42001,
      "parentAccountNumber" : 32001,
      "firstName" : "terry",
      "lastName" : "whitlock",
      "street1" : "UO  123",
      "city" : "TOTORON",
      "region" : "NO",
      "postalcode" : "LKM 111",
      "country" : "Canada"
    },
    "products" : [
      {
        "appUserGuid" : "ia744d7790000016899f8cf3f417d6df6",
        "id" : "0000000014",
        "name" : "ProView eLooseleaf",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}');
```

3. Oracle_SQL_Read_JSON

Les blocs de code suivants montrent comment convertir des données Oracle JSON au format de ligne.

Exemple de requête et de syntaxe

```
SELECT   JSON_OBJECT(
 'accountCounts' VALUE JSON_ARRAYAGG(
           JSON_OBJECT(
               'businessUnitId' VALUE business_unit_id,
                       'parentAccountNumber' VALUE parent_account_number,
                       'accountNumber' VALUE account_number,
                       'totalOnlineContactsCount' VALUE online_contacts_count,
                       'countByPosition' VALUE
                   JSON_OBJECT(
                       'taxProfessionalCount' VALUE tax_count,
                       'attorneyCount' VALUE attorney_count,
                       'nonAttorneyCount' VALUE non_attorney_count,
```

```
                        'clerkCount' VALUE clerk_count
                               ) ) ) ) FROM
   (SELECT   tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
clerk_count
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
 COLUMNS (
         parent_account_number NUMBER PATH
          '$.data.account.parentAccountNumber',
           account_number NUMBER PATH '$.data.account.accountNumber',
           business_unit_id NUMBER PATH '$.data.account.businessUnitId',
           position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
           ) AS tab_data
           INNER JOIN JSON_TABLE ( '{
       "accounts": [{
         "accountNumber": 42000,
         "parentAccountNumber": 32000,
         "businessUnitId": 7
       }, {
         "accountNumber": 42001,
         "parentAccountNumber": 32001,
         "businessUnitId": 6
       }]
     }', '$.accounts[*]' ERROR ON ERROR
     COLUMNS (
     parent_account_number PATH '$.parentAccountNumber',
     account_number PATH '$.accountNumber',
     business_unit_id PATH '$.businessUnitId')
     ) static_data
     ON ( static_data.parent_account_number = tab_data.parent_account_number
          AND static_data.account_number = tab_data.account_number
          AND static_data.business_unit_id = tab_data.business_unit_id )
       GROUP BY
           tab_data.business_unit_id,
           tab_data.parent_account_number,
```

```
            tab_data.account_number );
```

Le document JSON stocke les données sous forme de collections. Chaque collection peut avoir KEY et être VALUE associée. Chacun VALUE peut avoir des nids KEY et des VALUE paires. Le tableau suivant fournit des informations sur la lecture VALUE du document JSON spécifique.

CLÉ	HIÉRARCHIE ou CHEMIN à utiliser pour obtenir la VALEUR	VALEUR
`profileType`	`metadata` -> `profileType`	« P »
`positionId`	`data` -> `positionId`	« 0100"
`accountNumber`	`data`-> compte -> `accountNumber`	42000

Dans le tableau précédent, KEY `profileType` il s'agit VALUE d'un des `metadata`KEY. KEY`positionId`C'est VALUE l'un des `data`KEY. Le KEY `accountNumber` est un VALUE du `account`KEY, et le `account` KEY est un VALUE du `data`KEY.

Exemple de document JSON

```
{
  "metadata" : {
    "upperLastNameFirstName" : "ABC XYZ",
    "upperEmailAddress" : "abc@gmail.com",
"profileType" : "P"
  },
  "data" : {
    "onlineContactId" : "032323323",
    "displayName" : "Abc, Xyz",
    "firstName" : "Xyz",
    "lastName" : "Abc",
    "emailAddress" : "abc@gmail.com",
    "productRegistrationStatus" : "Not registered",
"positionId" : "0100",
    "arrayPattern" : " -",
    "account" : {
      "companyId" : "SMGE",
```

```
      "businessUnitId" : 7,
"accountNumber" : 42000,
      "parentAccountNumber" : 32000,
      "firstName" : "john",
      "lastName" : "doe",
      "street1" : "retOdertcaShr ",
      "city" : "new york",
      "postalcode" : "XY ABC",
      "country" : "United States"
    },
    "products" : [
      {
        "appUserGuid" : "i0acc4450000001823fbad478e2eab8a0",
        "id" : "0000000046",
        "name" : "ProView",
        "domain" : "EREADER",
        "registrationStatus" : false,
        "status" : "11"
      }
    ]
  }
}
```

Requête SQL utilisée pour obtenir les champs sélectionnés à partir du document JSON

```
select parent_account_number,account_number,business_unit_id,position_id from
 aws_test_table aws,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
COLUMNS (
parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
account_number NUMBER PATH '$.data.account.accountNumber',
business_unit_id NUMBER PATH '$.data.account.businessUnitId',
position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'
)) as sc
```

Dans la requête précédente, `JSON_TABLE` il existe une fonction intégrée à Oracle qui convertit les données JSON au format de ligne. La fonction JSON_TABLE attend des paramètres au format JSON.

Chaque élément `COLUMNS` possède un élément prédéfini`PATH`, et un élément approprié `VALUE` pour un élément donné `KEY` est renvoyé sous forme de ligne.

Résultat de la requête précédente

NUMÉRO_COMPTE_PARENT	NUMÉRO DE COMPTE	IDENTIFIANT DE L'UNITÉ_ENTREPRISE	IDENTIFIANT DE POSITION
32000	42000	7	0100
32001	42001	6	0090

4. Postgres_SQL_Read_JSON

Exemple de requête et de syntaxe

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::VARCHAR as positionId
from aws_test_pg_table) d ;
```

Dans Oracle, PATH est utilisé pour identifier le KEY et spécifiqueVALUE. Cependant, PostgreSQL utilise HIERARCHY un modèle pour KEY lire VALUE et à partir de JSON. Les mêmes données JSON mentionnées ci-dessous Oracle_SQL_Read_JSON sont utilisées dans les exemples suivants.

Requête SQL de type CAST non autorisée

(Si vous forcez le CAST texte, la requête échoue avec une erreur de syntaxe.)

```
select *
from (
select (json_doc::json->'data'->'account'->'parentAccountNumber') as
 parentAccountNumber,
(json_doc::json->'data'->'account'->'accountNumber')as accountNumber,
(json_doc::json->'data'->'account'->'businessUnitId') as businessUnitId,
(json_doc::json->'data'->'positionId')as positionId
from aws_test_pg_table) d ;
```

L'utilisation d'un seul opérateur supérieur à (>) renverra le résultat VALUE défini pour cela. KEY Par exemple, KEY :positionId, et VALUE :"0100".

CASTLe type n'est pas autorisé lorsque vous utilisez le seul opérateur supérieur à ()>.

Requête SQL de type CAST autorisée

```
select *
from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) d ;
```

Pour utiliser le typeCAST, vous devez utiliser l'opérateur double supérieur à. Si vous utilisez l'opérateur unique supérieur à, la requête renvoie le paramètre VALUE défini (par exemple, KEY :positionId, et VALUE :"0100"). L'utilisation de l'opérateur double supérieur à (>>) renvoie la valeur réelle définie pour cela KEY (par exemple, KEY :, et VALUE : positionId0100, sans guillemets).

Dans le cas précédent, parentAccountNumber est type CAST àINT, accountNumber est type CAST àINT, businessUnitId est type CAST à INT et positionId est type CAST àVARCHAR.

Les tableaux suivants présentent les résultats des requêtes qui expliquent le rôle de l'opérateur supérieur unique (>) et de l'opérateur double supérieur (). >>

Dans le premier tableau de table, la requête utilise l'opérateur unique supérieur à ()>. Chaque colonne est de type JSON et ne peut pas être convertie en un autre type de données.

parentAccountNumber	Numéro de compte	businessUnitId	ID du poste
2003565430	2003564830	7	« 0100 »
2005284042	2005284042	6	« 0090 »
2000272719	2000272719	1	« 0100 »

Dans le second tableau, la requête utilise l'opérateur double supérieur à ()>>. Chaque colonne prend en charge le type en CAST fonction de la valeur de la colonne. Par exemple, INTEGER dans ce contexte.

parentAccountNumber	Numéro de compte	businessUnitId	ID du poste
2003565430	2003564830	7	0100
2005284042	2005284042	6	0090
2000272719	2000272719	1	0100

5. Oracle_SQL_JSON_Aggregation_Join

Exemple de requête

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
```

```
       FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
  COLUMNS (
          parent_account_number NUMBER PATH
           '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Pour convertir les données au niveau des lignes au format JSON, Oracle dispose de fonctions intégrées telles que`JSON_OBJECT`, `JSON_ARRAY``JSON_OBJECTAGG`, et. `JSON_ARRAYAGG`

- `JSON_OBJECT`accepte deux paramètres : `KEY` et`VALUE`. Le `KEY` paramètre doit être codé en dur ou de nature statique. Le `VALUE` paramètre est dérivé de la sortie de la table.
- `JSON_ARRAYAGG`accepte `JSON_OBJECT` en tant que paramètre. Cela permet de regrouper l'ensemble d'`JSON_OBJECT`éléments sous forme de liste. Par exemple, si vous avez un `JSON_OBJECT` élément comportant plusieurs enregistrements (plusieurs `KEY` et `VALUE` paires dans le jeu de données), il `JSON_ARRAYAGG` ajoute l'ensemble de données et crée une liste. Selon le

langage de structure de données, `LIST` il s'agit d'un groupe d'éléments. Dans ce contexte, `LIST` il y a un groupe d'`JSON_OBJECT`éléments.

L'exemple suivant montre un `JSON_OBJECT` élément.

```
{
   "taxProfessionalCount": 0,
   "attorneyCount": 0,
   "nonAttorneyCount": 1,
   "clerkCount": 0
}
```

L'exemple suivant montre deux `JSON_OBJECT` éléments, `LIST` indiqués par des accolades (`[ ]`).

```
[
    {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
,
    {
        "taxProfessionalCount": 2,
        "attorneyCount": 1,
        "nonAttorneyCount": 3,
        "clerkCount":4
      }
]
```

Exemple de requête SQL

```
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
```

```
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               )
                        )
                                        )
             )
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE   0 END
            )      tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN        1    ELSE
  0 END
            )      attorney_count,

            SUM(CASE    WHEN tab_data.position_id = '0090' THEN        1    ELSE
  0 END
            )      non_attorney_count,

            SUM(CASE    WHEN tab_data.position_id = '0050' THEN        1    ELSE
  0 END
            )      clerk_count

        FROM
            aws_test_table scco,  JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
```

```
          "businessUnitId": 6
        }]
      }', '$.accounts[*]' ERROR ON ERROR
      COLUMNS (
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data ON ( static_data.parent_account_number =
 tab_data.parent_account_number
                         AND static_data.account_number = tab_data.account_number

                         AND static_data.business_unit_id =
 tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
```

Exemple de résultat de la requête SQL précédente

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
```

```
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

6. Postgres_SQL_JSON_Aggregation_Join

Les JSON_BUILD_OBJECT fonctions intégrées de PostgreSQL convertissent les données au niveau JSON_AGG des lignes au format JSON. JSON_BUILD_OBJECTPostgreSQL JSON_AGG et sont équivalents à Oracle et. JSON_OBJECT JSON_ARRAYAGG

Exemple de requête

```
select
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            )
        )
    )
)
from (
with tab as (select * from (
select (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER as
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER as accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER as businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar as positionId
from aws_test_pg_table) a ) ,
tab1 as ( select
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
```

```
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer
 businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
from (
select '{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }'::json as jc) b)
select
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
from tab1,tab
where tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
and tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
and tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
```

Exemple de résultat de la requête précédente

Les résultats d'Oracle et de PostgreSQL sont exactement les mêmes.

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
```

```
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

7. Procedure_Oracle_with_json_query

Ce code convertit la procédure Oracle en une fonction PostgreSQL dotée de requêtes SQL JSON. Il montre comment la requête transpose le JSON en lignes et inversement.

```
CREATE OR REPLACE PROCEDURE p_json_test(p_in_accounts_json IN varchar2,
 p_out_accunts_json  OUT varchar2)
IS
BEGIN
/*
p_in_accounts_json paramter should have following format:
       {
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
```

```
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }
*/
SELECT
    JSON_OBJECT(
        'accountCounts' VALUE JSON_ARRAYAGG(
            JSON_OBJECT(
                'businessUnitId' VALUE business_unit_id,
                        'parentAccountNumber' VALUE parent_account_number,
                        'accountNumber' VALUE account_number,
                        'totalOnlineContactsCount' VALUE online_contacts_count,
                        'countByPosition' VALUE
                    JSON_OBJECT(
                        'taxProfessionalCount' VALUE tax_count,
                        'attorneyCount' VALUE attorney_count,
                        'nonAttorneyCount' VALUE non_attorney_count,
                        'clerkCount' VALUE clerk_count
                               ) ) ) )
into p_out_accunts_json
FROM
    (SELECT
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number,
            SUM(1) online_contacts_count,
            SUM(CASE WHEN tab_data.position_id = '0095' THEN  1 ELSE 0 END) tax_count,
            SUM(CASE    WHEN tab_data.position_id = '0100' THEN 1 ELSE 0 END)
 attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0090' THEN 1 ELSE 0 END)
 non_attorney_count,
            SUM(CASE    WHEN tab_data.position_id = '0050' THEN 1 ELSE 0 END)
 clerk_count
        FROM aws_test_table scco,JSON_TABLE ( json_doc, '$' ERROR ON ERROR
            COLUMNS (
            parent_account_number NUMBER PATH '$.data.account.parentAccountNumber',
            account_number NUMBER PATH '$.data.account.accountNumber',
            business_unit_id NUMBER PATH '$.data.account.businessUnitId',
            position_id VARCHAR2 ( 4 ) PATH '$.data.positionId'    )
            ) AS tab_data
            INNER JOIN JSON_TABLE ( p_in_accounts_json, '$.accounts[*]' ERROR ON ERROR

      COLUMNS (
```

```
      parent_account_number PATH '$.parentAccountNumber',
      account_number PATH '$.accountNumber',
      business_unit_id PATH '$.businessUnitId')
      ) static_data
      ON ( static_data.parent_account_number = tab_data.parent_account_number
           AND static_data.account_number = tab_data.account_number
           AND static_data.business_unit_id = tab_data.business_unit_id )
        GROUP BY
            tab_data.business_unit_id,
            tab_data.parent_account_number,
            tab_data.account_number
    );
EXCEPTION
WHEN OTHERS THEN
   raise_application_error(-20001,'Error while running the JSON query');
END;
/
```

Exécution de la procédure

Le bloc de code suivant explique comment exécuter la procédure Oracle créée précédemment avec un exemple d'entrée JSON dans la procédure. Il vous donne également le résultat ou le résultat de cette procédure.

```
set serveroutput on;
declare
v_out varchar2(30000);
v_in varchar2(30000):= '{
        "accounts": [{
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }, {
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }]
      }';
begin
  p_json_test(v_in,v_out);
  dbms_output.put_line(v_out);
end;
/
```

Sortie de procédure

```
{
  "accountCounts": [
    {
      "businessUnitId": 6,
      "parentAccountNumber": 32001,
      "accountNumber": 42001,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
      "businessUnitId": 7,
      "parentAccountNumber": 32000,
      "accountNumber": 42000,
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

8. Fonction_Postgres_avec_requête JSON

Exemple de fonction

```
CREATE OR REPLACE  FUNCTION f_pg_json_test(p_in_accounts_json  text)
RETURNS text
LANGUAGE plpgsql
AS
$$
DECLARE
 v_out_accunts_json   text;
BEGIN
```

```
SELECT
JSON_BUILD_OBJECT ('accountCounts',
    JSON_AGG(
        JSON_BUILD_OBJECT ('businessUnitId',businessUnitId
        ,'parentAccountNumber',parentAccountNumber
        ,'accountNumber',accountNumber
        ,'totalOnlineContactsCount',online_contacts_count,
        'countByPosition',
            JSON_BUILD_OBJECT (
            'taxProfessionalCount',tax_professional_count
            ,'attorneyCount',attorney_count
            ,'nonAttorneyCount',non_attorney_count
            ,'clerkCount',clerk_count
            ))))
INTO v_out_accunts_json
FROM (
WITH tab AS (SELECT * FROM (
SELECT (json_doc::json->'data'->'account'->>'parentAccountNumber')::INTEGER AS
 parentAccountNumber,
(json_doc::json->'data'->'account'->>'accountNumber')::INTEGER AS accountNumber,
(json_doc::json->'data'->'account'->>'businessUnitId')::INTEGER AS businessUnitId,
(json_doc::json->'data'->>'positionId')::varchar AS positionId
FROM aws_test_pg_table) a ) ,
tab1 AS ( SELECT
(json_array_elements(b.jc -> 'accounts') ->> 'accountNumber')::integer accountNumber,
(json_array_elements(b.jc -> 'accounts') ->> 'businessUnitId')::integer businessUnitId,
(json_array_elements(b.jc -> 'accounts') ->> 'parentAccountNumber')::integer
 parentAccountNumber
FROM (
SELECT p_in_accounts_json::json AS jc) b)
SELECT
tab.businessUnitId::text,
tab.parentAccountNumber::text,
tab.accountNumber::text,
SUM(1) online_contacts_count,
SUM(CASE WHEN tab.positionId::text = '0095' THEN 1 ELSE 0  END)
  tax_professional_count,
SUM(CASE WHEN tab.positionId::text = '0100' THEN 1 ELSE 0  END)      attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0090' THEN      1  ELSE      0 END)
  non_attorney_count,
SUM(CASE  WHEN tab.positionId::text = '0050' THEN      1  ELSE      0 END)
  clerk_count
FROM tab1,tab
WHERE tab.parentAccountNumber::INTEGER=tab1.parentAccountNumber::INTEGER
```

```
AND tab.accountNumber::INTEGER=tab1.accountNumber::INTEGER
AND tab.businessUnitId::INTEGER=tab1.businessUnitId::INTEGER
GROUP BY      tab.businessUnitId::text,
            tab.parentAccountNumber::text,
            tab.accountNumber::text) a;
RETURN v_out_accunts_json;
END;
$$;
```

Exécution de la fonction

```
select    f_pg_json_test('{
        "accounts": [{
          "accountNumber": 42001,
          "parentAccountNumber": 32001,
          "businessUnitId": 6
        }, {
          "accountNumber": 42000,
          "parentAccountNumber": 32000,
          "businessUnitId": 7
        }]
      }')   ;
```

Sortie de fonction

La sortie suivante est similaire à la sortie de la procédure Oracle. La différence est que cette sortie est au format texte.

```
{
  "accountCounts": [
    {
      "businessUnitId": "6",
      "parentAccountNumber": "32001",
      "accountNumber": "42001",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 0,
        "nonAttorneyCount": 1,
        "clerkCount": 0
      }
    },
    {
```

```
      "businessUnitId": "7",
      "parentAccountNumber": "32000",
      "accountNumber": "42000",
      "totalOnlineContactsCount": 1,
      "countByPosition": {
        "taxProfessionalCount": 0,
        "attorneyCount": 1,
        "nonAttorneyCount": 0,
        "clerkCount": 0
      }
    }
  ]
}
```

Copiez les tables Amazon DynamoDB entre les comptes à l'aide de AWS Backup

Créée par Ramkumar Ramanujam (AWS)

Récapitulatif

Lorsque vous travaillez avec Amazon DynamoDB AWS sur, un cas d'utilisation courant consiste à copier ou à synchroniser des tables DynamoDB dans des environnements de développement, de test ou de préparation avec les données des tables présentes dans l'environnement de production. En règle générale, chaque environnement utilise un élément différent Compte AWS.

AWS Backup prend en charge la sauvegarde et la restauration des données entre régions et entre comptes pour DynamoDB, Amazon Simple Storage Service (Amazon S3), etc. Services AWS Ce modèle décrit les étapes d'utilisation de la sauvegarde et de la restauration AWS Backup entre comptes pour copier des tables DynamoDB entre les comptes. Comptes AWS

Conditions préalables et limitations

Prérequis

- Deux actifs Comptes AWS appartenant à la même organisation dans AWS Organizations
- Autorisations pour créer des tables DynamoDB dans les deux comptes
- AWS Identity and Access Management Autorisations (IAM) pour créer et utiliser AWS Backup des coffres-forts

Limites

- La source et la cible Comptes AWS doivent faire partie de la même organisation dans AWS Organizations.

Architecture

Pile technologique cible

- AWS Backup
- Amazon DynamoDB

Architecture cible

1. Créez la sauvegarde de la table DynamoDB dans AWS Backup le coffre de sauvegarde du compte source.
2. Copiez la sauvegarde dans le coffre de sauvegarde du compte cible.
3. Restaurez la table DynamoDB dans le compte cible en utilisant la sauvegarde du coffre de sauvegarde du compte cible.

Automatisation et mise à l'échelle

Vous pouvez l'utiliser AWS Backup pour planifier des sauvegardes afin qu'elles s'exécutent à des intervalles spécifiques.

Outils

- AWS Backupest un service entièrement géré destiné à centraliser et à automatiser la protection des données sur site Services AWS, dans le cloud et sur site. Ce service vous permet de configurer des politiques de sauvegarde et de surveiller l'activité de vos AWS ressources en un seul endroit. Il vous permet d'automatiser et de consolider les tâches de sauvegarde qui étaient auparavant effectuées service par service, et élimine le besoin de créer des scripts personnalisés et des processus manuels.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles avec une évolutivité sans faille.

Épopées

Activer les AWS Backup fonctionnalités dans les comptes source et cible

Tâche	Description	Compétences requises
Activez les fonctionnalités avancées pour DynamoDB et la sauvegarde entre comptes.	Dans la source et dans la cible Comptes AWS, procédez comme suit :	AWS DevOps, ingénieur en migration

Tâche	Description	Compétences requises
	1. Sur le AWS Management Console, ouvrez la AWS Backup console. 2. Sélectionnez Paramètres. 3. Sous Fonctionnalités avancées pour les sauvegardes Amazon DynamoDB, vérifiez que les fonctionnalités avancées sont activées ou choisissez Activer. 4. Sous Gestion entre comptes, pour la sauvegarde entre comptes, sélectionnez Activer.	

Créez des coffres-forts de sauvegarde dans les comptes source et cible

Tâche	Description	Compétences requises
Créez des coffres-forts de sauvegarde.	Dans la source et dans la cible Comptes AWS, procédez comme suit : 1. Sur la AWS Backup console, choisissez Backup vaults. 2. Choisissez Créer un coffre-fort de sauvegarde. 3. Copiez l'Amazon Resource Name (ARN) du coffre de sauvegarde et enregistrez-le.	AWS DevOps, ingénieur en migration

Tâche	Description	Compétences requises
	Les coffres-forts ARNs de sauvegarde source et cible seront nécessaires lorsque vous copiez la sauvegarde de la table DynamoDB entre les comptes source et cible.	

Effectuez des sauvegardes et des restaurations à l'aide de coffres-forts de sauvegarde

Tâche	Description	Compétences requises
Dans le compte source, créez une sauvegarde de table DynamoDB.	Pour créer une sauvegarde de la table DynamoDB dans le compte source, procédez comme suit : 1. Sur la page AWS Backup Tableau de bord, choisissez Créer une sauvegarde à la demande. 2. Dans la section Paramètre s, pour Type de ressource , sélectionnez DynamoDB, puis sélectionnez le nom de la table. 3. Dans la liste déroulante Backup vault, sélectionnez le coffre de sauvegarde que vous avez créé dans le compte source. 4. Sélectionnez la période de conservation que vous souhaitez.	AWS DevOps, DBA, ingénieur en migration

Tâche	Description	Compétences requises
	5. Choisissez Create on-demand backup (Créer une sauvegarde à la demande). Une nouvelle tâche de sauvegarde est créée. Pour surveiller l'état de la tâche de sauvegarde, sur la page AWS Backup Tâches, choisissez l'onglet Tâches de sauvegarde. Toutes les tâches de sauvegarde actives, en cours et terminées sont répertoriées dans cet onglet.	

Tâche	Description	Compétences requises
Copiez la sauvegarde du compte source vers le compte cible.	Une fois la tâche de sauvegarde terminée, copiez la sauvegarde de la table DynamoDB du coffre de sauvegarde du compte source vers le coffre de sauvegarde du compte cible. Pour copier le coffre de sauvegarde, dans le compte source, procédez comme suit : 1. Sur la AWS Backup console, choisissez Backup vaults. 2. Sous Sauvegardes, choisissez la sauvegarde de table DynamoDB. 3. Choisissez Actions, puis Copier. 4. Entrez le nom Région AWS du compte cible. 5. Pour l'ARN du coffre externe, entrez l'ARN du coffre-fort de sauvegarde que vous avez créé dans le compte cible. 6. Pour copier des sauvegard es du compte source vers le compte cible, dans le coffre de sauvegarde du compte cible, activez l'accès depuis un autre compte.	AWS DevOps, ingénieur en migration, DBA

Tâche	Description	Compétences requises
Restaurez la sauvegarde dans le compte cible.	Dans la cible Compte AWS, procédez comme suit : 1. Sur la AWS Backup console, choisissez Backup vaults. 2. Sous Sauvegardes, sélectionnez la sauvegarde que vous avez copiée depuis le compte source. 3. Choisissez Actions, Restaurer. 4. Entrez le nom de la table DynamoDB cible que vous souhaitez restaurer.	AWS DevOps, DBA, ingénieur en migration

Ressources connexes

- Utilisation AWS Backup avec DynamoDB
- Création de copies de sauvegarde sur Comptes AWS
- AWS Backup tarification

Copiez les tables Amazon DynamoDB entre les comptes à l'aide d'une implémentation personnalisée

Créée par Ramkumar Ramanujam (AWS)

Récapitulatif

Lorsque vous travaillez avec Amazon DynamoDB sur Amazon Web Services (AWS), un cas d'utilisation courant consiste à copier ou à synchroniser des tables DynamoDB dans des environnements de développement, de test ou de préparation avec les données des tables présentes dans l'environnement de production. En règle générale, chaque environnement utilise un compte AWS différent.

DynamoDB prend désormais en charge la sauvegarde entre comptes à l'aide d'AWS Backup. Pour plus d'informations sur les coûts de stockage associés à l'utilisation d'AWS Backup, consultez la tarification d'AWS Backup. Lorsque vous utilisez AWS Backup pour effectuer des copies entre comptes, les comptes source et cible doivent appartenir à une organisation AWS Organizations. Il existe d'autres solutions de sauvegarde et de restauration entre comptes à l'aide de services AWS tels qu'AWS Glue. L'utilisation de ces solutions augmente toutefois l'encombrement des applications, car il y a davantage de services AWS à déployer et à gérer.

Vous pouvez également utiliser Amazon DynamoDB Streams pour capturer les modifications de table dans le compte source. Vous pouvez ensuite lancer une fonction AWS Lambda et apporter les modifications correspondantes dans la table cible du compte cible. Mais cette solution s'applique aux cas d'utilisation dans lesquels les tables source et cible doivent toujours être synchronisées. Cela peut ne pas s'appliquer aux environnements de développement, de test et de préparation dans lesquels les données sont fréquemment mises à jour.

Ce modèle fournit les étapes permettant de mettre en œuvre une solution personnalisée pour copier une table Amazon DynamoDB d'un compte à un autre. Ce modèle peut être implémenté à l'aide de langages de programmation courants tels que C#, Java et Python. Nous vous recommandons d'utiliser un langage pris en charge par un SDK AWS.

Conditions préalables et limitations

Prérequis

- Deux comptes AWS actifs
- Tables DynamoDB dans les deux comptes

- Connaissance des rôles et des politiques d'AWS Identity and Access Management (IAM)
- Connaissance de l'accès aux tables Amazon DynamoDB à l'aide de n'importe quel langage de programmation courant, tel que C#, Java ou Python

Limites

Ce modèle s'applique aux tables DynamoDB dont la taille est inférieure ou égale à 2 Go environ. Grâce à une logique supplémentaire permettant de gérer les interruptions de connexion ou de session, les ralentissements, les échecs et les nouvelles tentatives, il peut être utilisé pour des tables plus volumineuses.

L'opération d'analyse DynamoDB, qui lit les éléments de la table source, ne peut récupérer que 1 Mo de données en un seul appel. Pour les tables plus grandes, supérieures à 2 Go, cette limitation peut augmenter le temps total nécessaire pour effectuer une copie complète de la table.

Architecture

Le schéma suivant montre l'implémentation personnalisée entre les comptes AWS source et cible. Les politiques IAM et les jetons de sécurité sont utilisés avec l'implémentation personnalisée. Les données sont lues depuis Amazon DynamoDB dans le compte source et écrites dans DynamoDB dans le compte cible.

Automatisation et évolutivité

Ce modèle s'applique aux tables DynamoDB dont la taille est plus petite, environ 2 Go.

Pour appliquer ce modèle à des tables de plus grande taille, vous devez résoudre les problèmes suivants :

- Pendant l'opération de copie de table, deux sessions actives sont maintenues à l'aide de jetons de sécurité différents. Si l'opération de copie de table prend plus de temps que les délais d'expiration des jetons, vous devez mettre en place une logique pour actualiser les jetons de sécurité.
- Si un nombre suffisant d'unités de capacité de lecture (RCUs) et d'unités de capacité d'écriture (WCUs) ne sont pas provisionnées, les lectures ou les écritures sur la table source ou cible peuvent être limitées. Assurez-vous de détecter et de gérer ces exceptions.
- Gérez tout autre échec ou exception et mettez en place un mécanisme de nouvelle tentative pour réessayer ou continuer à partir de l'endroit où l'opération de copie a échoué.

Outils

Outils

- Amazon DynamoDB — Amazon DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité sans faille.
- Les outils supplémentaires requis varient en fonction du langage de programmation que vous choisissez pour l'implémentation. Par exemple, si vous utilisez C#, vous aurez besoin de Microsoft Visual Studio et des NuGet packages suivants :
  - `AWSSDK`
  - `AWSSDK.DynamoDBv2`

Code

L'extrait de code Python suivant supprime et recrée une table DynamoDB à l'aide de la bibliothèque Boto3.

N'utilisez pas le `AWS_ACCESS_KEY_ID` et `AWS_SECRET_ACCESS_KEY` d'un utilisateur IAM car il s'agit d'informations d'identification à long terme, qui doivent être évitées pour l'accès programmatique aux services AWS. Pour plus d'informations sur les informations d'identification temporaires, consultez la section Bonnes pratiques.

Les `AWS_ACCESS_KEY_ID` et `TEMPORARY_SESSION_TOKEN` utilisés dans l'extrait de code suivant sont des informations d'identification temporaires extraites d'AWS Security Token Service (AWS STS). `AWS_SECRET_ACCESS_KEY`

```
import boto3
import sys
import json

#args = input-parameters = GLOBAL_SEC_INDEXES_JSON_COLLECTION,
 ATTRIBUTES_JSON_COLLECTION, TARGET_DYNAMODB_NAME, TARGET_REGION, ...

#Input param: GLOBAL_SEC_INDEXES_JSON_COLLECTION
#[{"IndexName":"Test-index","KeySchema":[{"AttributeName":"AppId","KeyType":"HASH"},
{"AttributeName":"AppType","KeyType":"RANGE"}],"Projection":
{"ProjectionType":"INCLUDE","NonKeyAttributes":["PK","SK","OwnerName","AppVersion"]}}]

#Input param: ATTRIBUTES_JSON_COLLECTION
```

```
#[{"AttributeName":"PK","AttributeType":"S"},
{"AttributeName":"SK","AttributeType":"S"},
{"AttributeName":"AppId","AttributeType":"S"},
{"AttributeName":"AppType","AttributeType":"N"}]

region = args['TARGET_REGION']
target_ddb_name = args['TARGET_DYNAMODB_NAME']

global_secondary_indexes = json.loads(args['GLOBAL_SEC_INDEXES_JSON_COLLECTION'])
attribute_definitions = json.loads(args['ATTRIBUTES_JSON_COLLECTION'])

# Drop and create target DynamoDB table
dynamodb_client = boto3.Session(
        aws_access_key_id=args['AWS_ACCESS_KEY_ID'],
        aws_secret_access_key=args['AWS_SECRET_ACCESS_KEY'],
        aws_session_token=args['TEMPORARY_SESSION_TOKEN'],
    ).client('dynamodb')

# Delete table
print('Deleting table: ' + target_ddb_name + ' ...')

try:
    dynamodb_client.delete_table(TableName=target_ddb_name)

    #Wait for table deletion to complete
    waiter = dynamodb_client.get_waiter('table_not_exists')
    waiter.wait(TableName=target_ddb_name)
    print('Table deleted.')
except dynamodb_client.exceptions.ResourceNotFoundException:
    print('Table already deleted / does not exist.')
    pass

print('Creating table: ' + target_ddb_name + ' ...')

table = dynamodb_client.create_table(
    TableName=target_ddb_name,
    KeySchema=[
        {
            'AttributeName': 'PK',
            'KeyType': 'HASH'  # Partition key
        },
        {
            'AttributeName': 'SK',
            'KeyType': 'RANGE'  # Sort key
```

```
        }
    ],
    AttributeDefinitions=attribute_definitions,
    GlobalSecondaryIndexes=global_secondary_indexes,
    BillingMode='PAY_PER_REQUEST'
)

waiter = dynamodb_client.get_waiter('table_exists')
waiter.wait(TableName=target_ddb_name)

print('Table created.')
```

Bonnes pratiques

Informations d’identification temporaires

Pour des raisons de sécurité, lorsque vous accédez aux services AWS par programmation, évitez d'utiliser le `AWS_ACCESS_KEY_ID` et d'un utilisateur IAM, car il s'agit `AWS_SECRET_ACCESS_KEY` d'informations d'identification à long terme. Essayez toujours d'utiliser des informations d'identification temporaires pour accéder aux services AWS par programmation.

Par exemple, un développeur code en dur le code `AWS_ACCESS_KEY_ID` et `AWS_SECRET_ACCESS_KEY` d'un utilisateur IAM dans l'application pendant le développement, mais ne supprime pas les valeurs codées en dur avant de transférer les modifications au référentiel de code. Ces informations d'identification exposées peuvent être utilisées par des utilisateurs involontaires ou malveillants, ce qui peut avoir de graves conséquences (en particulier si les informations d'identification exposées ont des privilèges d'administrateur). Ces informations d'identification exposées doivent être désactivées ou supprimées immédiatement à l'aide de la console IAM ou de l'AWS Command Line Interface (AWS CLI).

Pour obtenir des informations d'identification temporaires pour un accès programmatique aux services AWS, utilisez AWS STS. Les informations d'identification temporaires ne sont valides que pour la durée spécifiée (de 15 minutes à 36 heures). La durée maximale autorisée des informations d'identification temporaires varie en fonction de facteurs tels que les paramètres des rôles et le chaînage des rôles. Pour plus d'informations sur AWS STS, consultez la documentation.

Épopées

Configuration des tables DynamoDB

Tâche	Description	Compétences requises
Créez des tables DynamoDB.	Créez des tables DynamoDB, avec des index, dans les comptes AWS source et cible. Définissez le provisionnement des capacités en mode à la demande, ce qui permet à DynamoDB de dimension ner les capacités de lecture/é criture de manière dynamique en fonction de la charge de travail. Vous pouvez également utiliser une capacité provision née de 4 000 RCUs et 4 000 WCUs.	Développeur d'applications, DBA, ingénieur en migration
Renseignez le tableau source.	Remplissez la table DynamoDB du compte source avec des données de test. Le fait de disposer d'au moins 50 Mo de données de test vous permet de connaître le pic et la RCUs consommation moyenne pendant la copie de la table. Vous pouvez ensuite modifier le provisionnement de capacité selon vos besoins.	Développeur d'applications, DBA, ingénieur en migration

Configurer les informations d'identification pour accéder aux tables DynamoDB

Tâche	Description	Compétences requises
Créez des rôles IAM pour accéder aux tables DynamoDB source et cible.	Créez un rôle IAM dans le compte source avec les autorisations nécessaires pour accéder (lire) à la table DynamoDB du compte source. Ajoutez le compte source en tant qu'entité de confiance pour ce rôle. Créez un rôle IAM dans le compte cible avec des autorisations d'accès (création, lecture, mise à jour, suppression) à la table DynamoDB du compte cible. Ajoutez le compte cible en tant qu'entité de confiance pour ce rôle.	Développeur d'applications, AWS DevOps

Copier les données d'une table d'un compte à un autre

Tâche	Description	Compétences requises
Obtenez des informations d'identification temporaires pour les rôles IAM.	Obtenez des informations d'identification temporaires pour le rôle IAM créé dans le compte source. Obtenez des informations d'identification temporaires	Développeur d'applications, ingénieur en migration

Tâche	Description	Compétences requises
	pour le rôle IAM créé dans le compte cible. L'un des moyens d'obtenir les informations d'identification temporaires pour le rôle IAM consiste à utiliser AWS STS à partir de l'AWS CLI. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/<role-name> --role-session-name <session-name> --profile <profile-name>` Utilisez le profil AWS approprié (correspondant au compte source ou cible). Pour plus d'informations sur les différentes manières d'obtenir des informations d'identification temporaires, consultez les rubriques suivantes : • Référence de l'API AWS Security Token Service • Obtenir les informations d'identification du rôle IAM pour l'accès à la CLI	

Tâche	Description	Compétences requises
Initialisez les clients DynamoDB pour accéder à DynamoDB source et cible.	Initialisez les clients DynamoDB, fournis par le SDK AWS, pour les tables DynamoDB source et cible. • Pour le client DynamoDB source, utilisez les informations d'identification temporaires extraites du compte source. • Pour le client DynamoDB cible, utilisez les informations d'identification temporaires extraites du compte cible. Pour plus d'informations sur l'envoi de demandes à l'aide d'informations d'identification temporaires IAM, consultez la documentation AWS.	Développeur d’applications

Tâche	Description	Compétences requises
Supprimez et recréez la table cible.	Supprimez et recréez la table DynamoDB cible (ainsi que les index) dans le compte cible, à l'aide du client DynamoDB du compte cible. La suppression de tous les enregistrements d'une table DynamoDB est une opération coûteuse car elle consomme des ressources provision nées. WCUs La suppressi on et la recréation du tableau permettent d'éviter ces coûts supplémentaires. Vous pouvez ajouter des index à une table après l'avoir créée, mais cela prend 2 à 5 minutes de plus. La création d'index lors de la création d'une table, en transmettant la collectio n d'index à l'`createTab le` appel, est plus efficace.	Développeur d’applications

Tâche	Description	Compétences requises
Effectuez la copie du tableau.	Répétez les étapes suivantes jusqu'à ce que toutes les données soient copiées : • Effectuez une analyse de la table dans le compte source à l'aide du client DynamoDB source. Chaque analyse DynamoDB extrait seulement 1 Mo de données de la table. Vous devez donc répéter cette opération jusqu'à ce que tous les éléments ou enregistr ements soient lus. • Pour chaque ensemble d'éléments numérisés , inscrivez les éléments dans le tableau du compte cible, avec le client DynamoDB cible, à l'aide de l'`BatchWriteItem` appel dans le SDK AWS pour DynamoDB. Cela réduit le nombre de `PutItem` requêtes adressées à DynamoDB. • `BatchWriteItem` est limité à 25 écritures ou entrées, soit jusqu'à 16 Mo. Vous devez ajouter une logique permettant d'accumuler les articles numérisés par 25 avant	Développeur d’applications

Tâche	Description	Compétences requises
	d'appelerBatchWrit eItem .BatchWrit eItem renvoie une liste d'éléments qui n'ont pas pu être copiés correctement. À l'aide de cette liste, ajoutez une logique de nouvelle tentative pour effectuer un autre BatchWriteItem appel avec uniquement les éléments qui ont échoué. Pour plus d'informations, consultez l'implémentation de référence en C# (pour supprimer, créer et remplir des tables) dans la section Pièces jointes. Un exemple de fichier de configuration de table JavaScript Object Notation (JSON) est également joint.	

Ressources connexes

- Documentation Amazon DynamoDB
- Création d'un utilisateur IAM dans votre compte AWS
- AWS SDKs
- Utilisation d'informations d'identification temporaires avec les ressources AWS

Informations supplémentaires

Ce modèle a été implémenté à l'aide de C# pour copier une table DynamoDB contenant 200 000 éléments (taille moyenne des éléments de 5 Ko et taille de table de 250 Mo). La table DynamoDB cible a été configurée avec une capacité provisionnée de 4 000 et 4 000. RCUs WCUs

L'opération complète de copie du tableau (du compte source vers le compte cible), y compris la suppression et la recréation du tableau, a pris 5 minutes. Capacité totale d'unités consommées : 30 000 RCUs et environ 400 000 WCUs.

Pour plus d'informations sur les modes de capacité DynamoDB, consultez la section Mode de capacité de lecture/écriture dans la documentation AWS.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez des rapports détaillés sur les coûts et l'utilisation pour Amazon RDS et Amazon Aurora

Créée par Lakshmanan Lakshmanan (AWS) et Sudarshan Narasimhan

Récapitulatif

Ce modèle montre comment suivre les coûts d'utilisation des clusters Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora en configurant des balises de répartition des coûts définies par l'utilisateur. Vous pouvez utiliser ces balises pour créer des rapports détaillés sur les coûts et l'utilisation dans AWS Cost Explorer pour les clusters à plusieurs dimensions. Par exemple, vous pouvez suivre les coûts d'utilisation au niveau de l'équipe, du projet ou du centre de coûts, puis analyser les données dans Amazon Athena.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une ou plusieurs instances Amazon RDS ou Amazon Aurora

Limites

Pour connaître les restrictions relatives au balisage, consultez le guide de l'utilisateur d'AWS Billing.

Architecture

Pile technologique cible

- Amazon RDS ou Amazon Aurora
- AWS Rapport sur les coûts et l'utilisation
- AWS Cost Explorer
- Amazon Athena

Flux de travail et architecture

Le flux de travail de balisage et d'analyse comprend les étapes suivantes :

1. Un ingénieur de données, un administrateur de base de données ou un administrateur AWS crée des balises de répartition des coûts définies par l'utilisateur pour les clusters Amazon RDS ou Aurora.
2. Un administrateur AWS active les balises.
3. Les balises transmettent les métadonnées à AWS Cost Explorer.
4. Un ingénieur de données, un administrateur de base de données ou un administrateur AWS crée un rapport mensuel de répartition des coûts.
5. Un ingénieur de données, un administrateur de base de données ou un administrateur AWS analyse le rapport mensuel de répartition des coûts à l'aide d'Amazon Athena.

Le schéma suivant montre comment appliquer des balises pour suivre les coûts d'utilisation des instances Amazon RDS ou Aurora.

Le schéma d'architecture suivant montre comment le rapport de répartition des coûts est intégré à Amazon Athena à des fins d'analyse.

Le rapport mensuel de répartition des coûts est stocké dans un compartiment Amazon S3 que vous spécifiez. Lorsque vous configurez Athena avec le CloudFormation modèle AWS, comme décrit dans la section Epics, le modèle fournit plusieurs ressources supplémentaires, notamment un robot d'exploration AWS Glue, une base de données AWS Glue, un événement Amazon Simple Notification System (Amazon SNS), des fonctions AWS Lambda et des rôles AWS Identity and Access Management (IAM) pour les fonctions Lambda. Lorsque de nouveaux fichiers de données de coûts arrivent dans le compartiment S3, les notifications d'événements sont utilisées pour transmettre ces fichiers à une fonction Lambda en vue de leur traitement. La fonction Lambda lance une tâche d'explorateur AWS Glue pour créer ou mettre à jour la table dans le catalogue de données AWS Glue. Cette table est ensuite utilisée pour interroger des données dans Athena.

Outils

- Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide du SQL standard.

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré conçu pour le cloud et compatible avec MySQL et PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- AWS CloudFormation est un service d'infrastructure sous forme de code (IaC) qui vous permet de modéliser, de provisionner et de gérer facilement des ressources AWS et tierces.
- AWS Cost Explorer vous permet de visualiser et d'analyser vos coûts et votre utilisation d'AWS.

Épopées

Création et activation de balises pour votre cluster Amazon RDS ou Aurora

Tâche	Description	Compétences requises
Créez des balises de répartition des coûts définies par l'utilisateur pour votre cluster Amazon RDS ou Aurora.	Pour ajouter des balises à un cluster Amazon RDS ou Aurora nouveau ou existant, suivez les instructions de la section Ajouter, répertorier et supprimer des balises dans le guide de l'utilisateur Amazon Aurora. **Note** Pour plus d'informations sur la configuration d'un cluster Amazon Aurora, consultez les instructions relatives à MySQL et PostgreSQL dans le guide de l'utilisateur Amazon Aurora.	Administrateur AWS, ingénieur de données, DBA

Tâche	Description	Compétences requises
Activez les balises de répartition des coûts définies par l'utilisateur.	Suivez les instructions de la section Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de l'utilisateur d'AWS Billing.	Administrateur AWS

Création de rapports sur les coûts et l'utilisation

Tâche	Description	Compétences requises
Créez et configurez des rapports de coûts et d'utilisation pour vos clusters.	1. Connectez-vous à l'AWS Management Console et ouvrez la console de facturation AWS. 2. Dans le volet de navigation de gauche, sélectionnez Cost & Usage Reports. 3. Choisissez Créer un rapport. 4. Entrez un nom de rapport, conservez les paramètres par défaut pour les autres options, puis choisissez Next. 5. Choisissez Configurer et fournissez les détails d'un compartiment S3 existant. Vous pouvez également choisir de créer un nouveau compartiment S3 à partir de cet écran. Choisissez Suivant.	Propriétaire de l'application, administrateur AWS, administrateur de base de données, AWS général, ingénieur de données

Tâche	Description	Compétences requises
	6. Vérifiez la politique par défaut qui sera appliquée à votre compartiment, cochez la case de confirmation, puis sélectionnez Enregistrer. 7. Pour le préfixe du chemin du rapport, spécifiez le préfixe que vous souhaitez ajouter au nom du rapport. 8. Pour la granularité temporelle, choisissez Horaire, Quotidien ou Mensuel, selon la fréquence à laquelle vous souhaitez que les données soient collectées pour le rapport. 9. Pour le contrôle des versions des rapports, choisissez si vous souhaitez que les nouvelles versions du rapport soient créées séparément ou remplacez le rapport existant par chaque version. 10. Pour Activer l'intégration des données de rapport pour, choisissez Amazon Athena. Vérifiez que le type de compression est défini sur Parquet. 11. Choisissez Suivant.	

Tâche	Description	Compétences requises
	12. Vérifiez les paramètres du rapport, puis choisissez Réviser et terminer. Les données seront disponibles dans 24 heures.	

Analyser les données des rapports sur les coûts et l'utilisation

Tâche	Description	Compétences requises
Analysez les données du rapport sur les coûts et l'utilisation.	1. Configurez et utilisez Athena pour analyser les données du rapport. Pour obtenir des instructions, consultez la section Interrogation des rapports de coûts et d'utilisation à l'aide d'Amazon Athena dans le guide de l'utilisateur d'AWS Cost and Usage Reports. Nous vous recommandons d'utiliser le CloudFormation modèle AWS fourni par Athena. 2. Exécutez les requêtes Athena. Par exemple, vous pouvez utiliser la requête SQL suivante pour vérifier l'état de l'actualisation des données.	Propriétaire de l'application, administrateur AWS, administrateur de base de données, AWS général, ingénieur de données

Tâche	Description	Compétences requises
	`select status from cost_and_usage_data_status` Pour plus d'informations, consultez la section Exécution de requêtes Amazon Athena dans le guide de l'utilisateur d'AWS Cost and Usage Reports. **Note** Lorsque vous exécutez votre requête SQL, assurez-vous que la bonne base de données est sélectionnée dans la liste déroulante.	

Ressources connexes

Références

- Configuration d'Athena à l'aide de CloudFormation modèles AWS (recommandé)
- Configuration manuelle d'Athena
- Exécution de requêtes Amazon Athena
- Chargement des données du rapport vers d'autres ressources

Tutoriels et vidéos

- Analyser les rapports de coûts et d'utilisation à l'aide d'Amazon Athena (vidéo) YouTube

Déployez des instances de cluster de basculement SQL Server sur Amazon EC2 et Amazon à l'aide FSx de Terraform

Créée par Mark Hudson (AWS) et Matt Burgess (AWS)

Récapitulatif

Ce modèle utilise Terraform pour déployer des instances de cluster de basculement SQL Server (FCIs) sur des nœuds Windows Server Failover Cluster (WSFC) sur Amazon Elastic Compute Cloud (Amazon). EC2 En outre, le modèle utilise le stockage FSx partagé d'Amazon pour les données et les fichiers journaux.

Lorsque les bases de données SQL Server sont migrées vers AWS, le premier choix est Amazon RDS for SQL Server. Cependant, Amazon RDS for SQL Server n'est parfois pas adapté et SQL Server doit être déployé sur EC2 Amazon dans une architecture à haute disponibilité. Dans cette solution, SQL Server FCIs est installé sur les nœuds WSFC.

Le module Terraform inclus dans ce modèle fournit jusqu'à deux instances Amazon EC2 SQL Server. Un système de fichiers Amazon FSx pour Windows File Server agit en tant que témoin du quorum et stocke les données partagées et les fichiers journaux. Quel que soit le nombre d'instances configurées, les nœuds d'instance SQL Server créeront et rejoindront toujours un cluster FCI afin de garantir la parité environnementale. (Généralement, une instance est configurée pour le développement et deux instances pour les environnements de production.) Pour les configurations qui utilisent deux nœuds à des fins de haute disponibilité, un Network Load Balancer interne est configuré. Le Network Load Balancer utilise une sonde de santé configurée sur le cluster FCI pour identifier le nœud principal.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Amazon Virtual Private Cloud (Amazon VPC) avec deux sous-réseaux dans des zones de disponibilité distinctes.
- Ensemble d'options DHCP Amazon VPC. Configurez le nom de domaine pour qu'il corresponde à votre nom de domaine Active Directory et le domaine et les serveurs de noms NetBIOS pour qu'ils pointent vers vos contrôleurs de domaine Active Directory. Pour plus d'informations, consultez la section Configuration du VPC dans Informations supplémentaires.

- AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD).
- Image de machine Amazon personnalisée (AMI). Pour plus de détails, consultez la section Configuration de l'AMI dans Informations supplémentaires.
- Compartiment Amazon Simple Storage Service (Amazon S3) contenant l'image ISO de SQL Server. Cette condition préalable n'est requise que si vous utilisez EC2 Image Builder avec le `component.yaml` fichier fourni pour créer l'AMI personnalisée.
- AWS Key Management Service (AWS KMS) clé de chiffrement.
- Par défaut, SQL Server est installé à l'aide d'une clé de produit de l'édition développeur. Les systèmes de production sont censés utiliser une clé de produit valide transmise au module par la variable correspondante.

Limites

- Cette solution nécessite AWS Managed Microsoft AD. Toutefois, si vous préférez, vous pouvez plutôt utiliser une implémentation Active Directory autogérée. Pour ce faire, modifiez le module Amazon FSx Terraform inclus pour supprimer l'`active_directory_id`attribut. Ajoutez ensuite les quatre attributs requis pour l'autogestion d'Active Directory, comme indiqué dans la documentation Terraform.
- SQL Server est configuré pour utiliser l'authentification en mode mixte. Si vous préférez, vous pouvez utiliser l'authentification Windows uniquement. Pour ce faire, dans le script de données utilisateur fourni, supprimez les `/SAPWD` paramètres `/SECURITYMODE` et fournis à la `setup.exe` commande. Vous pouvez supprimer le `sql_accounts.tf` fichier et le `instances.tf` modifier pour supprimer l'`sql_sa_password`entrée.
- Lorsque vous supprimez un cluster déployé, vous devez supprimer les objets informatiques virtuels correspondants et les objets informatiques individuels dans Active Directory. Pour supprimer les objets, utilisez les outils d'administration Active Directory.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

Cette solution a été testée avec les versions suivantes :

- Windows Server 2019
- SQL Server 2019
- Terraform v0.13.0

Architecture

Pile technologique source

- SQL Server

Pile technologique cible

- SQL Server FCI sur les nœuds WSFC à l'aide d'Amazon EC2
- Serveur FSx de fichiers Amazon pour Windows
- Compartiment Amazon S3
- AWS Secrets Manager
- AWS Managed Microsoft AD
- AWS KMS
- AWS Identity and Access Management (JE SUIS)

Architecture cible

Le schéma suivant montre l'architecture de cette solution.

Le diagramme décrit les éléments suivants :

- Rôle IAM fournissant aux EC2 instances l'accès à Secrets Manager AWS KMS et à Secrets Manager
- Deux nœuds SQL Server déployés sur des EC2 instances Amazon dans des sous-réseaux privés répartis sur deux zones de disponibilité
- Un Network Load Balancer pour faciliter les connexions à l'instance SQL Server active (non déployé lors de la configuration d'un cluster à nœud unique)
- Système de fichiers Amazon FSx pour Windows File Server déployé dans les deux sous-réseaux privés pour un stockage partagé par les nœuds SQL Server

- Secrets Manager pour le stockage des informations d'identification et de configuration d'Active Directory et de SQL Server
- Compartiment Amazon S3 pour stocker l'image d'installation de SQL Server
- AWS Managed Microsoft AD pour l'authentification Windows
- AWS KMS pour créer la clé de chiffrement

Automatisation et mise à l'échelle

Vous pouvez automatiser le déploiement de l'architecture cible en utilisant les modules Terraform présents dans le GitHub référentiel. Vous devez modifier le `terraform.tfvars` fichier pour inclure des valeurs de variables spécifiques à votre environnement. Le compartiment Amazon S3, AWS Managed Microsoft AD les composants, la clé de AWS KMS chiffrement et certains secrets sont des conditions préalables à ce déploiement et ne sont pas inclus dans le code Terraform.

Outils

Services AWS

- AWS Directory Service for Microsoft Active Directorypermet à vos charges de travail et à vos AWS ressources sensibles aux annuaires d'utiliser Microsoft Active Directory dans le. AWS Cloud Dans ce modèle, AWS Managed Microsoft AD il est utilisé pour l'authentification Windows Server et SQL Server et pour le DNS.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement. Dans ce modèle, les instances de cluster de basculement SQL Server sont installées sur les EC2 instances Amazon.
- EC2 Image Builder vous aide à automatiser la création, la gestion et le déploiement d'images de serveur personnalisées.
- Amazon FSx pour Windows File Server fournit un stockage partagé entièrement géré sur Windows Server. Dans ce modèle, FSx le serveur de fichiers Windows fournit un stockage partagé pour les données et les fichiers journaux de SQL Server ainsi que pour le témoin du quorum.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données. Dans ce modèle, il est utilisé pour chiffrer les

secrets de Secrets Manager, le stockage SQL Server sur les volumes Amazon Elastic Block Store (Amazon EBS) et le système de fichiers FSx pour Windows File Server.

- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Dans ce modèle, les informations d'identification Active Directory pour l'installation et l'exécution de SQL Server, les informations `sa` d'identification utilisateur et les informations de connexion à la base de données sont stockées dans Secrets Manager.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données. Ce modèle utilise un compartiment Amazon S3 pour stocker l'image d'installation de SQL Server.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Autres outils

- Microsoft SQL Server FCIs est installé sur les nœuds de cluster Windows Server. En outre, ils peuvent être installés sur plusieurs sous-réseaux. Dans ce modèle, les instances FCI de SQL Server sont installées sur les nœuds WSFC.
- Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud. Dans ce modèle, Terraform est utilisé pour créer les ressources et configurer les instances FCI de SQL Server.
- Le clustering Windows Server Failover fournit des fonctionnalités d'infrastructure qui prennent en charge la haute disponibilité des applications de serveur hébergées telles que SQL Server. Dans ce modèle, les nœuds FCI utilisent la fonctionnalité WSFC pour fournir une haute disponibilité locale grâce à la redondance au niveau de l'instance.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub cluster-amazon-elastic-compute- cloud-amazon-fsx-microsoft -sql-server. Les ressources suivantes sont disponibles dans le référentiel :

- Un `README.md` fichier qui fournit une vue d'ensemble de la solution et des informations supplémentaires sur l'installation et l'utilisation

- Un ensemble de base de fichiers de configuration Terraform et un module FSx spécifique à Amazon pour approvisionner les composants de ce modèle
- Un script de configuration d'instance exécuté en tant que script de données EC2 utilisateur Amazon
- Un fichier `component.yam` L que Image Builder peut utiliser pour créer une AMI personnalisée

Bonnes pratiques

Sécurité et correctifs

- Les installations et configurations préalables de l'AMI constituent la configuration minimale requise pour déployer des clusters SQL Server FCI. Des logiciels et des configurations supplémentaires peuvent être nécessaires pour se conformer aux normes et aux exigences de sécurité de votre entreprise.
- Après le déploiement, appliquez régulièrement des correctifs à Windows. Corrigez directement les instances en cours d'exécution ou créez une nouvelle AMI avec les derniers correctifs Windows et remplacez les instances (une par une) à l'aide de la nouvelle AMI. AWS publie AMIs chaque mois un nouveau Windows contenant les derniers correctifs, pilotes et agents de lancement du système d'exploitation. Nous vous recommandons de vérifier la dernière AMI lorsque vous lancez de nouvelles instances ou lorsque vous créez vos propres images personnalisées.
- Les EC2 instances Amazon sont configurées pour autoriser tout le trafic sortant. Lors du déploiement dans un environnement de production, les règles de sortie du groupe de sécurité doivent être mises en place pour limiter ce trafic aux destinations requises.
- Le système de fichiers FSx pour Windows File Server peut enregistrer automatiquement des journaux d'audit pour le partage de fichiers et l'accès aux fichiers et aux dossiers et les expédier à la destination souhaitée si cela est requis dans votre environnement.
- Faites régulièrement pivoter les secrets de Secrets Manager automatiquement. Pour la paire de clés d' EC2 instance Amazon, envisagez une solution de rotation automatique telle que décrite dans Comment utiliser AWS Secrets Manager pour stocker et faire pivoter des paires de clés SSH en toute sécurité. Pour les informations d'identification Active Directory et les secrets des `sa` informations d'identification SQL Server, configurez la rotation automatique conformément à vos politiques de gestion des mots de passe.

Gestion d'Active Directory

- Dans le cadre du cluster FCI, Windows génère un objet de nom d'ordinateur (CNO) dans Active Directory. Le CNO répond aux requêtes DNS et transmet le trafic au nœud SQL actif. Nous vous déconseillons d'utiliser ce DNS fourni par Active Directory. Le TTL est trop élevé pour fournir un temps de basculement raisonnable et prend souvent jusqu'à 5 minutes pour refléter la nouvelle adresse IP principale. En revanche, pour les installations à haute disponibilité, le Network Load Balancer interne est configuré pour basculer en 30 secondes.
- Un administrateur de domaine Active Directory est requis pour créer le cluster. Cette exigence est due aux autorisations élevées requises pour créer les objets du cluster et modifier les autorisations dans Active Directory. Toutefois, les services SQL Server n'ont pas besoin de s'exécuter en tant qu'administrateur de domaine. Nous vous recommandons donc de créer un deuxième utilisateur Active Directory à cette fin. Toutefois, vous pouvez éliminer cet utilisateur si les services s'exécutent en tant qu'administrateur de domaine. Dans ce cas, l'utilisateur administrateur du domaine doit être ajouté au groupe d'administrateurs Active Directory créé dans le cadre de ce modèle.

Épopées

Configurer les informations d'identification du cluster

Tâche	Description	Compétences requises
Créez des groupes Active Directory.	Dans AWS Managed Microsoft AD, créez les groupes suivants : • Groupe d'administrateurs de cluster — Ce groupe sera ajouté au groupe d'adminis trateurs local sur chaque nœud de cluster. • Groupe de postes de travail distants du cluster : ce groupe sera ajouté au groupe local des utilisateurs du bureau à distance sur chaque nœud du cluster.	Administrateur AD

Tâche	Description	Compétences requises
	Pour plus de détails, consultez la section Création d'un AWS Managed Microsoft AD groupe dans la AWS documentation.	
Créez des utilisateurs Active Directory.	Dans AWS Managed Microsoft AD, créez les utilisateurs suivants • Utilisateur administrateur du domaine : utilisez ce compte pour créer le cluster. • Utilisateur du domaine : les services SQL Server utiliseront ce compte pour s'exécuter. Ajoutez cet utilisateur au groupe d'administrateurs du cluster que vous avez créé lors de la tâche précédente. Pour plus de détails, consultez la section Création AWS Managed Microsoft AD d'un utilisateur dans la AWS documentation.	Administrateur AD

Tâche	Description	Compétences requises
Ajoutez les informations d'identification Active Directory aux secrets.	Utilisez Secrets Manager pour créer quatre secrets afin de stocker les informations suivantes : • Nom d'utilisateur de l'administrateur du domaine • Mot de passe de l'utilisateur administrateur du domaine • Nom d'utilisateur de l'utilisateur du domaine • Mot de passe de l'utilisateur du domaine Pour plus de détails, consultez la section Créer un AWS Secrets Manager secret dans la AWS documentation.	Administrateur AWS

Préparez l'environnement

Tâche	Description	Compétences requises
Créez l'AMI Windows.	Créez une AMI Windows personnalisée qui inclut les logiciels et les configurations requis. Pour plus de détails, consultez la section Informations supplémentaires.	Administrateur AWS, AWS DevOps
Installez Terraform.	Pour installer Terraform, suivez les instructions sur le site Web de Terraform.	AWS DevOps

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le référentiel de ce modèle. Pour plus de détails, consultez la section Clonage d'un dépôt sur le GitHub site Web.	AWS DevOps

Installation du cluster

Tâche	Description	Compétences requises
Modifiez les variables Terraform.	Mettez à jour le `terraform.tfvars` fichier fourni pour définir toutes les variables sur des valeurs adaptées à votre environnement. Par exemple, mettez à jour les `domain_group_rdp_users` variables `domain_group_administrators` et pour utiliser votre nom de domaine Active Directory et le nom des groupes Active Directory créés précédemment.	AWS DevOps
Initialisez Terraform.	Pour voir le déploiement proposé, accédez à la racine du référentiel. Utilisez l'interface de ligne de commande (CLI) Terraform pour exécuter `terraform init` puis exécuter. `terraform plan`	AWS DevOps

Tâche	Description	Compétences requises
Déployez des ressources.	Pour déployer le cluster SQL et les ressources associées, utilisez la CLI Terraform pour l'exécuter. `terraform apply`	AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises
Validez le déploiement.	Pour valider le déploiement, procédez comme suit : 1. Connectez-vous à l'une des EC2 instances Amazon Windows déployées à l'aide de Remote Desktop. 2. Pour plus de détails, consultez la section Se connecter à votre instance Windows à l'aide du protocole RDP dans la AWS documentation. 3. Ouvrez le gestionnaire de clusters Windows Failover. Vérifiez que le cluster a été créé, que le rôle SQL Server a été créé et est en cours d'exécution. 4. Pour tester la connectivité et l'authentification avec SQL Server, utilisez un outil de base de données tel que SQL Server Management Studio pour vous connecter au point de terminaison SQL Server. (La valeur du point de terminaison est stockée dans Secrets Manager.) Pour plus de détails, consultez Connect to Microsoft SQL Server on Amazon EC2 dans la AWS documentation.	DBA, administrateur système AWS

Résolution des problèmes

Problème	Solution
Le provisionnement de Terraform est terminé mais Windows Failover Cluster Manager n'indique pas qu'un cluster a été créé ou que le cluster est dans un état inutilisable.	L'installation complète des ressources et la configuration des clusters peuvent prendre de 45 à 60 minutes. Une fois Terraform terminé, le script de données utilisateur doit s'exécute r jusqu'à la fin, ce qui nécessite plusieurs redémarrages. Pour suivre la progression, vous pouvez utiliser le `Checkpoints` répertoire du `C:\` lecteur et l'installation de SQL Server se connecte`C:\Program Data\Microsoft SQL Server\150\Log` . Lorsque vous avez terminé, le message Installation terminée est disponible dans le `C:\ProgramData \Amazon\EC2-Windows\Launch\Log\ UserdataExecution.log` fichier.
Après avoir provisionné un cluster fonctionn el, l'utilisation de Terraform pour supprimer et recréer le cluster échoue. Terraform est terminé, mais le cluster n'est pas correctement configuré.	Une partie du processus de provisionnement implique l'enregistrement des machines et des objets virtuels dans Active Directory et Active Directory DNS. Lorsque des noms d'ordinat eur existent pour les nœuds du EC2 cluster Amazon et le nœud du cluster, FCI ne peut pas s'initialiser correctement et échouera au provisionnement. Pour résoudre ce problème, effectuez les opérations suivantes : 1. Supprimez les EC2 nœuds Amazon, l'ordinat eur virtuel du cluster et l'identifiant du cluster dans les utilisateurs et ordinateurs Active Directory.

Problème	Solution
	2. Supprimez l'entrée DNS de l'ordinateur virtuel du cluster dans le DNS Active Directory. 3. Exécutez la commande suivante pour supprimer la ressource Terraform de la chaîne aléatoire cluster id. `terragrunt destroy -target=random_string.cluster_id` Cette action supprimera les EC2 instances Amazon existantes. 4. Exécutez `terraform apply` et attendez-vous aux trois nouvelles ressources suivantes : deux EC2 instances Amazon FCI et un identifiant de cluster de chaînes aléatoires.

Ressources connexes

AWS documentation

- Créez des images personnalisées avec Image Builder
- Création d'une clé KMS
- Création d'un bucket à usage général
- Création d'une politique clé
- Création de votre AWS Managed Microsoft AD

Informations supplémentaires

Informations sur le module Terraform

Ce module utilise à la fois la configuration de l'AMI et la configuration des données utilisateur pour obtenir un bon équilibre entre le temps de provisionnement et la stabilité. Pendant le provisionnement, Windows nécessite plusieurs redémarrages et des temps d'attente. Une méthode de points de contrôle a été mise en œuvre pour se protéger contre les boucles infinies lors des redémarrages des données utilisateur persistantes. Les données utilisateur sont configurées pour

être persistantes. Par conséquent, les scripts de configuration des données utilisateur doivent et doivent continuer à être développés pour être idempotents. L'idempotencie rationalise le processus de mise à jour, permettant aux instances d'être échangées au cours d'un cycle de mise à jour sans configuration manuelle pour rejoindre ou recréer des clusters FCI.

Chaînes de connexion SQL Server et clustering en cas de basculement

Le module publiera un secret contenant l'adresse du point de terminaison qui doit être utilisée dans les chaînes de connexion de cette base de données. Le nom du secret suit le format`{environment_name}/sqlserver/{cluster_name}/endpoint`. Pour les installations où un seul nœud est utilisé, vous pouvez vous attendre à ce qu'il s'agisse de l'adresse IP de l'interface SQL Server de l' EC2 instance Amazon. Pour les installations à haute disponibilité (deux instances), vous pouvez vous attendre à ce qu'il s'agisse du nom DNS du Network Load Balancer interne.

Le clustering virtuel par basculement n'est IPs pas pris en charge dans ce module. Une adresse IP virtuelle doit rester dans le même sous-réseau pour fonctionner. En AWS effet, un seul sous-réseau ne peut pas couvrir plusieurs zones de disponibilité. Par conséquent, l'utilisation du virtuel IPs empêcherait ce module d'être considéré comme hautement disponible.

Chaque EC2 instance Amazon reçoit trois adresses IP privées. Leur utilisation est la suivante :

- IP principale pour le trafic réseau : adresse IP source pour le trafic de sortie.
- Communications FCI : utilisées pour maintenir l'état et la synchronisation du cluster de basculement.
- SQL Server (port TCP 1433) : écoute également le trafic cardiaque afin de déterminer quelle instance est principale.

Configuration VPC

Les prérequis répertorient un ensemble d'options DHCP configuré pour utiliser Active Directory pour la résolution DNS. Cependant, cette condition préalable n'est pas une exigence stricte. L'exigence absolue est que les EC2 instances soient capables de résoudre votre nom de domaine Active Directory. Il est possible de répondre à cette exigence par d'autres moyens, par exemple en utilisant des Amazon Route 53 Resolver points de terminaison. Pour plus d'informations, consultez Intégrer la résolution DNS de votre service d'annuaire aux résolveurs Amazon Route 53 (article de AWS blog).

Configuration de l'AMI

L'AMI utilisée dans ce modèle doit contenir les logiciels et configurations prérequis suivants :

1. Téléchargez et étendez les fichiers d'installation de SQL Server 2019 dans`C:\SQL_Install_media`.
2. Installez les fonctionnalités Windows suivantes :
   - `Install-WindowsFeature Failover-Clustering`
   - `Install-WindowsFeature RSAT-AD-PowerShell`
   - `Install-WindowsFeature RSAT-AD-Tools`
   - `Install-WindowsFeature RSAT-Clustering-Mgmt`
   - `Install-WindowsFeature RSAT-Clustering-PowerShell`
   - `Install-WindowsFeature RSAT-Clustering-CmdInterface`
3. Désactivez le pare-feu Windows comme suit :
   - `Get-NetFirewallProfile | Set-NetFirewallProfile -Enabled False`
4. Activez la méthode d'authentification CredSSP (`<domain>`remplacez-la par le nom de domaine Windows de votre organisation) comme suit :
   - `Enable-WSManCredSSP -Role "Server" -Force`
   - `Enable-WSManCredSSP -Role "Client" -DelegateComputer *.<domain>.com -Force`
5. Définissez les clés de registre suivantes :
   - Autoriser les informations d'authentification NTLM :
     - `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation`
       - Nom : `AllowFreshCredentialsWhenNTLMOnly`
       - Valeur : 1
       - Type : `REG_DWORD`
   - Autoriser les ordinateurs du domaine local à utiliser NTLM depuis : PowerShell
     - Trajectoire : `HKLM:\Software\Policies\Microsoft\Windows\CredentialsDelegation\AllowFreshCredentialsWhenNTLMOnly`
       - Nom : 1
       - Valeur : `wsman/*.<domain>.com`
       - Type : `REG_SZ`
6. Configurez la PowerShell galerie comme suit :

- `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`
- `Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force`
- `Set-PSRepository -Name PSGallery -InstallationPolicy Trusted`

7. Installez les PowerShell modules Windows suivants * :
   - `Install-Module -Name ComputerManagementDsc`
   - `Install-Module -Name FailOverClusterDsc`
   - `Install-Module -Name PSDscResources`
   - `Install-Module -Name xSmbShare`
   - `Install-Module -Name xActiveDirectory`
   - `Install-Module -Name SqlServer`

Pour utiliser Image Builder afin de créer l'AMI, suivez les instructions de la section Création d'un pipeline d'images à l'aide de l'assistant EC2 Image Builderconsole de la documentation Image Builder. Pour créer le composant de la recette avec les prérequis précédents, procédez comme suit :

1. Téléchargez le fichier component.yaml depuis le `ami` dossier du référentiel. GitHub
2. Copiez le contenu dans un nouveau composant Image Builder.
3. Mettez à jour les espaces réservés suivants avec vos informations :
   - `<domain>`— Votre nom de domaine Active Directory
   - `<bucket_name>`— Nom du compartiment Amazon S3 contenant l'image SQL Server

Émuler des charges de travail Oracle RAC à l'aide de points de terminaison personnalisés dans Aurora PostgreSQL

Créée par HariKrishna Boorgadda (AWS)

Récapitulatif

Ce modèle décrit comment émuler des services dans une charge de travail Oracle Real Application Clusters (Oracle RAC) en utilisant Amazon Aurora PostgreSQL Compatible Edition avec des points de terminaison personnalisés qui répartissent les charges de travail entre les instances au sein d'un même cluster. Le modèle vous montre comment créer des points de terminaison personnalisés pour les bases de données Amazon Aurora. Les points de terminaison personnalisés vous permettent de répartir et d'équilibrer les charges de travail entre différents ensembles d'instances de base de données de votre cluster Aurora.

Dans un environnement Oracle RAC, les services peuvent couvrir une ou plusieurs instances et faciliter l'équilibrage de la charge de travail en fonction des performances des transactions. Les fonctionnalités du service incluent la restauration end-to-end sans surveillance, l'échelonnement des modifications en fonction de la charge de travail et la transparence totale de la localisation. Vous pouvez utiliser ce modèle pour émuler certaines de ces fonctionnalités. Par exemple, vous pouvez émuler la possibilité de router les connexions pour les applications de reporting.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un pilote JDBC PostgreSQL
- Une base de données compatible avec Aurora PostgreSQL
- Une base de données Oracle RAC migrée vers une base de données compatible Aurora PostgreSQL

Limites

- Pour connaître les limites applicables aux points de terminaison personnalisés, consultez la section Spécification des propriétés des points de terminaison personnalisés dans la documentation Amazon RDS.

Architecture

Pile technologique source

- Une base de données Oracle RAC à trois nœuds

Pile technologique cible

- Une base de données compatible Aurora PostgreSQL avec deux répliques de lecture

Architecture source

Le schéma suivant montre l'architecture d'une base de données Oracle RAC à trois nœuds.

Architecture cible

Le schéma suivant montre l'architecture d'une base de données compatible Aurora PostgreSQL avec deux répliques en lecture. Trois applications/services différents utilisent des points de terminaison personnalisés, qui desservent différents utilisateurs d'applications et redirigent le trafic et la charge entre les répliques principales et les répliques en lecture.

Outils

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

Épopées

Création du cluster compatible avec Aurora PostgreSQL

Tâche	Description	Compétences requises
Créer un cluster.	Pour créer le cluster, consultez la section Création d'un cluster de base de données et connexion à une base de données sur un cluster de base de données Aurora PostgreSQL dans la documentation Amazon RDS.	Administrateur AWS
Créez un groupe de paramètres personnalisé pour la charge de travail.	Pour créer un groupe de paramètres, consultez la section Création d'un groupe de paramètres de cluster de base de données dans la documentation Amazon RDS.	Administrateur AWS
Créez des notifications d'événements et des alarmes.	Vous pouvez utiliser les notifications d'événements et les CloudWatch alarmes Amazon pour vous avertir lorsque le cluster change d'état et pour capturer des métriques lorsqu'un seuil prédéfini est atteint. Pour créer une CloudWatch alarme, voir Création d'une CloudWatch alarme basée sur un seuil statique dans la CloudWatch documentation.	Administrateur AWS

Tâche	Description	Compétences requises
	Pour créer une notification d'événement, consultez la section Création d'une règle d' CloudWatch événements déclenchant un événement dans la CloudWatch documentation.	

Ajouter des répliques au cluster de base de données compatible Aurora PostgreSQL

Tâche	Description	Compétences requises
Ajoutez les répliques lues au cluster.	1. Créez une réplique de lecture. 2. **Note** Ajoutez la réplique en lecture dans la même zone de disponibilité que celle dans laquelle se trouve votre cluster de base de données. : vous pouvez utiliser une autre zone de disponibilité si des exigences doivent être satisfaites pour votre nœud de basculement.	Administrateur AWS
Notez le point de terminaison de lecture de la réplique.	Documentez votre point de terminaison de reproduction	Administrateur AWS

Tâche	Description	Compétences requises
	pour une utilisation ultérieure lors de la création des points de terminaison personnalisés.	

Création de points de terminaison personnalisés

Tâche	Description	Compétences requises
Entrez un nom pour le point de terminaison personnalisé.	Pour chaque point de terminaison dont vous avez besoin, créez un nom de point de terminaison unique associé à votre charge de travail ou à votre application.	Administrateur AWS
Ajoutez les membres du point de terminaison.	Ajoutez vos points de terminaison de reproduct ion de lecture à un groupe personnalisé. Pour plus d'informations, consultez Modifier un point de terminais on personnalisé dans la documentation Amazon RDS.	Administrateur AWS
(Facultatif) Ajoutez les futures instances au cluster.	Si vous souhaitez ajouter d'autres répliques ou points de terminaison au groupe personnalisé, consultez la section Ajouter des répliques Aurora à un cluster de bases de données dans la documentation Amazon RDS.	Administrateur AWS
Créez le point de terminaison.	Pour créer le point de terminaison, consultez la	Administrateur AWS

Tâche	Description	Compétences requises
	section Création d'un point de terminaison personnalisé dans la documentation Amazon RDS.	

Testez les connexions aux applications à l'aide de points de terminaison personnalisés

Tâche	Description	Compétences requises
Partagez les détails du point de terminaison personnalisé avec l'application qui indique votre charge de travail.	Ajoutez les détails de votre point de terminaison personnalisé aux détails de connexion à la base de données dans l'application de reporting que vous prévoyez de tester.	Administrateur AWS
Connectez la charge de travail à l'aide du point de terminaison personnalisé.	Validez les détails du point de terminaison personnalisé dans l'application de création de rapports.	Administrateur AWS
Vérifiez les détails de connexion dans la base de données.	1. Testez le nom d'utilisateur et le nombre de connexions pour votre application. 2. Vérifiez l'équilibrage de charge entre vos charges de travail pour vous assurer que les connexions sont réparties entre différent s points de terminaison personnalisés (répliques principales et répliques de lecture).	Administrateur AWS

Ressources connexes

- Types de points de terminaison Aurora
- Règles d'adhésion pour les points de terminaison personnalisés
- End-to-end Exemple de CLI AWS pour les points de terminaison personnalisés
- Amazon Aurora comme alternative à Oracle RAC
- Défis liés à la migration d'Oracle vers PostgreSQL et comment les surmonter

Activer les connexions chiffrées pour les instances de base de données PostgreSQL dans Amazon RDS

Créée par Rohit Kapoor (AWS)

Récapitulatif

Amazon Relational Database Service (Amazon RDS) prend en charge le chiffrement SSL pour les instances de base de données PostgreSQL. À l'aide du protocole SSL, vous pouvez chiffrer une connexion PostgreSQL entre vos applications et vos instances de base de données Amazon RDS for PostgreSQL. Par défaut, Amazon RDS pour PostgreSQL utilise le chiffrement. SSL/TLS and expects all clients to connect by using SSL/TLS Amazon RDS pour PostgreSQL prend en charge les versions 1.1 et 1.2 du protocole TLS.

Ce modèle décrit comment activer les connexions chiffrées pour une instance de base de données Amazon RDS for PostgreSQL. Vous pouvez utiliser le même processus pour activer les connexions chiffrées pour Amazon Aurora PostgreSQL Compatible Edition.

Conditions préalables et limitations

- Un compte AWS actif
- Une instance de base de données Amazon RDS pour PostgreSQL
- Un bundle SSL

Architecture

Outils

- pgAdmin est une plateforme d'administration et de développement open source pour PostgreSQL. Vous pouvez utiliser pgAdmin sous Linux, Unix, macOS et Windows pour gérer vos objets de base de données dans PostgreSQL 10 et versions ultérieures.
- Les éditeurs PostgreSQL fournissent une interface plus conviviale pour vous aider à créer, développer et exécuter des requêtes, ainsi qu'à modifier le code en fonction de vos besoins.

Bonnes pratiques

- Surveillez les connexions de base de données non sécurisées.

- Auditez les droits d'accès aux bases de données
- Assurez-vous que les sauvegardes et les instantanés sont chiffrés au repos.
- Surveillez l'accès aux bases de données.
- Évitez les groupes d'accès illimité.
- Améliorez vos notifications avec Amazon GuardDuty.
- Surveillez régulièrement le respect des politiques.

Épopées

Téléchargez un certificat fiable et importez-le dans votre magasin de confiance

Tâche	Description	Compétences requises
Chargez un certificat sécurisé sur votre ordinateur.	Pour ajouter des certificats au magasin Trusted Root Certification Authorities de votre ordinateur, procédez comme suit. (Ces instructions utilisent Window Server comme exemple.) 1. Dans Windows Server, choisissez Démarrer, Exécuter, puis tapez mmc. 2. Dans la console, choisissez Fichier, Ajouter/Supprimer un composant logiciel enfichable. 3. Sous Composants logiciels enfichables disponibles, sélectionnez Certificats, puis Ajouter. 4. Sous Ce composant logiciel enfichable gérera toujours les certificats pour,	DevOps ingénieur, ingénieur en migration, DBA

Tâche	Description	Compétences requises
	choisissez Compte d'ordinateur, Suivant. 5. Choisissez Ordinateur local, puis Terminer. 6. Si vous n'avez plus de composant logiciel enfichable à ajouter à la console, cliquez sur OK. 7. Dans l'arborescence de la console, double-cliquez sur Certificats. 8. Cliquez avec le bouton droit sur Autorités de certification racine fiables. 9. Choisissez Toutes les tâches, puis Importer pour importer les certificats téléchargés. 10. Suivez les étapes de l'assistant d'importation de certificats.	

Forcer les connexions SSL

Tâche	Description	Compétences requises
Créez un groupe de paramètres et définissez le paramètre rds.force_ssl.	Si l'instance de base de données PostgreSQL possède un groupe de paramètres personnalisé, modifiez le groupe de paramètres et `rds.force_ssl` passez à 1.	DevOps ingénieur, ingénieur en migration, DBA

Tâche	Description	Compétences requises
	Si l'instance de base de données utilise le groupe de paramètres par défaut qui n'`rds.force_ssl` est pas activé, créez un nouveau groupe de paramètres. Vous pouvez modifier le nouveau groupe de paramètres à l'aide de l'API Amazon RDS ou manuellement comme indiqué dans les instructions suivantes . Pour créer un nouveau groupe de paramètres : 1. Connectez-vous à la console de gestion AWS et ouvrez la console Amazon RDS pour la région AWS qui héberge l'instance de base de données. 2. Dans le panneau de navigation, choisissez Groupes de paramètres. 3. Choisissez Créer un groupe de paramètres, puis définissez les valeurs suivantes : • Pour la famille de groupes de paramètres, choisissez postgres14. • Dans Nom du groupe, tapez pgsql- -ssl<database_instance>.	

Tâche	Description	Compétences requises
	• Dans Description, entrez une description en forme libre pour le groupe de paramètres que vous ajoutez. • Choisissez Créer. 4. Choisissez le groupe de paramètres que vous avez créé. 5. Dans Parameter group actions (Actions de groupe de paramètres), choisissez Edit (Modifier). 6. Trouvez rds.force_ssl et remplacez sa valeur par 1. **Note** Effectuez des tests côté client avant de modifier ce paramètre. 7. Sélectionnez Enregistrer les modifications. Pour associer le groupe de paramètres à votre instance de base de données PostgreSQL : 1. Sur la console Amazon RDS, dans le volet de navigation, choisissez	

Tâche	Description	Compétences requises
	Databases, puis choisissez l'instance de base de données PostgreSQL. 2. Sélectionnez Modifier. 3. Sous Configuration supplémentaire, choisissez le nouveau groupe de paramètres, puis choisissez Continuer. 4. Sous Modifications du calendrier, sélectionnez Appliquer immédiatement. 5. Choisissez Modifier l'instance de base de données. Pour plus d'informations, consultez la documentation Amazon RDS.	
Forcez les connexions SSL.	Connectez-vous à l'instance de base de données Amazon RDS for PostgreSQL. Les tentatives de connexion qui n'utilisent pas le protocole SSL sont rejetées avec un message d'erreur. Pour plus d'informations, consultez la documentation Amazon RDS.	DevOps ingénieur, ingénieur en migration, DBA

Installer l'extension SSL

Tâche	Description	Compétences requises

Installez l'extension SSL.	1. Lancez une connexion psql ou pgAdmin en tant que DBA.
	2. Appelez la fonction ssl_is_used () pour déterminer si le protocole SSL est utilisé.
	`select ssl_is_used();`
	La fonction renvoie `t` si la connexion utilise le protocole SSL ; dans le cas contraire, elle renvoie le résultat`f`.
	3. Installez l'extension SSL.
	`create extension sslinfo;`
	`show ssl;`
	`select ssl_cipher();`
	Pour plus d'informations, consultez la documentation Amazon RDS.
		DevOps ingénieur, ingénieur en migration, DBA

Configuration de votre client PostgreSQL pour le protocole SSL

Tâche	Description	Compétences requises
Configurez un client pour le protocole SSL.	En utilisant le protocole SSL, vous pouvez démarrer	DevOps ingénieur, ingénieur en migration, DBA

Tâche	Description	Compétences requises

	le serveur PostgreSQL en prenant en charge les connexions chiffrées utilisant les protocoles TLS. Le serveur écoute les connexions standard et SSL sur le même port TCP, et négocie avec tout client qui se connecte pour savoir s'il convient d'utiliser le protocole SSL. Par défaut, il s'agit d'une option client.
	
	Si vous utilisez le client PSQL :
	
	1. Assurez-vous que le certificat Amazon RDS a été chargé sur votre ordinateur local.
	2. Lancez une connexion client SSL en ajoutant ce qui suit :
	
	`psql postgres -h SOMEHOST.amazonaws.com -p 8192 -U someuser sslmode=verify-full sslrootcert=rds-ssl-ca-cert.pem`
	`select ssl_cipher();`
	
	Pour les autres clients PostgreSQL :	

Tâche	Description	Compétences requises
	• Modifiez le paramètre de clé publique de l'application correspondante. Cela peut être disponible en option, dans le cadre de votre chaîne de connexion ou en tant que propriété sur la page de connexion dans les outils de l'interface graphique. Consultez les pages suivantes pour ces clients : • Documentation de pgAdmin • Documentation JDBC	

Résolution des problèmes

Problème	Solution
Impossible de télécharger le certificat SSL.	Vérifiez votre connexion au site Web et réessayez de télécharger le certificat sur votre ordinateur local.

Ressources connexes

- Documentation Amazon RDS pour PostgreSQL
- Utilisation du protocole SSL avec une instance de base de données PostgreSQL (documentation Amazon RDS)
- Connexions TCP/IP sécurisées avec SSL (documentation PostgreSQL)
- Utilisation du protocole SSL (documentation JDBC)

Chiffrer une instance de base de données Amazon RDS pour PostgreSQL existante

Créée par Piyush Goyal (AWS), Shobana Raghu (AWS) et Yaser Raja (AWS)

Récapitulatif

Ce modèle explique comment chiffrer une instance de base de données Amazon Relational Database Service (Amazon RDS) existante pour PostgreSQL dans le cloud AWS avec un temps d'arrêt minimal. Ce processus fonctionne également pour les instances de base de données Amazon RDS for MySQL.

Vous pouvez activer le chiffrement pour une instance de base de données Amazon RDS lorsque vous la créez, mais pas après sa création. Toutefois, vous pouvez ajouter le chiffrement à une instance de base de données non chiffrée en créant un instantané de votre instance de base de données, puis en créant une copie chiffrée de cet instantané. Vous pouvez ensuite restaurer une instance de base de données à partir de l'instantané chiffré pour obtenir une copie chiffrée de votre instance de base de données d'origine. Si votre projet prévoit des interruptions (au moins pour les transactions d'écriture) pendant cette activité, c'est tout ce que vous devez faire. Lorsque la nouvelle copie chiffrée de l'instance de base de données est disponible, vous pouvez faire pointer vos applications vers la nouvelle base de données. Toutefois, si votre projet ne prévoit pas de temps d'arrêt important pour cette activité, vous avez besoin d'une autre approche permettant de minimiser le temps d'arrêt. Ce modèle utilise le service AWS Database Migration Service (AWS DMS) pour migrer et répliquer en continu les données afin que le passage à la nouvelle base de données chiffrée puisse être effectué avec un temps d'arrêt minimal.

Les instances de base de données chiffrées Amazon RDS utilisent l'algorithme de chiffrement standard AES-256 pour chiffrer vos données sur le serveur qui héberge vos instances de base de données Amazon RDS. Une fois vos données chiffrées, Amazon RDS gère l'authentification de l'accès et le déchiffrement de vos données de manière transparente, avec un impact minimal sur les performances. Vous n'avez pas besoin de modifier vos applications clientes de base de données pour utiliser le chiffrement.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

- Une instance de base de données Amazon RDS pour PostgreSQL non chiffrée
- Expérience de travail avec (création, modification ou arrêt) de tâches AWS DMS (voir Utilisation des tâches AWS DMS dans la documentation AWS DMS)
- Connaissance d'AWS Key Management Service (AWS KMS) pour le chiffrement des bases de données (voir la documentation AWS KMS)

Limites

- Vous pouvez activer le chiffrement pour une instance de base de données Amazon RDS uniquement lorsque vous la créez, et non après la création de l'instance de base de données.
- Les données des tables non enregistrées ne seront pas restaurées à l'aide de snapshots. Pour plus d'informations, consultez les meilleures pratiques d'utilisation de PostgreSQL.
- Vous ne pouvez pas avoir un réplica en lecture chiffré d'une instance de base de données non chiffrée ni un réplica en lecture non chiffré d'une instance de base de données chiffrée.
- Vous ne pouvez pas restaurer un instantané non chiffré ou une sauvegarde non chiffrée vers une instance de base de données chiffrée.
- AWS DMS ne transfère pas automatiquement les séquences. Des étapes supplémentaires sont donc nécessaires pour gérer cela.

Pour plus d'informations, consultez la section Limitations des instances de base de données chiffrées Amazon RDS dans la documentation Amazon RDS.

Architecture

Architecture de la source

- Instance de base de données RDS non chiffrée

Architecture cible

- Instance de base de données RDS cryptée
  - L'instance de base de données RDS de destination est créée en restaurant la copie instantanée de base de données de l'instance de base de données RDS source.
  - Une clé AWS KMS est utilisée pour le chiffrement lors de la restauration du snapshot.
  - Une tâche de réplication AWS DMS est utilisée pour migrer les données.

Outils

Outils utilisés pour activer le chiffrement :

- Clé AWS KMS pour le chiffrement : lorsque vous créez une instance de base de données chiffrée, vous pouvez choisir une clé gérée par le client ou la clé gérée par AWS pour Amazon RDS afin de chiffrer votre instance de base de données. Si vous ne spécifiez pas l'identifiant de clé pour une clé gérée par le client, Amazon RDS utilise la clé gérée AWS pour votre nouvelle instance de base de données. Amazon RDS crée une clé gérée par AWS pour Amazon RDS pour votre compte AWS. Votre compte AWS possède une clé gérée AWS différente pour Amazon RDS pour chaque région AWS. Pour plus d'informations sur l'utilisation des clés KMS pour le chiffrement Amazon RDS, consultez la section Chiffrement des ressources Amazon RDS.

Outils utilisés pour la réplication continue :

- AWS DMS — Vous pouvez utiliser AWS Database Migration Service (AWS DMS) pour répliquer les modifications de la base de données source vers la base de données cible. Il est important de synchroniser les bases de données source et cible afin de minimiser les temps d'arrêt. Pour plus d'informations sur la configuration d'AWS DMS et la création de tâches, consultez la documentation AWS DMS.

Épopées

Créez un instantané de l'instance de base de données source et chiffrez-le

Tâche	Description	Compétences requises
Vérifiez les détails de l'instance de base de données PostgreSQL source.	Sur la console Amazon RDS, choisissez l'instance de base de données PostgreSQL source. Dans l'onglet Configuration, assurez-vous que le chiffrement n'est pas activé pour l'instance. Pour une illustration d'écran,	DBA

Tâche	Description	Compétences requises
	consultez la section Informations supplémentaires.	
Créez le snapshot de base de données.	Créez un instantané de base de données de l'instance que vous souhaitez chiffrer. Le temps nécessaire pour créer un instantané dépend de la taille de votre base de données. Pour obtenir des instructions, consultez la section Création d'un instantané de base de données dans la documentation Amazon RDS.	DBA

Tâche	Description	Compétences requises
Chiffrez le cliché.	Dans le volet de navigation de la console Amazon RDS, choisissez Snapshots, puis sélectionnez l'instantané de base de données que vous avez créé. Sous Actions, choisissez Copier un instantané. Indiquez la région AWS de destination et le nom de la copie instantanée de base de données dans les champs correspondants. Cochez la case Activer le chiffrement. Pour Clé principale, spécifiez l'identifiant de clé KMS à utiliser pour chiffrer la copie de l'instantané de base de données. Choisissez Copier l'instantané. Pour plus d'informations, consultez Copier un instantané dans la documentation Amazon RDS.	DBA

Préparer l'instance de base de données cible

Tâche	Description	Compétences requises
Restaurez le snapshot de base de données.	Sur la console Amazon RDS, choisissez Snapshots. Choisissez l'instantané chiffré que vous avez créé. Pour Actions, choisissez Restore Snapshot (Restaurer l'instantané). Pour l'identifia	DBA

Tâche	Description	Compétences requises
	nt d'instance de base de données, fournissez un nom unique pour la nouvelle instance de base de données. Passez en revue les détails de l'instance, puis choisisse z Restore DB Instance. Une nouvelle instance de base de données cryptée sera créée à partir de votre instantan é. Pour plus d'informations, consultez la section Restaurat ion à partir d'un instantané de base de données dans la documentation Amazon RDS.	
Migrez les données à l'aide d'AWS DMS.	Sur la console AWS DMS, créez une tâche AWS DMS. Pour le type de migration, choisissez Migrer les données existantes et répliquer les modifications en cours. Dans Paramètres des tâches, pour le mode de préparation de la table cible, choisissez Truncate. Pour plus d'informa tions, consultez la section Création d'une tâche dans la documentation AWS DMS.	DBA

Tâche	Description	Compétences requises
Activez la validation des données.	Dans Paramètres des tâches, choisissez Activer la validation. Cela vous permet de comparer les données source aux données cibles afin de vérifier que les données ont été migrées correctement.	DBA
Désactivez les contraintes sur l'instance de base de données cible.	Désactivez les déclencheurs et les contraintes de clé étrangère sur l'instance de base de données cible, puis lancez la tâche AWS DMS. Pour plus d'informations sur la désactivation des déclencheurs et des contraintes liées aux clés étrangères, consultez la documentation AWS DMS.	DBA
Vérifiez les données.	Une fois le chargement complet terminé, vérifiez les données de l'instance de base de données cible pour voir si elles correspondent aux données source. Pour plus d'informations, consultez la section Validation des données AWS DMS dans la documentation AWS DMS.	DBA

Passez à l'instance de base de données cible

Tâche	Description	Compétences requises
Arrêtez les opérations d'écriture sur l'instance de base de données source.	Arrêtez les opérations d'écriture sur l'instance de base de données source afin que le temps d'arrêt de l'application puisse commencer. Vérifiez qu'AWS DMS a terminé la réplication des données du pipeline. Activez les déclencheurs et les clés étrangères sur l'instance de base de données cible.	DBA
Mettre à jour les séquences de base	Si la base de données source contient des numéros de séquence, vérifiez et mettez à jour les séquences dans la base de données cible.	DBA
Configurez le point final de l'application.	Configurez les connexions de vos applications pour utiliser les nouveaux points de terminaison de l'instance de base de données Amazon RDS. L'instance de base de données est désormais cryptée.	DBA, propriétaire de l'application

Ressources connexes

- Création d'une tâche AWS DMS
- Surveillance des tâches de réplication à l'aide d'Amazon CloudWatch
- Surveillance des tâches AWS DMS

- Mise à jour de la clé de chiffrement Amazon RDS

Informations supplémentaires

Vérification du chiffrement de l'instance de base de données PostgreSQL source :

Remarques supplémentaires concernant ce modèle :

- Activez la réplication sur PostgreSQL en définissant `rds.logical_replication` le paramètre sur 1.

Remarque importante : les emplacements de réplication conservent les fichiers WAL (Write Ahead Log) jusqu'à ce qu'ils soient consommés en externe, par exemple par `pg_recvlogical` des tâches d'extraction, de transformation et de chargement (ETL) ou par AWS DMS. Lorsque vous définissez la valeur du `rds.logical_replication` paramètre sur 1, AWS DMS définit les `max_connections` paramètres `wal_levelmax_wal_senders`,`max_replication_slots`, et. Si des emplacements de réplication logiques sont présents mais qu'aucun consommateur n'est utilisé pour les fichiers WAL conservés par le slot de réplication, vous pouvez constater une augmentation de l'utilisation du disque du journal des transactions et une diminution constante de l'espace de stockage disponible. Pour plus d'informations et pour savoir comment résoudre ce problème, consultez l'article Comment puis-je identifier la cause de l'erreur « Aucun espace restant sur l'appareil » ou « » DiskFull sur Amazon RDS for PostgreSQL ? dans le centre de connaissances AWS Support.

- Les modifications de schéma que vous apportez à l'instance de base de données source après avoir créé le snapshot de base de données ne seront pas présentes sur l'instance de base de données cible.
- Après avoir créé une instance de base de données chiffrée, vous ne pouvez pas modifier la clé KMS utilisée par cette instance de base de données. Assurez-vous de déterminer vos exigences en matière de clé KMS avant de créer votre instance de base de données chiffrée.
- Vous devez désactiver les déclencheurs et les clés étrangères sur l'instance de base de données cible avant d'exécuter la tâche AWS DMS. Vous pouvez les réactiver une fois la tâche terminée.

Appliquer le balisage automatique des bases de données Amazon RDS au lancement

Créée par Susanne Kangnoh (AWS) et Archit Mathur (AWS)

Récapitulatif

Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud Amazon Web Services (AWS). Il fournit des capacités redimensionnables, à faible coût, pour les bases de données relationnelles classiques, et gère les tâches courantes d'administration de base de données.

Vous pouvez utiliser le balisage pour classer vos ressources AWS de différentes manières.
Le balisage des bases de données relationnelles est utile lorsque votre compte comporte de nombreuses ressources et que vous souhaitez identifier rapidement une ressource spécifique en fonction des balises. Vous pouvez utiliser les balises Amazon RDS pour ajouter des métadonnées personnalisées à vos instances de base de données RDS. Une balise se compose d'une clé et d'une valeur définies par l'utilisateur. Nous vous recommandons de créer un ensemble cohérent de balises pour répondre aux exigences de votre organisation.

Ce modèle fournit un CloudFormation modèle AWS pour vous aider à surveiller et à étiqueter les instances de base de données RDS. Le modèle crée un événement Amazon CloudWatch Events qui surveille l'DBInstanceévénement AWS CloudTrail Create. (CloudTrail capture les appels d'API pour Amazon RDS sous forme d'événements.) Lorsqu'il détecte cet événement, il appelle une fonction AWS Lambda qui applique automatiquement les clés de balise et les valeurs que vous définissez. Le modèle envoie également une notification indiquant que l'instance a été balisée, à l'aide d'Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un bucket Amazon Simple Storage Service (Amazon S3) pour télécharger le code Lambda.
- Adresse e-mail à laquelle vous souhaitez recevoir des notifications de marquage.

Limites

- La solution prend en charge la CloudTrail création DBInstance d'événements. Il ne crée pas de notifications pour d'autres événements.

Architecture

Architecture du flux de travail

Automatisation et mise à l'échelle

- Vous pouvez utiliser le CloudFormation modèle AWS à plusieurs reprises pour différents comptes et régions AWS. Vous ne devez exécuter le modèle qu'une seule fois dans chaque région ou compte.

Outils

Services AWS

- AWS CloudTrail — AWS CloudTrail est un service AWS qui vous aide dans les domaines de la gouvernance, de la conformité et de l'audit opérationnel et des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS. CloudWatch Events prend connaissance des changements opérationnels au fur et à mesure qu'ils se produisent et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans qu'il soit nécessaire de configurer ou de gérer des serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service Web qui permet aux applications, aux utilisateurs finaux et aux appareils d'envoyer et de recevoir instantanément des notifications depuis le cloud.

Code

Ce modèle inclut une pièce jointe contenant deux fichiers :

- `index.zip`est un fichier compressé qui inclut le code Lambda pour ce modèle.
- `rds.yaml`est un CloudFormation modèle qui déploie le code Lambda.

Consultez la section Epics pour plus d'informations sur l'utilisation de ces fichiers.

Épopées

Déployez le code Lambda

Tâche	Description	Compétences requises
Téléchargez le code dans un compartiment S3.	Créez un nouveau compartiment S3 ou utilisez un compartiment S3 existant pour télécharger le `index.zip` fichier joint (code Lambda). Ce compartiment doit se trouver dans la même région AWS que les ressources (instances de base de données RDS) que vous souhaitez surveiller.	Architecte du cloud
Déployez le CloudFormation modèle.	Ouvrez la console Cloudformation dans la même région AWS que le compartiment S3 et déployez le `rds.yaml`	Architecte du cloud

Tâche	Description	Compétences requises
	fichier fourni dans la pièce jointe. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou sélectionné dans le premier épisode épique. Ce compartiment S3 contient le fichier .zip pour le code Lambda et doit se trouver dans la même région AWS que CloudFormation le modèle et les instances de base de données RDS que vous souhaitez surveiller.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple, ou). `index.zip` `controls/index.zip`	Architecte du cloud
Indiquez une adresse e-mail.	Indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications de violation.	Architecte du cloud

Tâche	Description	Compétences requises
Spécifiez un niveau de journalisation.	Spécifiez le niveau de journalisation et la verbosité. `Info`désigne des messages d'information détaillés sur la progression de l'application et ne doit être utilisé que pour le débogage. `Error`désigne les événements d'erreur susceptib les de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud
Entrez les clés et les valeurs de balise pour vos instances de base de données RDS.	Entrez les clés de balise et les valeurs requises que vous souhaitez appliquer automatiq uement à l'instance RDS. Pour plus d'informations, consultez la section Marquage des ressources Amazon RDS dans la documentation AWS.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'abonnement par e-mail.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Pour recevoir des notificat ions lorsque vos instances	Architecte du cloud

Tâche	Description	Compétences requises
	sont étiquetées, vous devez confirmer cet abonnement par e-mail.	

Ressources connexes

- Création d'un compartiment (documentation Amazon S3)
- Marquage des ressources Amazon RDS (documentation Amazon Aurora)
- Chargement d'objets (documentation Amazon S3)
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail (CloudWatch documentation Amazon)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Estimation du coût d'une table DynamoDB pour une capacité à la demande

Créée par Moinul Al-Mamun (AWS)

Récapitulatif

Amazon DynamoDB est une base de données transactionnelle NoSQL qui fournit une latence à un chiffre en millisecondes, même à l'échelle du pétaoctet. Cette offre sans serveur Amazon Web Services (AWS) gagne en popularité en raison de ses performances et de son évolutivité constantes. Vous n'avez pas besoin de provisionner l'infrastructure sous-jacente. Votre table unique peut atteindre des pétaoctets.

Avec le mode capacité à la demande, vous payez par demande pour les lectures et les écritures de données effectuées par votre application sur les tables. Les frais AWS sont basés sur le cumul des unités de demande de lecture (RRUs) et des unités de demande d'écriture (WRUs) par mois. DynamoDB surveille la taille de votre table en permanence tout au long du mois afin de déterminer vos frais de stockage. Il prend en charge la sauvegarde continue avec point-in-time-recovery (PITR). DynamoDB surveille la taille de vos tables compatibles PITR en permanence tout au long du mois afin de déterminer vos frais de sauvegarde.

Pour estimer le coût DynamoDB d'un projet, il est important de calculer la quantité de RRU, de WRU et de stockage qui sera consommée aux différentes étapes du cycle de vie de votre produit. Pour une estimation approximative des coûts, vous pouvez utiliser le calculateur de prix AWS, mais vous devez fournir un nombre approximatif de RRUs WRUs, et les exigences de stockage pour votre table. Il peut être difficile de les estimer au début du projet. Le calculateur de prix AWS ne prend pas en compte le taux de croissance des données ni la taille des éléments, ni le nombre de lectures et d'écritures pour la table de base et les index secondaires globaux (GSIs) séparément. Pour utiliser le calculateur de prix AWS, vous devez estimer tous ces aspects en supposant des chiffres approximatifs pour le WRU, le RRU et la taille du stockage afin d'obtenir votre estimation des coûts.

Ce modèle fournit un mécanisme et un modèle Microsoft Excel réutilisable pour estimer les facteurs de coût de base de DynamoDB, tels que les coûts d'écriture, de lecture, de stockage, de sauvegarde et de restauration, pour le mode capacité à la demande. Il est plus détaillé que le calculateur de prix AWS, et il prend en compte le tableau de base et les GSIs exigences indépendamment. Il prend également en compte le taux de croissance mensuel des données par article et prévoit les coûts sur trois ans.

Conditions préalables et limitations

Prérequis

- Connaissances de base de la conception de modèles de données DynamoDB et DynamoDB
- Connaissance de base de la tarification DynamoDB, de la WRU, de la RRU, du stockage, de la sauvegarde et de la restauration (pour plus d'informations, voir Tarification de la capacité à la demande)
- Connaissance de vos données, de votre modèle de données et de la taille des éléments dans DynamoDB
- Connaissance de DynamoDB GSIs

Limites

- Le modèle fournit un calcul approximatif, mais il ne convient pas à toutes les configurations. Pour obtenir une estimation plus précise, vous devez mesurer la taille individuelle de chaque article dans le tableau de base et GSIs.
- Pour une estimation plus précise, vous devez prendre en compte le nombre prévu d'écritures (insertion, mise à jour et suppression) et de lectures pour chaque élément au cours d'un mois moyen.
- Ce modèle permet d'estimer uniquement les coûts d'écriture, de lecture, de stockage, de sauvegarde et de restauration pour les prochaines années sur la base d'hypothèses de croissance des données fixes.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.

Autres outils

- AWS Pricing Calculator est un outil de planification basé sur le Web que vous pouvez utiliser pour créer des estimations pour vos cas d'utilisation d'AWS.

Bonnes pratiques

Pour réduire les coûts, prenez en compte les meilleures pratiques de conception DynamoDB suivantes.

- Conception de clés de partition : utilisez une clé de partition à cardinalité élevée pour répartir la charge de manière uniforme.
- Modèle de conception de liste de contiguïté : utilisez ce modèle de conception pour la gestion one-to-many et many-to-many les relations.
- Index clairsemé — Utilisez un index clairsemé pour votre. GSIs Lorsque vous créez un GSI, vous spécifiez une clé de partition et éventuellement une clé de tri. Seuls les éléments de la table de base contenant une clé de partition de GSI correspondante apparaissent dans l'index fragmenté. Cela permet de rester GSIs plus petit.
- Surcharge d'index : utilisez le même GSI pour indexer différents types d'élément.
- Partitionnement d'écriture de GSI : partitionnez judicieusement afin de distribuer les données entre les partitions pour des requêtes plus efficaces et plus rapides.
- Objets de grande taille : stockez uniquement les métadonnées dans la table, enregistrez le blob dans Amazon S3 et conservez la référence dans DynamoDB. Divisez les éléments volumineux en plusieurs éléments et indexez efficacement à l'aide des clés de tri.

Pour d'autres bonnes pratiques de conception, veuillez consulter le Guide du développeur Amazon DynamoDB.

Épopées

Extraire les informations relatives aux éléments de votre modèle de données DynamoDB

Tâche	Description	Compétences requises
Obtenez la taille de l'article.	1. Vérifiez combien de types d'articles vous allez stocker dans votre table. 2. Pour calculer la taille de chaque élément en kilo-octets, ajoutez les tailles de clé et de valeur de chaque attribut. 3. Calculez la taille des éléments pour une table de base et pour chaque GSI.	Ingénieur de données

Tâche	Description	Compétences requises

Estimez le coût d'écriture.	Pour estimer le coût d'écriture en mode capacité à la demande, vous devez d'abord mesurer la quantité WRUs qui sera consommée en un mois. Pour cela, vous devez prendre en compte les facteurs suivants :
	• Nombre d'opérations de création, de mise à jour et de suppression pour chaque élément au cours d'un mois.
	• Nombre de disponibles GSIs. Examinez chaque indice indépendamment.
	  • Taille moyenne d'un élément d'index
	  • Nombre de temps de synchronisation sur un index
	• Combien de nouveaux éléments (composants ou produits, par exemple) seront ajoutés au tableau chaque mois ? Le nombre d'éléments ajoutés peut être différent chaque mois, mais vous pouvez supposer un taux de croissance moyen en fonction de vos analyses de rentabilisation.
		Ingénieur de données

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Informations supplémentaires.	
Estimez le coût de lecture.	Pour estimer le coût de lecture en mode à la demande, vous devez d'abord mesurer la quantité RRUs qui sera consommée en un mois. Pour cela, vous devez prendre en compte les facteurs suivants : • Nombre de disponibles GSIs. Examinez chaque indice indépendamment. • Taille moyenne d'un élément d'index • Nombre moyen de lectures par produit et par mois. • Nombre total d'éléments disponibles (composants ou produits) dans le tableau DynamoDB.	Ingénieur de données, développeur d'applications

Tâche	Description	Compétences requises
Estimez la taille et le coût du stockage.	Tout d'abord, estimez le besoin de stockage mensuel moyen en fonction de la taille de votre article indiquée dans le tableau. Calculez ensuite le coût du stockage en multiplia nt la taille du stockage par le prix par Go de stockage pour votre région AWS. Si vous avez déjà saisi des données pour estimer le coût d'écriture, il n'est pas nécessaire de les saisir à nouveau pour calculer la taille de stockage. Dans le cas contraire, pour estimer la taille du stockage, vous devez prendre en compte les facteurs suivants : • Nombre d'éléments de données dans un module (produit) en fonction de la conception de votre table. • Taille moyenne de l'article en kilo-octets. • Nombre de disponibles GSIs. Examinez chaque indice indépendamment. • Taille moyenne d'un élément d'index • Combien de nouveaux produits seront ajoutés	Ingénieur de données

Tâche	Description	Compétences requises
	au tableau chaque mois ? Le nombre de nouveaux produits peut varier d'un mois à l'autre, mais vous pouvez supposer un taux de croissance moyen en fonction de vos analyses de rentabilisation. Cet exemple utilise en moyenne 10 millions de nouveaux produits par mois.	

Entrez les informations relatives à l'article et à l'objet dans le modèle Excel

Tâche	Description	Compétences requises
Téléchargez le modèle Excel depuis la section Pièces jointes et adaptez-le à votre tableau des cas d'utilisation.	1. Téléchargez le modèle Excel. 2. Ajustez le module commercial et GSIs, en fonction de la conception de votre table.	Ingénieur de données
Entrez les informations dans le modèle Excel.	1. Mettez à jour les informations de l'article dans la feuille. Mettez à jour les données uniquement dans les cellules oranges. 2. Ajustez les numéros d'objets : combien pourrait-on ajouter au tableau chaque mois ?	Ingénieur de données

Tâche	Description	Compétences requises
	3. Mettez à jour les prix du WRU et du RRU par million pour votre région AWS. 4. Mettez à jour les prix du stockage et de la sauvegarde par Go par mois pour votre région AWS. 5. Mettez à jour le prix de récupération par Go pour votre région AWS. Le modèle comporte trois éléments, ou entités : informations, métadonnées et relations. Il y en a deux GSIs. Pour votre cas d'utilisation, si vous avez besoin de plus d'éléments, créez de nouvelles lignes. Si vous en avez besoin de plus GSIs, copiez un bloc GSI existant et collez-le pour créer autant de blocs GSI que nécessaire. Ajustez ensuite les calculs des colonnes SUM et TOTAL.	

Ressources connexes

Références

- Tarification d'Amazon DynamoDB pour la capacité à la demande
- Calculateur de tarification AWS pour DynamoDB
- Bonnes pratiques de conception et d'architecture avec DynamoDB

- Mise en route avec DynamoDB

Guides et modèles

- Modélisation de données avec Amazon DynamoDB
- Estimation des coûts de stockage pour une table Amazon DynamoDB

Informations supplémentaires

Écrire un exemple de calcul des coûts

La conception du modèle de données DynamoDB indique trois éléments pour un produit et une taille moyenne de 4 Ko. Lorsque vous ajoutez un nouveau produit dans la table de base DynamoDB, il consomme le nombre d'éléments * (taille de l'article/unité d'écriture de 1 Ko) = 3 * (4/1) = 12 WRU. Dans cet exemple, pour écrire 1 Ko, le produit consomme 1 WRU.

Lire l'exemple de calcul des coûts

Pour obtenir l'estimation du RRU, considérez la moyenne du nombre de fois que chaque article sera lu par mois. Par exemple, l'élément d'information sera lu en moyenne 10 fois par mois, l'élément de métadonnées sera lu deux fois et l'élément de relation sera lu cinq fois. Dans le modèle d'exemple, le nombre total de RRU pour tous les composants = nombre de nouveaux composants créés chaque mois * RRU par composant et par mois = 10 millions * 17 RRU = 170 millions de RRU par mois.

Chaque mois, de nouveaux éléments (composants ou produits) seront ajoutés et le nombre total de produits augmentera au fil du temps. Ainsi, les exigences en matière de RRU augmenteront également au fil du temps.

- Pour le premier mois de RRU, la consommation sera de 170 millions.
- Pour le deuxième mois, la consommation de RRU sera de 2 * 170 millions = 340 millions.
- Pour le troisième mois, la consommation de RRU sera de 3* 170 millions = 510 millions.

Le graphique suivant montre la consommation mensuelle de RRU et les prévisions de coûts.

Notez que les prix indiqués dans le graphique ne sont fournis qu'à titre d'illustration. Pour créer des prévisions précises adaptées à votre cas d'utilisation, consultez la page de tarification d'AWS et utilisez ces prix dans la feuille Excel.

Exemples de calcul des coûts de stockage, de sauvegarde et de restauration

Le stockage, la sauvegarde et la restauration DynamoDB sont tous connectés les uns aux autres. La sauvegarde est directement liée au stockage, et la restauration est directement liée à la taille de la sauvegarde. À mesure que la taille de la table augmente, les coûts de stockage, de sauvegarde et de restauration correspondants augmentent proportionnellement.

Taille et coût du stockage

Le coût du stockage augmentera au fil du temps en fonction du taux de croissance de vos données. Supposons, par exemple, que la taille moyenne d'un composant ou d'un produit dans la table de base GSIs soit de 11 Ko et que 10 millions de nouveaux produits soient ajoutés chaque mois dans votre table de base de données. Dans ce cas, la taille de votre table DynamoDB augmentera (11 Ko x 10 millions) /1024/1024 = 105 Go par mois. Le premier mois, la taille de stockage de votre table sera de 105 Go, le deuxième mois, elle sera de 105 + 105 = 210 GBs, etc.

- Le premier mois, le coût du stockage sera de 105 Go* par Go pour votre région AWS.
- Le deuxième mois, le coût du stockage sera de 210 Go* par Go pour votre région.
- Pour le troisième mois, le coût du stockage sera de 315 Go* par Go pour votre région.

Pour connaître la taille et le coût du stockage pour les trois prochaines années, consultez la section Taille du stockage et prévisions.

Coût de sauvegarde

Les coûts de sauvegarde augmenteront au fil du temps en fonction du taux de croissance de vos données. Lorsque vous activez la sauvegarde continue avec point-in-time-recovery (PITR), les frais de sauvegarde continue sont basés sur le nombre moyen de Go de stockage par mois. Au cours d'un mois civil, la taille moyenne des sauvegardes serait identique à la taille de stockage de votre table, bien que la taille réelle puisse être légèrement différente. Comme de nouveaux produits seront ajoutés chaque mois, la taille totale du stockage et la taille de sauvegarde augmenteront au fil du temps. Par exemple, le premier mois, la taille de sauvegarde moyenne de 105 Go pourrait passer à 210 Go le deuxième mois.

- Le premier mois, le coût de sauvegarde sera de 105 Go par mois*, prix de sauvegarde continue par Go pour votre région AWS.
- Pour le deuxième mois, le coût de sauvegarde sera de 210 Go par mois* prix de sauvegarde continue par Go pour votre région.

- Pour le troisième mois, le coût de sauvegarde sera de 315 Go par mois* prix de sauvegarde continue par Go pour votre région.
- et ainsi de suite

Le coût de sauvegarde est inclus dans le graphique de la section Taille du stockage et prévisions des coûts.

Coûts de recouvrement

Lorsque vous effectuez une sauvegarde continue avec PITR activé, les frais d'opération de restauration sont basés sur la taille de la restauration. Chaque fois que vous effectuez une restauration, vous payez en fonction des gigaoctets de données restaurées. Si la taille de votre table est importante et que vous effectuez une restauration plusieurs fois par mois, cela sera coûteux.

Pour estimer le coût de restauration, cet exemple suppose que vous effectuez une restauration PITR une fois par mois à la fin du mois. L'exemple utilise la taille de sauvegarde moyenne mensuelle comme taille des données de restauration pour le mois en question. Pour le premier mois, la taille de sauvegarde moyenne est de 105 Go, et pour la restauration à la fin du mois, la taille des données de restauration serait de 105 Go. Pour le deuxième mois, ce serait 210 GBs, et ainsi de suite.

Le coût de restauration augmentera au fil du temps en fonction du taux de croissance de vos données.

- Pendant le premier mois, le coût de restauration sera de 105 Go* par Go pour votre région AWS.
- Pour le deuxième mois, le coût de restauration sera de 210 Go* le prix de restauration par Go pour votre région.
- Pour le troisième mois, le coût de restauration sera de 315 Go* par Go pour votre région.

Pour plus d'informations, consultez l'onglet Stockage, sauvegarde et restauration du modèle Excel et le graphique de la section suivante.

Taille du stockage et prévisions des coûts

Dans le modèle, la taille de stockage facturable réelle est calculée en soustrayant le niveau gratuit de 25 Go par mois pour la classe de table Standard. Dans la feuille, vous trouverez un graphique de prévision ventilé en valeurs mensuelles.

L'exemple de graphique suivant prévoit la taille de stockage mensuelle en Go, le coût de stockage facturable, le coût de sauvegarde à la demande et le coût de restauration pour les 36 prochains mois

civils. Tous les frais sont en dollars américains. Le graphique montre clairement que les coûts de stockage, de sauvegarde et de restauration augmentent proportionnellement à l'augmentation de la taille du stockage.

Notez que les prix utilisés dans le graphique sont fournis à titre d'illustration uniquement. Pour créer des prix précis adaptés à votre cas d'utilisation, consultez la page de tarification d'AWS et utilisez ces prix dans le modèle Excel.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Estimation des coûts de stockage pour une table Amazon DynamoDB

Créée par Moinul Al-Mamun (AWS)

Récapitulatif

Amazon DynamoDB est une base de données transactionnelle NoSQL qui fournit une latence à un chiffre en millisecondes, même à l'échelle du pétaoctet. Cette offre sans serveur populaire de AWS fournit des performances et une évolutivité constantes. Vous n'avez pas besoin de provisionner du stockage, et votre table unique peut atteindre des pétaoctets.

DynamoDB surveille la taille de votre table en permanence tout au long du mois afin de déterminer vos frais de stockage. AWS vous facture ensuite la taille moyenne du stockage en gigaoctets. Plus votre table s'agrandit au fil du temps, plus vos coûts de stockage augmenteront. Pour calculer le coût de stockage, vous pouvez utiliser le calculateur de AWS prix, mais vous devez indiquer la taille approximative de votre table, y compris les index secondaires globaux (GSIs), ce qui est très difficile à estimer au début du projet. De plus, le calculateur de AWS prix ne prend pas en compte le taux de croissance des données.

Ce modèle fournit un mécanisme et un modèle Microsoft Excel réutilisable pour calculer la taille et le coût du stockage DynamoDB. Il prend en compte les exigences de stockage de la table de base et de la table GSIs indépendante. Il calcule la taille du stockage en tenant compte de la taille de vos éléments individuels et du taux de croissance des données au fil du temps.

Pour obtenir une estimation, insérez deux informations dans le modèle :

- La taille de chaque élément en kilo-octets pour la table de base et GSIs
- Combien de nouveaux objets ou produits pourraient être ajoutés au tableau, en moyenne, par mois (par exemple, 10 millions)

Le modèle génère un graphique de prévision du stockage et des coûts pour les trois prochaines années, comme le montre l'exemple suivant.

Conditions préalables et limitations

Prérequis

- Connaissance de base de DynamoDB, notamment du stockage et de la tarification DynamoDB

- Connaissance de vos données, de votre modèle de données et de la taille des éléments dans DynamoDB
- Connaissance des index secondaires globaux DynamoDB () GSIs

Limites

- Le modèle fournit un calcul approximatif, mais il ne convient pas à toutes les configurations. Pour obtenir une estimation plus précise, vous devez mesurer la taille individuelle de chaque article dans le tableau de base et GSIs.
- Ce modèle permet d'estimer uniquement la taille et le coût du stockage pour les prochaines années sur la base d'hypothèses de croissance des données fixes.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.

Autres outils

- AWS Le calculateur de prix est un outil de planification en ligne que vous pouvez utiliser pour créer des estimations pour vos cas AWS d'utilisation.

Épopées

Extraire les informations relatives aux éléments de votre modèle de données DynamoDB

Tâche	Description	Compétences requises
Obtenez la taille de l'article.	1. Déterminez le nombre de types d'articles différents que vous allez stocker dans votre table. 2. Pour calculer la taille de chaque élément en kilo-octe	Ingénieur de données

Tâche	Description	Compétences requises
	ts, ajoutez la `Value` taille `Key` et la taille de chaque attribut. 3. Calculez la taille des éléments pour une table de base et pour chaque GSI.	
Obtenez le nombre d'objets ajoutés en un mois.	Estimez le nombre de composants ou d'objets qui seront ajoutés à la table DynamoDB, en moyenne, en un mois.	Ingénieur de données

Entrez les informations relatives à l'article et à l'objet dans le modèle Excel

Tâche	Description	Compétences requises
Téléchargez et ajustez la feuille de calcul Excel.	1. Téléchargez le modèle Excel à partir du document ci-joint. 2. Ajustez le module commercial et GSIs, en fonction de la conception de votre table.	Ingénieur de données
Entrez les informations dans le modèle Excel.	1. Mettez à jour les informations sur l'article dans la feuille. 2. Ajustez les numéros d'objets : combien pourrait-on ajouter au tableau chaque mois ?	Ingénieur de données

Tâche	Description	Compétences requises
	3. Mettez à jour le prix du stockage par Go par mois pour votre. Région AWS	

Ressources connexes

- Tarification de la capacité à la demande pour Amazon DynamoDB
- AWS Calculateur de prix pour DynamoDB

Informations supplémentaires

Notez que le modèle ci-joint prévoit uniquement la taille et le coût du stockage pour la classe de table de stockage standard. Sur la base des prévisions relatives aux coûts de stockage et en tenant compte de la taille de chaque article et du taux de croissance du produit ou de l'objet, vous pouvez estimer les éléments suivants :

- Coût d'exportation des données
- Coûts de sauvegarde et de restauration
- Exigences relatives au stockage des données.

Coût de stockage des données Amazon DynamoDB

DynamoDB surveille en permanence la taille de vos tables afin de déterminer vos frais de stockage. DynamoDB mesure la taille de vos données facturables en ajoutant la taille brute en octets de vos données plus une surcharge de stockage par article qui dépend des fonctionnalités que vous avez activées. Pour plus d'informations, consultez le Guide du développeur DynamoDB.

Le prix du stockage des données dépend de la classe de votre table. Les 25 premiers Go stockés chaque mois sont gratuits si vous utilisez la classe de table DynamoDB Standard. Pour plus d'informations sur les coûts de stockage pour les classes de tables Standard et Standard-Infrequent Access selon les différentes classes Régions AWS, consultez la section Tarification de la capacité à la demande.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Estimez la taille du moteur Amazon RDS pour une base de données Oracle à l'aide des rapports AWR

Créée par Abhishek Verma (AWS) et Eduardo Valentim (AWS)

Récapitulatif

Lorsque vous migrez une base de données Oracle vers Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora, le calcul du processeur, de la mémoire et des E/S de disque pour la base de données cible est une exigence essentielle. Vous pouvez estimer la capacité requise de la base de données cible en analysant les rapports Oracle Automatic Workload Repository (AWR). Ce modèle explique comment utiliser les rapports AWR pour estimer ces valeurs.

La base de données Oracle source peut être sur site ou hébergée sur une instance Amazon Elastic Compute Cloud (Amazon EC2), ou il peut s'agir d'une instance de base de données Amazon RDS for Oracle. La base de données cible peut être n'importe quelle base de données Amazon RDS ou Aurora.

> **Note**
>
> Les estimations de capacité seront plus précises si votre moteur de base de données cible est Oracle. Pour les autres bases de données Amazon RDS, la taille du moteur peut varier en raison des différences d'architecture de base de données.

Nous vous recommandons d'exécuter le test de performance avant de migrer votre base de données Oracle.

Conditions préalables et limitations

Prérequis

- Une licence Oracle Database Enterprise Edition et une licence Oracle Diagnostics Pack pour télécharger les rapports AWR.

Versions du produit

- Toutes les éditions d'Oracle Database pour les versions 11g (versions 11.2.0.3.v1 et ultérieures) et jusqu'à 12.2, et 18c,19c.

- Ce modèle ne couvre pas les systèmes Oracle Engineered ou Oracle Cloud Infrastructure (OCI).

Architecture

Pile technologique source

L'un des éléments suivants :

- Une base de données Oracle sur site
- Une base de données Oracle sur une EC2 instance
- Une instance de base de données Amazon RDS pour Oracle

Pile technologique cible

- Toute base de données Amazon RDS ou Amazon Aurora

Architecture cible

Pour plus d'informations sur le processus de migration complet, consultez le modèle Migrer une base de données Oracle vers Aurora PostgreSQL à l'aide d'AWS DMS et d'AWS SCT.

Automatisation et mise à l'échelle

Si vous avez plusieurs bases de données Oracle à migrer et que vous souhaitez utiliser des indicateurs de performance supplémentaires, vous pouvez automatiser le processus en suivant les étapes décrites dans le billet de blog Ajustement de la taille des instances Amazon RDS à grande échelle en fonction des indicateurs de performance Oracle.

Outils

- Oracle Automatic Workload Repository (AWR) est un référentiel intégré aux bases de données Oracle. Il collecte et stocke périodiquement les données relatives à l'activité du système et à la charge de travail, qui sont ensuite analysées par Automatic Database Diagnostic Monitor (ADDM). AWR prend régulièrement des instantanés des données de performance du système (par défaut, toutes les 60 minutes) et stocke les informations (par défaut, jusqu'à 8 jours). Vous pouvez utiliser les vues et les rapports AWR pour analyser ces données.

Bonnes pratiques

- Pour calculer les besoins en ressources de votre base de données cible, vous pouvez utiliser un seul rapport AWR, plusieurs rapports AWR ou des vues AWR dynamiques. Nous vous recommandons d'utiliser plusieurs rapports AWR pendant la période de pointe afin d'estimer les ressources nécessaires pour gérer ces pics de charge. En outre, les vues dynamiques fournissent davantage de points de données qui vous aident à calculer les besoins en ressources avec plus de précision.
- Vous devez estimer les IOPS uniquement pour la base de données que vous prévoyez de migrer, et non pour les autres bases de données et processus qui utilisent le disque.
- Pour calculer la quantité d'E/S utilisée par la base de données, n'utilisez pas les informations de la section Profil de charge du rapport AWR. Utilisez plutôt la section Profil d'E/S, si elle est disponible, ou passez directement à la section Statistiques d'activité de l'instance et examinez les valeurs totales des opérations physiques de lecture et d'écriture.
- Lorsque vous estimez l'utilisation du processeur, nous vous recommandons d'utiliser la méthode des métriques de base de données plutôt que les statistiques du système d'exploitation (OS), car elle est basée sur le processeur utilisé uniquement par les bases de données. (Les statistiques du système d'exploitation incluent également l'utilisation du processeur par d'autres processus.) Vous devez également consulter les recommandations relatives au processeur dans le rapport ADDM afin d'améliorer les performances après la migration.
- Tenez compte des limites de débit d'E/S (débit Amazon Elastic Block Store (Amazon EBS) et débit réseau) pour la taille spécifique de l'instance lorsque vous déterminez le type d'instance approprié.
- Exécutez le test de performance avant la migration pour valider la cylindrée du moteur.

Épopées

Création d'un rapport AWR

Tâche	Description	Compétences requises
Activez le rapport AWR.	Pour activer le rapport, suivez les instructions de la documentation Oracle.	DBA

Tâche	Description	Compétences requises
Vérifiez la durée de conservation.	Pour vérifier la durée de conservation du rapport AWR, utilisez la requête suivante. `SQL> SELECT snap_interval,retention FROM dba_hist_wr_control;`	DBA
Générez le cliché.	Si l'intervalle entre les instantanés AWR n'est pas suffisamment précis pour capturer le pic de charge de travail, vous pouvez générer le rapport AWR manuellement. Pour générer l'instantané AWR manuel, utilisez la requête suivante. `SQL> EXEC dbms_workload_repository.create_snapshot;`	DBA
Vérifiez les instantanés récents.	Pour vérifier les instantanés AWR récents, utilisez la requête suivante. `SQL> SELECT snap_id, to_char(begin_interval_time,'dd/MON/yy hh24:mi') Begin_Interval, to_char(end_interval_time,'dd/MON/yy hh24:mi') End_Interval FROM dba_hist_snapshot ORDER BY 1;`	DBA

Estimation des besoins en E/S sur disque

Tâche	Description	Compétences requises
Choisissez une méthode.	L'IOPS est la mesure standard des opérations d'entrée et de sortie par seconde sur un périphérique de stockage et inclut les opérations de lecture et d'écriture. Si vous migrez une base de données sur site vers AWS, vous devez déterminer le pic d'E/S disque utilisé par la base de données. Vous pouvez utiliser les méthodes suivantes pour estimer les E/S de disque pour votre base de données cible : • Section « Profil de charge » du rapport AWR • Section des statistiques d'activité de l'instance du rapport AWR (utilisez cette section pour Oracle Database 12c ou version ultérieure) • Section du profil d'E/S du rapport AWR (utilisez cette section pour les versions de base de données Oracle antérieures à 12c) • Vues AWR	DBA

Tâche	Description	Compétences requises
	Les étapes suivantes décrivent ces quatre méthodes.	

Tâche	Description	Compétences requises
Option 1 : utilisez le profil de charge.	Le tableau suivant montre un exemple de la section Profil de charge du rapport AWR. **Important** Pour des informations plus précises, nous vous recommandons d'utiliser l'option 2 (profils d'E/S) ou l'option 3 (statistiques d'activité de l'instance) au lieu du profil de charge. Par seco / Par trans on / Par Exec / Par appel Heur (s) de base de donn 26,6 0.2 0,00 0,02 Proc r (s) de base 18,0 0.1 0,00 0,01	DBA

Tâche	Description	Compétences requises
	de donn Proc r (s) d'arri - plan 0.2 0.0 0,00 0,00 Taille de rétab emer (octe 2 458 539,9 17 097,5 Lectu logiq (bloc 3 371 931,5 23 449,6 Bloq les modi ions 21 643,5 150,5 Lectu phys (bloc 13 575,1 94,4 Écrit phys (bloc 3 467,3 24.1 Lisez les dema 3 586,8 24,9	

Tâche	Description	Compétences requises
	d'E/S : Rédi des dema d'E/S : Lire l'IO (Mo) Écrir IO (Mo) Ligne de num ion par mess e insta ée : Mess e insta ée de lectu logiq de sess 574, 106, 27.1 0.0 4.0 0.7 0.2 0.0	

Tâche	Description	Compétences requises
	Appe de l'utilis teur : 1 245,7 8,7 Anal (SQL 4 626,2 32,2 Anal appr ies (SQL 8,9 0.1 Zone de trava SQL (Mo) 824,9 5.7 Conn s : 1,7 0.0 Exéc (SQL 136 656,5 950,4 Annu ns : 22,9 0.2 Tran ons : 143,8 Sur la base de ces informations, vous pouvez calculer IOPs le débit comme suit :	

Tâche	Description	Compétences requises
	IOPS = demandes d'E/S de lecture : + Demandes d'E/S d'écriture = 3 586,8 + 574,7 = 4134,5 Débit = lecture physique (blocs) + écriture physique (blocs) = 13 575,1 + 3 467,3 = 17 042,4 La taille des blocs dans Oracle étant de 8 Ko, vous pouvez calculer le débit total comme suit : Le débit total en Mo est de 17042,4 * 8 * 1024/1024/1024 = 133,2 Mo **Warning** N'utilisez pas le profil de charge pour estimer la taille de l'instance. Ce n'est pas aussi précis que les statistiques d'activité des instances ou les profils d'E/S.	

Tâche	Description	Compétences requises
Option 2 : utiliser les statistiques d'activité de l'instance.	Si vous utilisez une version d'Oracle Database antérieure à 12c, vous pouvez utiliser la section Instance Activity Stats du rapport AWR pour estimer les IOPS et le débit. Le tableau suivant présente un exemple de cette section. Statistique / Total / par seconde / par Trans nombre total de demandes d'E/S en lecture physiq / 2 547 333 217 / 3 610,28 / 25,11 nombre total d'octets de lecture physiq / 80 776 296 124 928 / 114 482 426,26 / 796 149,98 nombre total de demandes d'E/S en / 534 198 208 / 757,11 / 5,27	DBA

Tâche	Description	Compétences requises
	écritur physiq nombr 25 36 251 total 517 165 508,18 d'octet 678 631,84 en 849 écritur 024 physiq Sur la base de ces informations, vous pouvez calculer le total des IOPS et le débit comme suit : Nombre total d'IOPS = 3 610,28 + 757,11 = 4 367 Mbits/s totaux = 114 482 426,26 + 36 165 631,84 = 150648058,1/1024/1024 = 143 Mbits/s	

Tâche	Description	Compétences requises
Option 3 : utiliser des profils d'E/S.	Dans Oracle Database 12c, le rapport AWR inclut une section Profils d'E/S qui présente toutes les informations dans un seul tableau et fournit des données plus précises sur les performances de la base de données. Le tableau suivant présente un exemple de cette section. Lectur +é criture par secon Nombr total de demar 4 367,4 3 610,3 757,1 Demar de base de donné 4 161,5 3 586,8 574,7 Demar optimis s : 0.0 0.0 0.0 Demar de 179,3 2,8 176,6	DBA

Tâche	Description	Compétences requises
	rétabli ement Total (Mo) : 143,7 109,2 34,5 Base de donné (MB) : 133,1 106,1 27.1 Total optimi (Mo) : 0.0 0.0 0.0 Rétabl (Mo) : 7.6 2.7 4,9 Base de donné (blocs) 17 042,4 13 575,1 3 467,3 Via le cache tampo (blocs) 5 898,5 5 360,9 537,6 Direct (blocs) 11 143,9 8 214,2 2 929,7 Ce tableau fournit les valeurs suivantes pour le débit et le total des IOPS :	

Tâche	Description	Compétences requises
	Débit = 143 Mbits/s (à partir de la cinquième ligne, intitulée Total, deuxième colonne) IOPS = 4 367,4 (à partir de la première ligne, intitulée Total des demandes, deuxième colonne)	

Option 4 : Utiliser les vues AWR.	Vous pouvez voir les mêmes informations d'IOPS et de débit en utilisant les vues AWR. Pour obtenir ces informations, utilisez la requête suivante :
	
	`break on report`
	`compute sum of Value on report`
	`select METRIC_NAME,avg(AVERAGE) as "Value"`
	`from dba_hist_sysmetric_summary`
	`where METRIC_NAME in ('Physical Read Total IO Requests Per Sec','Physical Write Total IO Requests Per Sec')`
	`group by metric_name;`
		DBA

Estimation des besoins en CPU

Tâche	Description	Compétences requises
Choisissez une méthode.	Vous pouvez estimer le processeur requis pour la base de données cible de trois manières : • En utilisant les cœurs réellement disponibles du processeur • En utilisant les cœurs utilisés en fonction des statistiques du système d'exploitation • En utilisant les cœurs utilisés sur la base des statistiques de la base de données Si vous examinez les cœurs utilisés, nous vous recommandons d'utiliser la méthode des métriques de base de données plutôt que des statistiques du système d'exploitation, car elle est basée sur le processeur utilisé uniquement par les bases de données que vous envisagez de migrer. (Les statistiques du système d'exploitation incluent également l'utilisation du processeur par d'autres processus	DBA

Tâche	Description	Compétences requises
	.) Vous devez également consulter les recommandations relatives au processeur dans le rapport ADDM afin d'améliorer les performances après la migration. Vous pouvez également estimer les besoins en fonction de la génération de processeurs. Si vous utilisez différentes générations de processeurs, vous pouvez estimer le processeur requis pour la base de données cible en suivant les instructions du livre blanc Démystifier le nombre de v CPUs pour des performances de charge de travail optimales.	

Tâche	Description	Compétences requises

Option 1 : Estimer les besoins en fonction des noyaux disponibles.	Dans les rapports de l'AWR :
	• CPUs font référence à logique et virtuel CPUs.
	• Les cœurs sont le nombre de processeurs contenus dans un chipset de processeur physique.
	• Un socket est un appareil physique qui connecte une puce à une carte. Les processeurs multicœurs ont des sockets avec plusieurs cœurs de processeur.
	
	Vous pouvez estimer les noyaux disponibles de deux manières :
	• En utilisant les commandes du système d'exploitation
	• En utilisant le rapport AWR
	
	Pour estimer les cœurs disponibles à l'aide des commandes du système d'exploitation
	
	Utilisez la commande suivante pour compter les cœurs du processeur.
	`$ cat /proc/cpuinfo | grep "cpu cores"|uniq`
	`cpu cores : 4`
		DBA

Tâche	Description	Compétences requises

	`cat /proc/cpuinfo | egrep "core id|physical id" | tr -d "\n" | sed s/physical/\\nphysical/g | grep -v ^$ | sort | uniq | wc -l`
	
	Utilisez la commande suivante pour compter les sockets du processeur.
	
	`grep "physical id" /proc/cpuinfo | sort -u`
	`physical id : 0`
	`physical id : 1`
	
	Note
	Nous ne recommandons pas d'utiliser les commandes du système d'exploitation telles que nmon et sar pour extraire l'utilisation du processeur. Cela est dû au fait que ces calculs incluent l'utilisation du processeur par d'autres processus et peuvent ne pas refléter le processeur réel utilisé par la base de données.	

Tâche	Description	Compétences requises
	Pour estimer les cœurs disponibles à l'aide du rapport AWR Vous pouvez également déduire l'utilisation du processeur à partir de la première section du rapport AWR. Voici un extrait du rapport. D ID Inst Insé Heu Vers RA N de un de bas num dém de don X <DE XX) 1 05 12.1 NO sep 0 20 à 23:(Nor Plat CPU Noy Dou Mém d'hó e (Go) <ho Linu 80 80 2 441,7 e> x86 64 bits Dans cet exemple, le CPUs nombre est de 80, ce qui indique qu'ils sont logiques (virtuels) CPUs. Vous pouvez	

Tâche	Description	Compétences requises
	également constater que cette configuration comporte deux sockets, un processeur physique sur chaque socket (pour un total de deux processeurs physiques) et 40 cœurs pour chaque processeur physique ou socket.	

Tâche	Description	Compétences requises
Option 2 : Estimez l'utilisation du processeur à l'aide des statistiques du système d'exploitation.	Vous pouvez vérifier les statistiques d'utilisation du processeur du système d'exploitation soit directement dans le système d'exploitation (à l'aide de sar ou d'un autre utilitaire du système d'exploitation hôte), soit en consultant les valeurs IDLE/(IDLE+BUSY) de la section Statistiques du système d'exploitation du rapport AWR. Vous pouvez voir les secondes de processeur consommées directement depuis v$osstat. Les rapports AWR et Statspack présentent également ces données dans la section Statistiques du système d'exploitation. Si plusieurs bases de données se trouvent sur la même boîte, elles ont toutes les mêmes valeurs v$osstat pour BUSY_TIME. Statistique / Valeur / Valeur finale OCTETS DE MÉMOIR GRATUI / 6 810 677 248 / 12 280 799 232	DBA

Tâche	Description		Compétences requises
	OCTETS 175 160 DE 627 380 MÉMOIF 333 653 INACTIF 632 568 SWAP_F 17 145 17 145 _BYTES 614 872 336 384 PÉRIOD 1 305 OCCUPE 569 937 HEURE 4 312 D'INACT 718 ITÉ 839 HEURE 53 417 D'ATTEN 174 DE L'IOWA NICE_TI 29 815 SYS_TIM 148 567 570 HEURE 1 146 DE 918 L'UTILIS 783 TEUR CHARGE 25 29 VM EN 593 OCTETS 920	

Tâche	Description		Compétences requises
	VM_OUT TES	327 680	
	MEMOIR CTETS_I SIQUE	474 362 417 152	
	NUM_PR SSEURS	80	
	NOMBRI DE CPU_CC	80	
	NUM CPU SOCKET	2	
	TAILLE MAXIMA DE LA RÉCEPT GLOBAL	4 194 304	
	TAILLE MAXIMA DE L'ENVOI GLOBAL	2 097 152	
	TCP_RE VE_SIZE EFAULT	87 380	

Tâche	Description	Compétences requises
	TCP_RE 6 291 VE_SIZE 456 AX TAILLE 4 096 DE RÉCEPT TCP_MI TCP_SE 16 384 SIZE_DE ULT TCP_SE 4 194 SIZE_MA 304 TCP_SE 4 096 SIZE_MI S'il n'y a aucun autre consommateur important de CPU dans le système, utilisez la formule suivante pour calculer le pourcentage d'utilisation du processeur : Utilisation = Temps de charge/ Temps total Temps de pointe = exigences = V$OSSTAT.BUSY_TIME C = Durée totale (occupé et inactif)	

Tâche	Description	Compétences requises
	C = capacité = V$OSTAT.BUSY_TIME + V$OSTAT.IDLE_TIME Utilisation = BUSY_TIME/(BUSY_TIME + IDLE_TIME) = -1 305 569 937/(1 305 569 937 + 4 312 718 839) = 23 % utilisés	

Tâche	Description	Compétences requises
Option 3 : Estimez l'utilisation du processeur à l'aide des métriques de base de données.	Si plusieurs bases de données sont en cours d'exécution dans le système, vous pouvez utiliser les métriques de base de données qui apparaissent au début du rapport. Snap ID / Snap Time / Sess / Curse Sessic Com Snap 1846 28 sept. 20 h 00 : 42 1226 35,8 Fin du snap 1854 6 octob 2020 13:0(1876 41,1 Écha 11 759,((minu Heur de base de donn 312 625,4 (minu Pour obtenir des mesures d'utilisation du processeur, utilisez cette formule :	DBA

Tâche	Description	Compétences requises
	Utilisation du processeur de la base de données (% de la puissance CPU disponible) = temps CPU/NUM_CPUS/ temps écoulé où l'utilisation du processeur est décrite par le temps du processeur et représente le temps passé sur le processeur, et non le temps d'attente du processeur. Ce calcul aboutit à : = 312,625,40/11,759,64/80 = 33 % du processeur est utilisé Nombre de cœurs (33 %) * 80 = 26,4 cœurs Nombre total de cœurs = 26,4 * (120 %) = 31,68 cœurs Vous pouvez utiliser la plus élevée de ces deux valeurs pour calculer l'utilisation du processeur de l'instance de base de données Amazon RDS ou Aurora. **Note** Sur IBM AIX, l'utilisation calculée ne correspond pas aux valeurs du système d'exploitation ou de	

Tâche	Description	Compétences requises
	la base de données. Ces valeurs sont identiques sur les autres systèmes d'exploitation.	

Estimation des besoins en mémoire

Tâche	Description	Compétences requises
Estimez les besoins en mémoire à l'aide des statistiq ues de mémoire.	Vous pouvez utiliser le rapport AWR pour calculer la mémoire de la base de données source et la faire correspondre à celle de la base de données cible. Vous devez également vérifier les performances de la base de données existante et réduire vos besoins en mémoire pour réduire les coûts, ou augmenter vos besoins pour améliorer les performances. Cela nécessite une analyse détaillée du temps de réponse de l'AWR et du contrat de niveau de service (SLA) de l'applica tion. Utilisez la somme de l'utilisation de la zone globale du système Oracle (SGA) et de la zone globale du programme (PGA) comme estimation de l'utilisation de la mémoire pour Oracle.	DBA

Tâche	Description	Compétences requises
	Ajoutez 20 % supplémentaires pour que le système d'exploit ation détermine une taille de mémoire cible requise. Pour Oracle RAC, utilisez la somme de l'utilisation de mémoire estimée sur tous les nœuds RAC et réduisez la mémoire totale, car elle est stockée sur des blocs communs. 1. Vérifiez les indicateurs dans le tableau des pourcenta ges d'efficacité de l'instanc e. Le tableau utilise les termes suivants : • Le pourcentage d'impact sur la mémoire tampon est le pourcentage de fois où un bloc particulier a été trouvé dans le cache de la mémoire tampon au lieu d'effectuer une E/S physique. Pour de meilleures performances, visez 100 %. • La valeur de la mémoire tampon Nowait % doit être proche de 100 %. • Le pourcentage de Latch Hit doit être proche de 100 %. • Le pourcentage de processeur non analysabl	

Tâche	Description	Compétences requises
	e est le pourcentage du temps processeur consacré à des activités autres que l'analyse syntaxique. Cette valeur doit être proche de 100 %. Pourcentages d'efficacité des instances (objectif 100 %) Tamp 99,99 Rétab 100,00 Nowa NoWa % : % d'imp sur la mémc tampc 99,84 % de tri en mémc 100,00 % d'acc à la bibliot que : 748,7 Analy logicie e % : 99,81 Exécu pour analy 96,61 % de clics sur le verrou 100,00	

Tâche	Description	Compétences requises

Analy le proce r pour analy: Elaps	72,73	% Proce r non analy:	99,21
% d'acc au cache Flash	0,00		

Dans cet exemple, toutes les métriques semblent correctes. Vous pouvez donc utiliser le SGA et le PGA pour la base de données existante comme exigence de planification des capacités.

2. Consultez la section des statistiques de mémoire et calculez le SGA/PGA.

	Comme	Fin
Mémoire hôte (Mo) :	452 387,3	452 387,3
Utilisation du	220 544,0	220 544,0

Tâche	Description	Compétences requises
	SGA (Mo) :	
	Utilisation du PGA (Mo) : 36 874,9 45 270,0	
	Mémoire d'instance totale utilisée = SGA + PGA = 220 Go + 45 Go = 265 Go Ajoutez 20 % de mémoire tampon : Mémoire d'instance totale = 1,2 * 265 Go = 318 Go Étant donné que les cartes SGA et PGA représentent 70 % de la mémoire de l'hôte, la quantité totale de mémoire requise est la suivante : Mémoire hôte totale = 318/0,7 = 464 Go **Note** Lorsque vous migrez vers Amazon RDS for Oracle, le PGA et le SGA sont précalculés sur la base d'une formule prédéfinie. Assurez-vous que les	

Tâche	Description	Compétences requises
	valeurs précalculées sont proches de vos estimations.	

Déterminer le type d'instance de base de données de la base de données cible

Tâche	Description	Compétences requises
Déterminez le type d'instance de base de données en fonction des estimations des E/S de disque, du processeur et de la mémoire.	Sur la base des estimations des étapes précédentes, la capacité de la base de données Amazon RDS ou Aurora cible doit être la suivante : • 68 cœurs de processeur • Débit de 143 Mbits/s • 4367 IOPS pour les E/S de disque • 464 Go de mémoire Dans la base de données Amazon RDS ou Aurora cible, vous pouvez mapper ces valeurs au type d'instance db.r5.16xlarge, qui a une capacité de 32 cœurs, 512 Go de RAM et un débit de 13 600 Mbit/s. Pour plus d'informations, consultez le billet de blog AWS Right size Amazon RDS instances	DBA

Tâche	Description	Compétences requises
	at scale based on Oracle performance metrics.	

Ressources connexes

- Classe d'instance de base de données Aurora (documentation Amazon Aurora)
- Stockage d'instances de base de données Amazon RDS (documentation Amazon RDS)
- Outil AWS Miner (GitHub référentiel)

Exportez les tables Amazon RDS for SQL Server vers un compartiment S3 à l'aide d'AWS DMS

Créée par Subhani Shaik (AWS)

Récapitulatif

Amazon Relational Database Service (Amazon RDS) pour SQL Server ne prend pas en charge le chargement de données sur d'autres serveurs liés à un moteur de base de données sur le cloud Amazon Web Services (AWS). Vous pouvez plutôt utiliser AWS Database Migration Service (AWS DMS) pour exporter les tables Amazon RDS for SQL Server vers un bucket Amazon Simple Storage Service (Amazon S3), où les données sont disponibles pour d'autres moteurs de base de données.

AWS DMS vous aide à migrer des bases de données vers AWS rapidement et en toute sécurité. La base de données source reste pleinement opérationnelle pendant la migration, minimisant ainsi les interruptions de service pour les applications qui dépendent de la base de données. AWS DMS peut migrer vos données vers et depuis les bases de données commerciales et open source les plus utilisées.

Ce modèle utilise AWS Secrets Manager lors de la configuration des points de terminaison AWS DMS. Secrets Manager vous aide à protéger les secrets nécessaires pour accéder à vos applications, services et ressources informatiques. Vous pouvez utiliser le service pour alterner, gérer et récupérer les informations d'identification de base de données, les clés d'API et d'autres secrets tout au long de leur cycle de vie. Les utilisateurs et les applications récupèrent les secrets en appelant Secrets Manager, ce qui réduit le besoin de coder en dur les informations sensibles. Secrets Manager propose une rotation secrète avec intégration intégrée à Amazon RDS, Amazon Redshift et Amazon DocumentDB. En outre, le service est extensible à d'autres types de secrets, notamment les clés d'API et les OAuth jetons. Avec Secrets Manager, vous pouvez contrôler l'accès aux secrets en utilisant des autorisations précises et en contrôlant la rotation des secrets de manière centralisée pour les ressources du cloud AWS, des services tiers et sur site.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Compartiment S3
- Un cloud privé virtuel (VPC)

- Un sous-réseau de base de données
- Amazon RDS for SQL Server
- Rôle AWS Identity and Access Management (IAM) avec accès (objets list, get et put) au compartiment S3 pour le compte de l'instance Amazon RDS.
- Secrets Manager pour stocker les informations d'identification de l'instance RDS.

Architecture

Pile technologique

- Amazon RDS for SQL Server
- AWS DMS
- Amazon S3
- AWS Secrets Manager

Architecture cible

Le schéma suivant montre l'architecture permettant d'importer des données depuis l'instance Amazon RDS vers le compartiment S3 à l'aide d'AWS DMS.

1. La tâche de migration AWS DMS se connectant à l'instance Amazon RDS source via le point de terminaison source
2. Copier des données depuis l'instance Amazon RDS source
3. La tâche de migration AWS DMS se connectant au compartiment S3 cible via le point de terminaison cible
4. Exportation des données copiées vers le compartiment S3 au format CSV (valeurs séparées par des virgules)

Outils

Services AWS

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.

Autres services

- Microsoft SQL Server Management Studio (SSMS) est un outil de gestion de SQL Server, y compris l'accès, la configuration et l'administration des composants de SQL Server.

Épopées

Configuration de l'instance Amazon RDS for SQL Server

Tâche	Description	Compétences requises
Créez l'instance Amazon RDS for SQL Server.	1. Ouvrez la console de gestion AWS, choisissez RDS et utilisez l'option de création standard pour créer une instance Amazon RDS avec l'édition requise, telle que SQL Server Express Edition, SQL Server Standard Edition ou SQL Server Enterprise Edition. Pour la version, choisissez 2016 ou version ultérieure.	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	2. Sous Modèles, sélectionnez Dev/Test.	
Configurez les informations d'identification pour l'instance.	1. Entrez un nom pour l'instance. 2. Entrez un nom d'utilisateur et un mot de passe pour l'instance Amazon RDS.	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
Configurez la classe d'instance, le stockage, le dimensionnement automatique et la disponibilité.	1. Sélectionnez la classe d'instance de base de données dans la liste : classes Standard, Memory Optimized et Burstable. Choisissez le type d'instance de base de données qui alloue la capacité de calcul, de réseau et de mémoire requise par les charges de travail planifiées pour cette instance de base de données. Pour plus d'informations, consultez la documentation AWS. 2. Sélectionnez le type de stockage dans la liste : SSD à usage général, SSD IOPS provisionné ou magnétique. Allouez la taille de stockage par défaut selon les besoins. 3. Choisissez Activer le dimensionnement automatique du stockage pour augmenter le stockage Amazon RDS en fonction de votre planification des capacités. 4. Un déploiement multi-AZ avec une instance de réplication est pris en charge par AWS DMS. En cas de panne de la zone	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	de disponibilité, du matériel interne ou du réseau, AWS DMS créera une instance de secours et fournira une haute disponibilité (HA) par le biais d'un basculement automatique vers les répliques de secours. En fonction de la taille de votre importation, sélectionnez l'option appropriée.	
Spécifiez le VPC, le groupe de sous-réseaux, l'accès public et le groupe de sécurité.	Sélectionnez le VPC, les groupes de sous-réseaux de base de données et le groupe de sécurité VPC selon les besoins pour créer l'instance Amazon RDS. Suivez les meilleures pratiques, par exemple : • N'activez pas l'accès public à l'instance de base de données RDS. • N'utilisez pas le CIDR 0.0.0.0/0 dans les groupes de sécurité. • Utilisez uniquement l'adresse IP et les détails du port requis pour accéder à l'instance RDS.	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
Configurez la surveillance, la sauvegarde et la maintenance.	1. Spécifiez les options de sauvegarde souhaitées. Par défaut, les sauvegard es automatisées sont activées avec une période de conservation de 7 jours. 2. Choisissez les paramètre s de fenêtre de mise à niveau automatique et de maintenance appropriés pour appliquer les modificat ions ou les opérations de maintenance en attente à la base de données par Amazon RDS. 3. Choisissez Créer une base de données.	DBA, ingénieur DevOps

Configuration de la base de données et exemples de données

Tâche	Description	Compétences requises
Créez une table et chargez les données d'exemple.	Dans la nouvelle base de données, créez une table. Utilisez l'exemple de code de la section Informations supplémentaires pour charger des données dans le tableau.	DBA, ingénieur DevOps

Configurer les informations d'identification

Tâche	Description	Compétences requises
Créez le secret.	1. Sur la console, choisissez Secrets Manager, puis Stocker un nouveau secret. 2. Entrez un nom d'utilisateur et un mot de passe pour la base de données Amazon RDS for SQL Server. Ce secret sera utilisé pour le point de terminaison source AWS DMS.	DBA, ingénieur DevOps

Configurer l'accès entre la base de données et le compartiment S3

Tâche	Description	Compétences requises
Créez un rôle IAM pour accéder à Amazon RDS.	1. Sur la console, choisissez IAM et créez un rôle IAM qui donne à un compartiment S3 un accès en lecture/écriture à Amazon RDS. 2. Sous Fonctionnalité, sélectionnez Intégration S3.	DBA, ingénieur DevOps

Création du compartiment S3

Tâche	Description	Compétences requises
Créez le compartiment S3.	Pour enregistrer les données depuis Amazon RDS for SQL Server, sur la console,	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	choisissez S3, puis Create bucket. Assurez-vous que le compartiment S3 n'est pas accessible au public.	

Configurer l'accès entre AWS DMS et le compartiment S3

Tâche	Description	Compétences requises
Créez un rôle IAM pour qu'AWS DMS accède à Amazon S3.	Créez un rôle IAM qui permet à AWS DMS de répertorier, d'obtenir et de placer des objets depuis le compartiment S3.	DBA, ingénieur DevOps

Configuration d'AWS DMS

Tâche	Description	Compétences requises
Créez le point de terminaison source AWS DMS.	1. Sur la console, choisisse z Database Migration Service, puis Endpoints. Créez le point de terminais on source en cochant la case Sélectionner une instance de base de données RDS. 2. Pour le moteur source, sélectionnez Microsoft SQL Server. 3. Sous Accès à la base de données des terminaux, choisissez AWS Secrets	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	Manager, puis entrez le secret et le rôle IAM que vous avez créés précédemment, ainsi que le nom de la base de données. 4. Testez le point de terminaison source.	
Créez le point de terminaison cible AWS DMS.	Créez le point de terminaison cible en sélectionnant Amazon S3 comme moteur cible. Indiquez le nom du compartiment S3 et le nom du dossier pour le rôle IAM que vous avez créé précédemment.	DBA, ingénieur DevOps
Créez l'instance de réplication AWS DMS.	Dans le même VPC, le même sous-réseau et le même groupe de sécurité, créez l'instance de réplication AWS DMS. Pour plus d'informations sur le choix d'une classe d'instance, consultez la documentation AWS.	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
Créez la tâche de migration AWS DMS.	Pour exporter les données d'Amazon RDS for SQL Server vers le compartiment S3, créez une tâche de migration de base de données. Pour le type de migration, choisissez Migrer les données existantes. Sélectionnez les points de terminaison et l'instance de réplication AWS DMS que vous avez créés.	DBA, ingénieur DevOps

Exportez les données vers le compartiment S3

Tâche	Description	Compétences requises
Exécutez la tâche de migration de base de données.	Pour exporter les données de la table SQL Server, lancez la tâche de migration de base de données. La tâche exportera les données d'Amazon RDS for SQL Server vers le compartiment S3 au format CSV.	DBA, ingénieur DevOps

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez les ressources.	Pour éviter des coûts supplémentaires, utilisez la console pour supprimer	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	les ressources dans l'ordre suivant : 1. Tâche de migration 2. Instance de réplication 3. Points de terminaison 4. Compartiment S3 5. Instance de base de données	

Ressources connexes

- AWS DMS
- Amazon S3
- Amazon RDS for SQL Server
- Intégration avec Amazon S3

Informations supplémentaires

Pour créer la base de données et la table, et pour charger les données d'exemple, utilisez le code suivant.

```
--Step1: Database creation in RDS SQL Server
CREATE DATABASE [Test_DB]
 ON  PRIMARY
( NAME = N'Test_DB', FILENAME = N'D:\rdsdbdata\DATA\Test_DB.mdf' , SIZE = 5120KB ,
 FILEGROWTH = 10%)
 LOG ON
( NAME = N'Test_DB_log', FILENAME = N'D:\rdsdbdata\DATA\Test_DB_log.ldf' , SIZE =
 1024KB , FILEGROWTH = 10%)
GO

--Step2: Create Table
USE Test_DB
GO
Create Table Test_Table(ID int, Company Varchar(30), Location Varchar(20))
```

```
--Step3: Load sample data.
USE Test_DB
GO
Insert into Test_Table values(1,'AnyCompany','India')
Insert into Test_Table values(2,'AnyCompany','USA')
Insert into Test_Table values(3,'AnyCompany','UK')
Insert into Test_Table values(4,'AnyCompany','Hyderabad')
Insert into Test_Table values(5,'AnyCompany','Banglore')
```

Gérer les blocs anonymes dans les instructions Dynamic SQL dans Aurora PostgreSQL

Créée par anuradha chintha (AWS)

Récapitulatif

Ce modèle vous montre comment éviter l'erreur que vous obtenez lors de la gestion de blocs anonymes dans des instructions Dynamic SQL. Vous recevez un message d'erreur lorsque vous utilisez l'outil AWS Schema Conversion Tool pour convertir une base de données Oracle en une base de données Aurora PostgreSQL Edition compatible. Pour éviter cette erreur, vous devez connaître la valeur d'une variable de 0UT liaison, mais vous ne pouvez connaître la valeur d'une variable de 0UT liaison qu'après avoir exécuté l'instruction SQL. L'erreur est due au fait que l'AWS Schema Conversion Tool (AWS SCT) ne comprend pas la logique contenue dans l'instruction Dynamic SQL. AWS SCT ne peut pas convertir l'instruction SQL dynamique en code PL/SQL (c'est-à-dire en fonctions, procédures et packages).

Conditions préalables et limitations

Prérequis

- Compte AWS actif
- Instance de base de données (DB) Aurora PostgreSQL
- Amazon Relational Database Service (Amazon RDS) pour instance de base de données Oracle
- Terminal interactif PostgreSQL (psql)
- SQL *Plus
- `AWS_ORACLE_EXT`schéma (inclus dans le pack d'extension AWS SCT) dans votre base de données cible
- Dernière version d'AWS Schema Conversion Tool (AWS SCT) et ses pilotes requis

Architecture

Pile technologique source

- Base de données Oracle 10g et version ultérieure sur site

Pile technologique cible

- Amazon Aurora PostgreSQL
- Amazon RDS for PostgreSQL
- Outil de conversion de schéma AWS (AWS SCT)

Architecture de migration

Le schéma suivant montre comment utiliser les variables de 0UT liaison AWS SCT et Oracle pour scanner le code de votre application à la recherche d'instructions SQL intégrées et convertir le code dans un format compatible utilisable par une base de données Aurora.

Le schéma suivant illustre le flux de travail suivant :

1. Générez un rapport AWS SCT pour la base de données source en utilisant Aurora PostgreSQL comme base de données cible.
2. Identifiez le bloc anonyme dans le bloc de code SQL dynamique (pour lequel AWS SCT a généré l'erreur).
3. Convertissez le bloc de code manuellement et déployez le code sur une base de données cible.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.
- AWS Schema Conversion Tool (AWS SCT) vous aide à rendre les migrations de bases de données hétérogènes prévisibles en convertissant automatiquement le schéma de base de données source et la majorité des objets du code de base de données dans un format compatible avec la base de données cible.

Autres outils

- pgAdmin vous permet de vous connecter à votre serveur de base de données et d'interagir avec celui-ci.
- Oracle SQL Developer est un environnement de développement intégré que vous pouvez utiliser pour développer et gérer des bases de données dans Oracle Database. Vous pouvez utiliser SQL *Plus ou Oracle SQL Developer pour ce modèle.

Épopées

Configuration de la base de données source Oracle

Tâche	Description	Compétences requises
Créez une instance Oracle sur Amazon RDS ou Amazon EC2.	Pour créer une instance de base de données Oracle sur Amazon RDS, consultez la section Création d'une instance de base de données Oracle et connexion à une base de données sur une instance de base de données Oracle dans la documentation Amazon RDS. Pour créer une instance de base de données Oracle sur Amazon Elastic Compute Cloud (Amazon EC2), consultez Amazon EC2 for Oracle dans la documentation AWS Prescriptive Guidance.	DBA
Créez un schéma de base de données et des objets pour la migration.	Vous pouvez utiliser Amazon Cloud Directory pour créer un schéma de base de données. Pour plus d'informations, consultez la section Create a	DBA

Tâche	Description	Compétences requises
	Schema dans la documentation Cloud Directory.	
Configurez les groupes de sécurité entrants et sortants.	Pour créer et configurer des groupes de sécurité, consultez la section Contrôle de l'accès à l'aide de groupes de sécurité dans la documentation Amazon RDS.	DBA
Vérifiez que la base de données est en cours d'exécution.	Pour vérifier l'état de votre base de données, consultez la section Affichage des événements Amazon RDS dans la documentation Amazon RDS.	DBA

Configuration de la base de données Aurora PostgreSQL cible

Tâche	Description	Compétences requises
Créez une instance Aurora PostgreSQL dans Amazon RDS.	Pour créer une instance Aurora PostgreSQL, consultez la section Création d'un cluster de base de données et connexion à une base de données sur un cluster de base de données Aurora PostgreSQL dans la documentation Amazon RDS.	DBA
Configurez un groupe de sécurité entrant et sortant.	Pour créer et configurer des groupes de sécurité, consultez la section Fournir un accès au cluster de base de données	DBA

Tâche	Description	Compétences requises
	dans le VPC en créant un groupe de sécurité dans la documentation Aurora.	
Vérifiez que la base de données Aurora PostgreSQL est en cours d'exécution.	Pour vérifier l'état de votre base de données, consultez la section Affichage des événements Amazon RDS dans la documentation Aurora.	DBA

Configuration d'AWS SCT

Tâche	Description	Compétences requises
Connectez AWS SCT à la base de données source.	Pour connecter AWS SCT à votre base de données source, consultez la section Connexion à PostgreSQL en tant que source dans la documentation AWS SCT.	DBA
Connectez AWS SCT à la base de données cible.	Pour connecter AWS SCT à votre base de données cible, consultez le document What is the AWS Schema Conversion Tool ? dans le guide de l'utilisateur d'AWS Schema Conversion Tool.	DBA
Convertissez le schéma de base de données dans AWS SCT et enregistrez le code converti automatiquement sous forme de fichier SQL.	Pour enregistrer les fichiers convertis par AWS SCT, consultez la section Enregistrer et appliquer votre schéma converti dans AWS SCT dans	DBA

Tâche	Description	Compétences requises
	le guide de l'utilisateur d'AWS Schema Conversion Tool.	

Migrer le code

Tâche	Description	Compétences requises
Obtenez le fichier SQL pour une conversion manuelle.	Dans le fichier converti AWS SCT, extrayez le fichier SQL qui nécessite une conversion manuelle.	DBA
Mettez à jour le script.	Mettez à jour manuellement le fichier SQL.	DBA

Ressources connexes

- Amazon RDS
- Fonctionnalités d'Amazon Aurora

Informations supplémentaires

L'exemple de code suivant montre comment configurer la base de données source Oracle :

```
CREATE or replace PROCEDURE calc_stats_new1 (
  a NUMBER,
  b NUMBER,
  result out NUMBER)
IS
BEGIN
result:=a+b;
END;
/
```

```
set serveroutput on ;
```

```
DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;
  DBMS_OUTPUT.PUT_LINE('output:'||output);

END;
```

L'exemple de code suivant montre comment configurer la base de données Aurora PostgreSQL cible :

```
 w integer,
 x integer)
RETURNS integer
AS
$BODY$
DECLARE
begin
return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized
      ('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );

PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
```

```
END;
$BODY$
LANGUAGE  plpgsql;


DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

Gérez les fonctions Oracle surchargées dans la compatibilité avec Aurora PostgreSQL

Créée par Sumana Yanamandra (AWS)

Récapitulatif

Le code que vous migrez d'une base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL peut inclure des fonctions surchargées. Ces fonctions ont la même définition, c'est-à-dire le même nom de fonction et le même nombre et le même type de données de paramètres d'entrée (`IN`), mais le type de données ou le nombre de paramètres de sortie () peuvent être différents. `OUT`

Ces incohérences de paramètres peuvent entraîner des problèmes dans PostgreSQL, car il est difficile de déterminer la fonction à exécuter. Ce modèle montre comment gérer les fonctions surchargées lorsque vous migrez le code de votre base de données vers une version compatible avec Aurora PostgreSQL.

Conditions préalables et limitations

Prérequis

- Une instance de base de données Oracle comme base de données source
- Une instance de base de données compatible avec Aurora PostgreSQL comme base de données cible (voir les instructions de la documentation Aurora)

Versions du produit

- Oracle Database 9i ou version ultérieure
- Version 18.4.0.376 d'Oracle SQL Developer
- client PGadmin 4
- Version 11 ou ultérieure compatible avec Aurora PostgreSQL (voir Identification des versions d'Amazon Aurora PostgreSQL dans la documentation Aurora)

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.

Autres outils

- Oracle SQL Developer est un environnement de développement intégré gratuit permettant de travailler avec SQL dans les bases de données Oracle dans le cadre de déploiements traditionnels et dans le cloud.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Épopées

Créez une fonction simple

Tâche	Description	Compétences requises
Créez une fonction dans PostgreSQL dotée d'un paramètre d'entrée et d'un paramètre de sortie.	L'exemple suivant illustre une fonction nommée `test_overloading` dans Aurora PostgreSQL compatible. Cette fonction possède deux paramètres : un paramètre de texte d'entrée et un paramètre de texte de sortie. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE BEGIN`	Ingénieur de données, compatible avec Aurora PostgreSQL

Tâche	Description	Compétences requises
	`str2 := 'Success'; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Exécutez la fonction dans PostgreSQL.	Exécutez la fonction que vous avez créée à l'étape précédente.
	`select public.test_overloading('Test');`
	Il devrait afficher le résultat suivant.
	`Success`
		Ingénieur de données, compatible avec Aurora PostgreSQL

Surcharger la fonction

Tâche	Description	Compétences requises
Utilisez le même nom de fonction pour créer une fonction surchargée dans PostgreSQL.	Créez une fonction surchargée compatible avec Aurora PostgreSQL qui utilise le même nom de fonction que votre fonction précédente. L'exemple suivant est également nommé `test_overloading` , mais il comporte trois paramètres : un	Ingénieur de données, compatible avec Aurora PostgreSQL

Tâche	Description	Compétences requises
	paramètre de texte en entrée, un paramètre de texte en sortie et un paramètre entier en sortie. `CREATE OR REPLACE FUNCTION public.test_overloading( str1 text, OUT str2 text, OUT num1 integer) LANGUAGE 'plpgsql' COST 100 VOLATILE AS $BODY$ DECLARE str3 text; BEGIN str2 := 'Success'; num1 := 100; RETURN ; EXCEPTION WHEN others THEN RETURN ; END; $BODY$;`	

Tâche	Description	Compétences requises

Exécutez la fonction dans PostgreSQL.	Lorsque vous exécutez cette fonction, elle échoue avec le message d'erreur suivant.
	
	`ERROR: cannot change return type of existing function`
	`HINT: Use DROP FUNCTION test_overloading(text) first.`
	
	Cela se produit parce que la compatibilité avec Aurora PostgreSQL ne prend pas directement en charge la surcharge de fonctions. Il ne peut pas identifier la fonction à exécuter, car le nombre de paramètres de sortie est différent dans la deuxième version de la fonction, bien que les paramètres d'entrée soient identiques.
		Ingénieur de données, compatible avec Aurora PostgreSQL

Appliquez la solution

Tâche	Description	Compétences requises
Ajoutez INOUT au premier paramètre de sortie.	Pour contourner le problème, modifiez le code de fonction en représentant le premier paramètre de sortie sous `INOUT` la forme.	Ingénieur de données, compatible avec Aurora PostgreSQL

Tâche	Description	Compétences requises

	CREATE OR REPLACE
	 FUNCTION public.te
	st_overloading(
	str1 text,
	INOUT str2
	 text,
	OUT num1
	 integer)
	LANGUAGE 'plpgsql'
	
	COST 100
	VOLATILE
	AS $BODY$
	DECLARE
	str3 text;
	BEGIN
	
	str2 :=
	 'Success';
	num1 := 100;
	
	RETURN ;
	EXCEPTION
	WHEN others THEN
	RETURN ;
	END;
	$BODY$;	

Tâche	Description	Compétences requises

Exécutez la fonction révisée.	Exécutez la fonction que vous avez mise à jour à l'aide de la requête suivante. Vous passez une valeur nulle comme deuxième argument de cette fonction, car vous avez déclaré ce paramètre `INOUT` pour éviter l'erreur.
	`select public.test_overloading('Test', null);`
	La fonction est maintenant créée avec succès.
	`Success, 100`
		Ingénieur de données, compatible avec Aurora PostgreSQL

Valider les résultats.	Vérifiez que le code contenant la fonction surchargée a été correctement converti.	Ingénieur de données, compatible avec Aurora PostgreSQL

Ressources connexes

- Utilisation d'Amazon Aurora PostgreSQL (documentation Aurora)
- Surcharge des fonctions dans Oracle (documentation Oracle)
- Surcharge de fonctions dans PostgreSQL (documentation PostgreSQL)

Aidez à appliquer le balisage DynamoDB

Créée par Mansi Suratwala (AWS)

Récapitulatif

Ce modèle met en place des notifications automatiques lorsqu'une balise Amazon DynamoDB prédéfinie est manquante ou supprimée d'une ressource DynamoDB sur le cloud Amazon Web Services (AWS).

DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité. DynamoDB vous permet de vous décharger des charges administratives liées à l'exploitation et au dimensionnement d'une base de données distribuée. Lorsque vous utilisez DynamoDB, vous n'avez pas à vous soucier de l'approvisionnement, de l'installation et de la configuration du matériel, de la réplication, de l'application de correctifs logiciels ou de la mise à l'échelle du cluster.

Le modèle utilise un CloudFormation modèle AWS, qui crée un événement Amazon CloudWatch Events et une fonction AWS Lambda. L'événement surveille toute information de balisage DynamoDB nouvelle ou existante à l'aide d'AWS. CloudTrail Si une balise prédéfinie est manquante ou supprimée, CloudWatch déclenche une fonction Lambda, qui vous envoie une notification Amazon Simple Notification Service (Amazon SNS) vous informant de la violation.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un bucket Amazon Simple Storage Service (Amazon S3) pour le fichier Lambda .zip contenant le script Python permettant d'exécuter la fonction Lambda

Limites

- La solution ne fonctionne que lorsque les `UntagResource` CloudTrail événements `TagResource` ou se produisent. Il ne crée pas de notifications pour d'autres événements.

Architecture

Pile technologique cible

- Amazon DynamoDB
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Vous pouvez utiliser le CloudFormation modèle AWS à plusieurs reprises pour différents comptes et régions AWS. Vous ne devez exécuter le modèle qu'une seule fois dans chaque région ou compte.

Outils

Outils

- Amazon DynamoDB — DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité.
- AWS CloudTrail CloudTrail est un service AWS qui vous aide en matière de gouvernance, de conformité, d'audit opérationnel et de gestion des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — Lambda est un service de calcul qui prend en charge l'exécution de code sans qu'il soit nécessaire de configurer ou de gérer des serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service Web qui permet aux applications, aux utilisateurs finaux et aux appareils d'envoyer et de recevoir instantanément des notifications depuis le cloud.

Code

- Un fichier .zip du projet est disponible en pièce jointe.

Épopées

Définition du compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques. Ce compartiment S3 hébergera le fichier .zip du code Lambda. Votre compartiment S3 doit se trouver dans la même région AWS que la ressource DynamoDB surveillée.	Architecte du cloud

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le fichier .zip de code Lambda fourni dans la section Pièces jointes dans le compartiment S3. Le compartiment S3 doit se trouver dans la même région	Architecte du cloud

Tâche	Description	Compétences requises
	que la ressource DynamoDB surveillée.	

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle AWS.	Sur la CloudFormation console AWS, déployez le CloudFormation modèle AWS fourni dans la section Pièces jointes. Dans l'épopée suivante, indiquez les valeurs des paramètres.	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Nommez le compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou choisi dans le premier épisode épique.	Architecte du cloud
Fournissez la clé Amazon S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,). `<folder>/<file-name>.zip`	Architecte du cloud
Fournissez une adresse e-mail	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud

Tâche	Description	Compétences requises
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événement s d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud
Entrez les clés de balise DynamoDB requises.	Assurez-vous que les balises sont séparées par des virgules, sans espaces entre elles (par exemple,`Applicati onId,CreatedBy,Env ironment,Organizat ion`). L'événement CloudWatch Events recherche ces balises et envoie une notification si elles ne sont pas trouvées.	Architecte du cloud

Confirmez votre abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse	Architecte du cloud

Tâche	Description	Compétences requises
	e-mail que vous avez fournie. Pour recevoir des notificat ions de violation, vous devez confirmer cet abonnement par e-mail.	

Ressources connexes

- Création d'un compartiment S3
- Téléchargement de fichiers dans un compartiment S3
- Marquage des ressources dans DynamoDB
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Mettre en œuvre la reprise après sinistre entre régions avec AWS DMS et Amazon Aurora

Créée par Mark Hudson (AWS)

Récapitulatif

Les catastrophes naturelles ou provoquées par l'homme peuvent survenir à tout moment et avoir un impact sur la disponibilité des services et des charges de travail exécutés dans une région AWS donnée. Pour atténuer les risques, vous devez développer un plan de reprise après sinistre (DR) qui intègre les fonctionnalités interrégionales intégrées des services AWS. Pour les services AWS qui ne fournissent pas par nature de fonctionnalités interrégionales, le plan de reprise après sinistre doit également fournir une solution pour gérer leur basculement entre les régions AWS.

Ce modèle vous guide tout au long d'une configuration de reprise après sinistre impliquant deux clusters de bases de données Amazon Aurora compatibles Edition dans une même région. Pour répondre aux exigences de reprise après sinistre, les clusters de bases de données sont configurés pour utiliser la fonctionnalité de base de données globale Amazon Aurora, avec une seule base de données couvrant plusieurs régions AWS. Une tâche AWS Database Migration Service (AWS DMS) réplique les données entre les clusters de la région locale. Cependant, AWS DMS ne prend actuellement pas en charge le basculement des tâches entre les régions. Ce modèle inclut les étapes nécessaires pour contourner cette limitation et configurer AWS DMS de manière indépendante dans les deux régions.

Conditions préalables et limitations

Prérequis

- Certaines régions AWS principales et secondaires prenant en charge les bases de données mondiales Amazon Aurora.
- Deux clusters de bases de données Amazon Aurora compatibles Edition indépendants regroupés dans un seul compte dans la région principale.
- Classe d'instance de base de données db.r5 ou supérieure (recommandé).
- Une tâche AWS DMS dans la région principale effectuant une réplication continue entre les clusters de bases de données existants.
- Ressources de la région DR en place pour répondre aux exigences relatives à la création d'instances de base de données. Pour plus d'informations, consultez la section Utilisation d'une instance de base de données dans un VPC.

Limites

- Pour obtenir la liste complète des limites des bases de données mondiales Amazon Aurora, consultez Limitations des bases de données mondiales Amazon Aurora.

Versions du produit

- Édition compatible avec Amazon Aurora MySQL 5.7 ou 8.0. Pour plus d'informations, consultez les versions d'Amazon Aurora.

Architecture

Pile technologique cible

- Cluster de bases de données mondial Amazon Aurora MySQL Compatible Edition
- AWS DMS

Architecture cible

Le schéma suivant montre une base de données globale pour deux régions AWS, l'une avec les bases de données principales et de rapport et la réplication AWS DMS, et l'autre avec les bases de données principales et de rapports secondaires.

Automatisation et évolutivité

Vous pouvez utiliser AWS CloudFormation pour créer l'infrastructure requise dans la région secondaire, telle que le cloud privé virtuel (VPC), les sous-réseaux et les groupes de paramètres. Vous pouvez également utiliser AWS CloudFormation pour créer les clusters secondaires dans la région DR et les ajouter à la base de données globale. Si vous avez utilisé des CloudFormation modèles pour créer les clusters de base de données dans la région principale, vous pouvez les mettre à jour ou les compléter avec un modèle supplémentaire pour créer la ressource de base de données globale. Pour plus d'informations, consultez Création d'un cluster de base de données Amazon Aurora avec deux instances de base de données et Création d'un cluster de base de données global pour Aurora MySQL.

Enfin, vous pouvez créer les tâches AWS DMS dans les régions principale et secondaire en utilisant les événements CloudFormation After Failover et Failback. Pour de plus amples informations, veuillez consulter AWS::DMS::ReplicationTask.

Outils

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré compatible avec MySQL et PostgreSQL. Ce modèle utilise Amazon Aurora MySQL Compatible Edition.
- Les bases de données mondiales Amazon Aurora sont conçues pour les applications distribuées dans le monde entier. Une seule base de données mondiale Amazon Aurora peut couvrir plusieurs régions AWS. Il réplique vos données sans aucun impact sur les performances de la base de données. Il permet également des lectures locales rapides avec une faible latence dans chaque région et assure la reprise après sinistre en cas de panne à l'échelle de la région.
- AWS DMS permet une migration ponctuelle ou une réplication continue. Une tâche de réplication continue permet de synchroniser vos bases de données source et cible. Une fois configurée, la tâche de réplication en cours applique en permanence les modifications de source à la cible avec une latence minimale. Toutes les fonctionnalités d'AWS DMS, telles que la validation des données et les transformations, sont disponibles pour toutes les tâches de réplication.

Épopées

Préparer les clusters de bases de données existants dans la région principale

Tâche	Description	Compétences requises
Modifiez le groupe de paramètres du cluster de base de données.	Dans le groupe de paramètres du cluster de bases de données existant, activez la journalisation binaire au niveau des lignes en définissant le **`binlog_format`** paramètre sur une valeur de ligne. AWS DMS nécessite une journalisation binaire au niveau des lignes pour les	Administrateur AWS

Tâche	Description	Compétences requises
	bases de données compatibles MySQL lors de la réplication continue ou de la capture des données modifiées (CDC). Pour plus d'informations, consultez Utilisation d'une base de données compatible avec MySQL gérée par AWS comme source pour AWS DMS.	

Tâche	Description	Compétences requises

Mettez à jour la période de conservation des journaux binaires de la base de données.	À l'aide d'un client MySQL installé sur l'appareil de votre utilisateur final ou d'une instance Amazon Elastic Compute Cloud (Amazon EC2), exécutez la procédure stockée suivante fournie par Amazon Relational Database Service (Amazon RDS) sur le nœud d'écriture du cluster de base de données principal , XX où est le nombre d'heures nécessaires pour conserver les journaux.
	`call mysql.rds_set_configuration('binlog retention hours', XX)`
	Confirmez le réglage en exécutant la commande suivante.
	`call mysql.rds_show_configuration;`
	Les bases de données compatibles MySQL gérées par AWS purgent les journaux binaires dès que possible. Par conséquent, la période de conservation doit être suffisamment longue pour garantir que les journaux ne sont pas purgés avant l'exécuti
		DBA

Tâche	Description	Compétences requises
	on de la tâche AWS DMS. Une valeur de 24 heures est généralement suffisant e, mais elle doit être basée sur le temps nécessaire pour configurer la tâche AWS DMS dans la région DR.	

Mettre à jour la tâche AWS DMS existante dans la région principale

Tâche	Description	Compétences requises

Enregistrez l'ARN de la tâche AWS DMS.	Utilisez l'Amazon Resource Name (ARN) pour obtenir le nom de la tâche AWS DMS pour une utilisation ultérieur e. Pour récupérer l'ARN de la tâche AWS DMS, affichez la tâche dans la console ou exécutez la commande suivante.
	`aws dms describe-replication-tasks`
	Un ARN ressemble à ce qui suit.
	`arn:aws:dms:us-east-1:<accountid>:task:AN6HFFMPM246XOZVEUHCNSOVF7MQCLTOZUIRAMY`
		Administrateur AWS

Tâche	Description	Compétences requises
	Les caractères situés après le dernier deux-points correspondent au nom de la tâche utilisé lors d'une étape ultérieure.	
Modifiez la tâche AWS DMS existante pour enregistrer le point de contrôle.	AWS DMS crée des points de contrôle contenant des informations afin que le moteur de réplication connaisse le point de reprise du flux de modifications. Pour enregistrer les informations relatives aux points de contrôle, effectuez les opérations suivantes dans la console : 1. Arrêtez la tâche AWS DMS. 2. Utilisez l'éditeur JSON dans la tâche pour définir le TaskRecoveryTableEnabled paramètre sur true. 3. Démarrez la tâche AWS DMS.	Administrateur AWS

Tâche	Description	Compétences requises
Validez les informations du point de contrôle.	À l'aide d'un client MySQL connecté au point de terminaison du rédacteur du cluster, interrogez la nouvelle table de métadonnées dans le cluster de base de données rapporteur pour vérifier qu'elle existe et qu'elle contient les informations sur l'état de réplication. Exécutez la commande suivante. `select * from awsdms_control.awsdms_txn_state;` Le nom de la tâche issu de l'ARN doit se trouver dans ce tableau dans la `Task_Name` colonne.	DBA

Étendre les deux clusters Amazon Aurora à une région DR

Tâche	Description	Compétences requises
Créez une infrastructure de base dans la région DR.	Créez les composants de base nécessaires à la création et à l'accès aux clusters Amazon Aurora : • Cloud privé virtuel (VPC) • Sous-réseaux • Groupe de sécurité	Administrateur AWS

Tâche	Description	Compétences requises
	• Listes de contrôle d'accès au réseau • Groupe de sous-réseaux • Groupe de paramètres de base de données • Groupe de paramètres de cluster de bases de données Assurez-vous que la configuration des deux groupes de paramètres correspond à celle de la région principale.	
Ajoutez la région DR aux deux clusters Amazon Aurora.	Ajoutez une région secondaire (la région DR) aux clusters Amazon Aurora principaux et déclarants. Pour plus d'informations, consultez Ajouter une région AWS à une base de données mondiale Amazon Aurora.	Administrateur AWS

Effectuer un basculement

Tâche	Description	Compétences requises
Arrêtez la tâche AWS DMS.	La tâche AWS DMS dans la région principale ne fonctionnera pas correctement après le basculement et doit être arrêtée pour éviter les erreurs.	Administrateur AWS

Tâche	Description	Compétences requises
Effectuez un basculement géré.	Effectuez un basculement géré du cluster de base de données principal vers la région DR. Pour obtenir des instructions, consultez la section Réalisation de basculements planifiés gérés pour les bases de données mondiales Amazon Aurora. Une fois le basculement sur le cluster de base de données principal terminé, effectuez la même activité sur le cluster de bases de données rapporteur.	Administrateur AWS, DBA
Chargez les données dans la base de données principale.	Insérez les données de test dans le nœud d'écriture de la base de données principale du cluster de bases de données DR. Ces données seront utilisées pour valider le bon fonctionnement de la réplication.	DBA
Créez l'instance de réplication AWS DMS.	Pour créer l'instance de réplication AWS DMS dans la région DR, consultez Création d'une instance de réplication.	Administrateur AWS, DBA

Tâche	Description	Compétences requises
Créez les points de terminaison source et cible AWS DMS.	Pour créer les points de terminaison source et cible AWS DMS dans la région DR, consultez Création de points de terminaison source et cible. La source doit pointer vers l'instance d'écriture du cluster de base de données principal. La cible doit pointer vers l'instance d'écriture du cluster de base de données de rapporteurs.	Administrateur AWS, DBA
Obtenez le point de contrôle de réplication.	Pour obtenir le point de contrôle de réplication, utilisez un client MySQL pour interroger la table de métadonnées en exécutant la commande suivante sur le nœud d'écriture du cluster de base de données rapporteur dans la région DR. `select * from awsdms_control.awsdms_txn_state;` Dans le tableau, recherchez la valeur task_name qui correspond à l'ARN de la tâche AWS DMS qui existe dans la région principale que vous avez obtenue lors du deuxième épisode épique.	DBA

Tâche	Description	Compétences requises
Créez une tâche AWS DMS.	À l'aide de la console, créez une tâche AWS DMS dans la région DR. Dans la tâche, spécifiez une méthode de migration consistant à répliquer uniquement les modifications de données. Pour plus d'informations, consultez la section Création d'une tâche. 1. Dans les paramètres de la tâche, utilisez l'assistant pour spécifier les éléments suivants : • Mode de démarrage CDC pour les transacti ons source : active le mode de démarrage CDC personnalisé • Point de départ CDC personnalisé pour les transactions sources — Spécifiez un point de contrôle de récupération 2. Dans la case Point de contrôle de restauration, entrez la valeur du point de contrôle de réplication précédemment obtenue par le biais de la requête de base de données sur la `awsdms_txn_state` table.	Administrateur AWS, DBA

Tâche	Description	Compétences requises
	3. Dans la section des paramètres des tâches, sélectionnez l'éditeur JSON et définissez le TaskRecoveryTableEnabledparamètre sur true. Définissez le paramètre Démarrer la tâche de migration d'AWS DMS sur Automatiquement lors de la création.	
Enregistrez l'ARN de la tâche AWS DMS.	Utilisez l'ARN pour obtenir le nom de la tâche AWS DMS pour une utilisation ultérieure. Pour récupérer l'ARN de la tâche AWS DMS, exécutez la commande suivante. `aws dms describe-replication-tasks`	Administrateur AWS, DBA
Validez les données répliquées.	Interrogez le cluster de base de données rapporteur dans la région DR pour confirmer que les données de test que vous avez chargées dans le cluster de base de données principal ont été répliquées.	DBA

Effectuer un retour en arrière

Tâche	Description	Compétences requises
Arrêtez la tâche AWS DMS.	La tâche AWS DMS dans la région DR ne fonctionnera pas correctement après le failback et doit être arrêtée pour éviter les erreurs.	Administrateur AWS
Effectuez un retour en arrière géré.	Replacez le cluster de base de données principal dans la région principale. Pour obtenir des instructions, consultez la section Réalisation de basculements planifiés gérés pour les bases de données mondiales Amazon Aurora. Une fois le retour sur le cluster de base de données principal terminé, effectuez la même activité sur le cluster de base de données rapporteur.	Administrateur AWS, DBA
Obtenez le point de contrôle de réplication.	Pour obtenir le point de contrôle de réplication, utilisez un client MySQL pour interroger la table de métadonnées en exécutant la commande suivante sur le nœud d'écriture du cluster de base de données rapporteur dans la région DR. `select * from awsdms_control.awsdms_txn_state;`	DBA

Tâche	Description	Compétences requises
	Dans le tableau, trouvez la `task_name` valeur correspondant à l'ARN de la tâche AWS DMS qui existe dans la région DR que vous avez obtenue lors de la quatrième épopée.	
Mettez à jour les points de terminaison source et cible d'AWS DMS.	Une fois les clusters de base de données défaillan ts, vérifiez les clusters de la région principale pour déterminer quels nœuds sont les instances d'écriture. Vérifiez ensuite que les points de terminaison source et cible AWS DMS existants dans la région principale pointent vers les instances du rédacteur. Si ce n'est pas le cas, mettez à jour les points de terminaison avec les noms DNS (Domain Name System) de l'instance du rédacteur.	Administrateur AWS

Tâche	Description	Compétences requises
Créez une tâche AWS DMS.	À l'aide de la console, créez une tâche AWS DMS dans la région principale. Dans la tâche, spécifiez une méthode de migration consistant à répliquer uniquement les modifications de données. Pour plus d'informations, consultez la section Création d'une tâche. 1. Dans les paramètres de la tâche, utilisez l'assistant et spécifiez les éléments suivants : • Mode de démarrage CDC pour les transactions source : active le mode de démarrage CDC personnalisé • Point de départ CDC personnalisé pour les transactions sources — Spécifiez un point de contrôle de récupération 2. Dans la case Point de contrôle de restauration, entrez la valeur du point de contrôle de réplication précédemment obtenue par le biais de la requête de base de données sur la `awsdms_txn_state` table.	Administrateur AWS, DBA

Tâche	Description	Compétences requises
	3. Toujours dans la section des paramètres des tâches, sélectionnez l'éditeur JSON et définissez le TaskRecoveryTableEnabledparamètre sur true. 4. Enfin, définissez le paramètre Démarrer la tâche de migration d'AWS DMS sur Automatiquement lors de la création.	
Enregistrez la tâche AWS DMS Amazon Resource Name (ARN).	Utilisez l'ARN pour obtenir le nom de la tâche AWS DMS pour une utilisation ultérieure. Pour récupérer l'ARN de la tâche AWS DMS, exécutez la commande suivante : `aws dms describe-replication-tasks` Le nom de la tâche sera nécessaire lors de l'exécution d'un autre basculement géré ou lors d'un scénario de reprise après sinistre.	Administrateur AWS, DBA
Supprimez les tâches AWS DMS.	Supprimez la tâche AWS DMS d'origine (actuellement arrêtée) dans la région principale et la tâche AWS DMS existante (actuellement arrêtée) dans la région secondaire.	Administrateur AWS

Ressources connexes

- Configuration de votre cluster de base de données Amazon Aurora
- Utilisation de bases de données globales Amazon Aurora
- Utilisation d'Amazon Aurora MySQL
- Utilisation d'une instance de réplication AWS DMS
- Utilisation des points de terminaison AWS DMS
- Utilisation des tâches AWS DMS
- Qu'est-ce qu'AWS CloudFormation ?

Informations supplémentaires

Les bases de données mondiales Amazon Aurora sont utilisées dans cet exemple pour la reprise après sinistre car elles fournissent un objectif de temps de restauration (RTO) effectif de 1 seconde et un objectif de point de reprise (RPO) inférieur à 1 minute, tous deux inférieurs aux solutions répliquées traditionnelles et idéaux pour les scénarios de reprise après sinistre.

Les bases de données mondiales Amazon Aurora offrent de nombreux autres avantages, notamment les suivants :

- Lectures globales avec latence locale — Les consommateurs du monde entier peuvent accéder aux informations d'une région locale, avec une latence locale.
- Clusters de base de données Amazon Aurora secondaires évolutifs : les clusters secondaires peuvent être mis à l'échelle indépendamment, ce qui permet d'ajouter jusqu'à 16 répliques en lecture seule.
- Réplication rapide des clusters de base de données Amazon Aurora principaux vers les clusters secondaires : la réplication a peu d'impact sur les performances du cluster principal. Elle se produit au niveau de la couche de stockage, avec des latences de réplication entre régions typiques de moins d'une seconde.

Ce modèle utilise également AWS DMS pour la réplication. Les bases de données Amazon Aurora permettent de créer des répliques en lecture, ce qui peut simplifier le processus de réplication et la configuration de la reprise après sinistre. Cependant, AWS DMS est souvent utilisé pour effectuer une réplication lorsque des transformations de données sont requises ou lorsque la base de données cible nécessite des index supplémentaires que la base de données source ne possède pas.

Migrer les fonctions et procédures Oracle comportant plus de 100 arguments vers PostgreSQL

Créée par Srinivas Potlachervoo (AWS)

Récapitulatif

Ce modèle montre comment migrer les fonctions et procédures de base de données Oracle comportant plus de 100 arguments vers PostgreSQL. Par exemple, vous pouvez utiliser ce modèle pour migrer les fonctions et procédures Oracle vers l'un des services de base de données AWS compatibles avec PostgreSQL suivants :

- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

PostgreSQL ne prend pas en charge les fonctions ou les procédures comportant plus de 100 arguments. Pour contourner le problème, vous pouvez définir un nouveau type de données dont les champs de type correspondent aux arguments de la fonction source. Vous pouvez ensuite créer et exécuter une fonction PL/pgSQL qui utilise le type de données personnalisé comme argument.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance de base de données Oracle (DB) Amazon RDS
- Une instance de base de données Amazon RDS pour PostgreSQL ou une instance de base de données compatible avec Aurora PostgreSQL

Versions du produit

- Instance de base de données Oracle Amazon RDS 10.2 et versions ultérieures
- Instance de base de données Amazon RDS PostgreSQL versions 9.4 et ultérieures, ou instances de base de données compatibles Aurora PostgreSQL versions 9.4 et ultérieures
- Oracle SQL Developer version 18 et versions ultérieures
- pgAdmin version 4 et versions ultérieures

Architecture

Pile technologique source

- Instance de base de données Oracle Amazon RDS 10.2 et versions ultérieures

Pile technologique cible

- Instance de base de données Amazon RDS PostgreSQL versions 9.4 et ultérieures, ou instances de base de données compatibles Aurora PostgreSQL versions 9.4 et ultérieures

Outils

Services AWS

- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.
- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.

Autres services

- Oracle SQL Developer est un environnement de développement intégré qui simplifie le développement et la gestion des bases de données Oracle dans les déploiements traditionnels et basés sur le cloud.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Bonnes pratiques

Assurez-vous que le type de données que vous créez correspond aux champs de type inclus dans la fonction ou procédure Oracle source.

Épopées

Exécuter une fonction ou une procédure Oracle comportant plus de 100 arguments

Tâche	Description	Compétences requises
Créez ou identifiez une fonction ou une procédure Oracle/PLSQL existante comportant plus de 100 arguments.	Créez une fonction ou une procédure Oracle/PLSQL comportant plus de 100 arguments. -ou- Identifiez une fonction ou une procédure Oracle/PLSQL existante comportant plus de 100 arguments. Pour plus d'informations, consultez les sections 14.7 Instruction CREATE FUNCTION et 14.11 Instruction CREATE PROCEDURE de la documentation de la base de données Oracle.	Connaissances d'Oracle/PLSQL
Compilez la fonction ou la procédure Oracle/PLSQL.	Compilez la fonction ou la procédure Oracle/PLSQL. Pour plus d'informations, voir Compiler une fonction dans la documentation de la base de données Oracle.	Connaissances d'Oracle/PLSQL
Exécutez la fonction Oracle/PLSQL.	Exécutez la fonction ou la procédure Oracle/PLSQL. Enregistrez ensuite le résultat.	Connaissances d'Oracle/PLSQL

Définissez un nouveau type de données qui correspond aux arguments de la fonction ou de la procédure source

Tâche	Description	Compétences requises
Définissez un nouveau type de données dans PostgreSQL.	Définissez un nouveau type de données dans PostgreSQL qui inclut tous les mêmes champs que ceux qui apparaissent dans les arguments de la fonction ou de la procédure Oracle source. Pour plus d'informations, consultez CREATE TYPE dans la documentation de PostgreSQL.	Connaissances de PostgreSQL PL/pgSQL

Créez une fonction PostgreSQL qui inclut le nouvel argument TYPE

Tâche	Description	Compétences requises
Créez une fonction PostgreSQL qui inclut le nouveau type de données.	Créez une fonction PostgreSQL qui inclut le nouvel argument. TYPE Pour consulter un exemple de fonction, consultez la section Informations supplémentaires de ce modèle.	Connaissances de PostgreSQL PL/pgSQL
Compilez la fonction PostgreSQL.	Compilez la fonction dans PostgreSQL. Si les nouveaux champs de type de données correspondent aux arguments de la fonction source ou de	Connaissances de PostgreSQL PL/pgSQL

Tâche	Description	Compétences requises
	la procédure, la fonction se compile correctement.	
Exécutez la fonction PostgreSQL.	Exécutez la fonction PostgreSQL.	Connaissances de PostgreSQL PL/pgSQL

Résolution des problèmes

Problème	Solution
La fonction renvoie l'erreur suivante : ERREUR : erreur de syntaxe à proximité de « » <statement>	Assurez-vous que toutes les instructions de la fonction se terminent par un point-virgule (). `;`
La fonction renvoie l'erreur suivante : ERREUR : « » n'est pas une variable connue <variable>	Assurez-vous que la variable utilisée dans le corps de la fonction est répertoriée dans la `DECLARE` section de la fonction.

Ressources connexes

- Utilisation d'Amazon Aurora PostgreSQL (Guide de l'utilisateur Amazon Aurora pour Aurora)
- TYPE DE CRÉATION (documentation PostgreSQL)

Informations supplémentaires

Exemple de fonction PostgreSQL incluant un argument TYPE

```
CREATE OR REPLACE FUNCTION test_proc_new
(
    IN p_rec type_test_proc_args
)
RETURNS void
AS
$BODY$
```

```
BEGIN

    /*
    **************
    The body would contain code to process the input values.
    For our testing, we will display couple of values.
    ***************
    */
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_acct_id: ', p_rec.p_acct_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_id: ', p_rec.p_ord_id);
    RAISE NOTICE USING MESSAGE = CONCAT_WS('', 'p_ord_date: ', p_rec.p_ord_date);

END;
$BODY$
LANGUAGE plpgsql
COST 100;
```

Migrer les instances de base de données Amazon RDS for Oracle vers d'autres comptes utilisant AMS

Créée par Pinesh Singal (AWS)

Récapitulatif

Ce modèle vous montre comment migrer une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle d'un compte AWS vers un autre compte AWS. Le modèle s'applique aux scénarios dans lesquels le compte AWS source n'utilise pas AWS Managed Services (AMS) mais le compte cible utilise AMS. Vous pouvez effectuer la migration en utilisant une demande de modification (RFC) dans AMS au lieu d'utiliser l'AWS Management Console pour effectuer des opérations de base de données. Cette approche permet de minimiser les temps d'arrêt pour une base de données source Oracle de plusieurs téraoctets comportant un grand nombre de transactions. Par exemple, le temps d'indisponibilité d'une base de données de 400 à 900 Go peut durer environ deux ou trois heures. Le temps de migration de la base de données est directement proportionnel à la taille de l'instance de base de données Amazon RDS for Oracle.

> **Important**
>
> Ce modèle vous oblige à prendre un instantané de base de données de l'instance de base de données Amazon RDS for Oracle dans un compte source, à copier l'instantané sur un compte cible qui utilise AMS, puis à créer une nouvelle instance de base de données à partir de cet instantané en augmentant RFCs.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif pour le compte source
- Un compte AWS actif qui utilise AMS pour le compte cible
- Instance de base de données Amazon RDS pour Oracle, opérationnelle

Limites

- Les mêmes propriétés ou configurations pour les instances de base de données du compte source sont copiées sur une nouvelle instance de base de données cible sur AMS.

- La méthode RFC utilisée dans cette approche de migration comporte des fonctionnalités limitées pour prendre en charge Amazon RDS for Oracle. Vous pouvez accéder à toutes les fonctionnalités d'Amazon RDS for Oracle en utilisant un modèle CloudFormation AWS pour effectuer la migration de la base de données.
- Une application peut être interrompue pendant plusieurs heures, car la migration doit être terminée pendant les interruptions planifiées. Pendant le temps d'arrêt, vous arrêtez l'instance de base de données dans le compte source, puis vous passez en ligne sur une nouvelle instance de base de données dans le compte cible.
- Cette approche de migration ne s'applique pas à la migration d'une instance de base de données d'une région AWS vers une autre région au sein du même compte AWS.

Versions du produit

- Instance Oracle Database Standard Edition 2 (SE2) 12.1.0.2.v2 et versions ultérieures sur Amazon RDS for Oracle
- Amazon RDS pour Oracle 11g n'est plus pris en charge (pour plus d'informations, consultez Amazon RDS pour Oracle dans la documentation Amazon RDS.)

Architecture

Pile technologique source

- Instance de base de données Oracle SE2 12.1.0.2.v2 sur Amazon RDS pour Oracle
- Groupe de sous-réseaux Amazon RDS
- Groupe d'options Amazon RDS (si nécessaire)
- Groupe de paramètres Amazon RDS (si nécessaire)
- Groupe de sécurité Amazon Virtual Private Cloud (Amazon VPC)
- AWS Key Management Service (AWS KMS) avec clés gérées par AWS ou clés gérées par le client
- Rôle AWS Identity and Access Management (IAM) (si nécessaire)

Pile technologique cible

- Instance de base de données Oracle SE2 12.1.0.2.v2 sur Amazon RDS pour Oracle
- Groupe de sous-réseaux Amazon RDS
- Groupe d'options Amazon RDS (si nécessaire)

- Groupe de paramètres Amazon RDS (si nécessaire)
- Groupe de sécurité Amazon VPC
- AWS Managed Services (AMS)
- AWS KMS avec clés gérées par AWS et clés gérées par le client
- Rôle IAM (si nécessaire)

Architecture de migration source et cible

Le schéma suivant montre la migration d'une instance de base de données Amazon RDS pour Oracle d'un compte AWS vers une instance de base de données Amazon RDS for Oracle d'un autre compte AWS utilisant AMS.

Le schéma suivant illustre le flux de travail suivant :

1. Prenez un instantané de base de données de l'instance de base de données Amazon RDS for Oracle dans le compte source.
2. Copiez le cliché sur AMS dans le compte cible.
3. Créez une nouvelle instance de base de données Amazon RDS for Oracle à partir de l'instantané du compte cible.

Automatisation et mise à l'échelle

Vous pouvez automatiser et dimensionner la migration en utilisant des CloudFormation modèles et RFCs en créant dans AMS. CloudFormation vous permet d'utiliser toutes les fonctionnalités d'Amazon RDS for Oracle, y compris la possibilité de configurer et de restaurer l'instance de base de données lorsque vous créez une instance de base de données Amazon RDS pour Oracle à partir d'un instantané.

Outils

- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Managed Services (AMS) vous aide à exploiter votre infrastructure AWS de manière plus efficace et plus sécurisée.

Épopées

Préparez-vous au transfert sur le compte cible

Tâche	Description	Compétences requises
Créez une clé AWS KMS personnalisée.	1. Lancez une RFC automatisée appelée Create KMS key pour créer une clé KMS personnalisée à partir de votre compte cible. 2. **Note** Partagez votre clé KMS personnalisée avec le compte source. : vous ne pouvez pas partager les instances de base de données Amazon RDS pour Oracle qui utilisent la clé gérée par AWS par défaut pour Amazon RDS `aws/rds` (). Partagez plutôt l'instance de base de données en la chiffrant à nouveau à partir de votre clé KMS.	AWS, AMS
Créez un groupe de sécurité.	Lancez une RFC automatisée appelée Créer un groupe	AWS, AMS

Tâche	Description	Compétences requises
	de sécurité afin de créer un groupe de sécurité pour votre VPC à partir de votre compte cible. Assurez-vous de spécifier les éléments suivants : • Nouveau nom du groupe de sécurité • Règles d'entrée et de sortie TCP et UDP • Étiquettes standard	

Tâche	Description	Compétences requises
(Facultatif) Passez en revue vos ressources Amazon RDS.	Les ressources suivantes sont créées lors de la création d'une instance de base de données Amazon RDS for Oracle : • Groupe de sous-réseaux Amazon RDS (basé sur l'ID du sous-réseau) • Groupe d'options Amazon RDS (basé sur l'instantané de l'instance de base de données source) • Groupe de paramètres Amazon RDS (basé sur l'instantané de l'instance de base de données) Si vous souhaitez consulter les ressources Amazon RDS créées lors de la création de votre instance de base de données, vous pouvez vous connecter à votre instance de base de données Oracle et rechercher votre groupe de sous-réseaux, votre groupe d'options et votre groupe de paramètres dans la console Amazon RDS.	AWS

Réduction des dépenses sur le compte source

Tâche	Description	Compétences requises
Arrêtez l'application.	Arrêtez l'application et les services qui en dépendent . Vous devez arrêter tout le trafic vers la base de données dans le compte source.	Propriétaire de l'application
Prenez un instantané manuel.	Créez manuellement un instantané de base de données de l'instance de base de données Amazon RDS for Oracle dans le compte source.	AWS
Arrêtez l'instance de base de données.	Arrêtez l'instance de base de données Amazon RDS for Oracle.	AWS
Copiez le cliché.	Copiez le cliché de base de données sur le même compte source, puis utilisez la clé KMS personnalisée partagée depuis le compte cible pour rechiffrer le fichier de capture de base de données copié.	AWS
Partagez le cliché.	Partagez le nouvel instantané (copié avec la clé KMS personnalisée) avec le compte cible.	AWS

Réduction sur le compte cible

Tâche	Description	Compétences requises
Copiez le cliché.	Lancez une RFC automatisée appelée Copy RDS snapshot pour copier l'instantané de base de données sur le même compte cible et utilisez la clé KMS gérée par AWS par défaut créée pour le rechiffrement. Cela est nécessaire pour que le compte cible soit le propriétaire du nouvel instantané et pour permettre à l'instance de base de données Amazon RDS pour Oracle créée à partir de l'instantané d'être associée au groupe d'options, si nécessaire.	AWS, AMS
Créez une instance de base de données à partir du snapshot.	Lancez une RFC automatisée appelée Create DB from snapshot pour créer une instance de base de données Amazon RDS for Oracle à partir de l'instantané. Assurez-vous de spécifier les éléments suivants : • Nouvel identifiant de capture créé à l'étape précédente • ID du VPC • ID de sous-réseau (subnet)	AWS, AMS

Tâche	Description	Compétences requises
	• ID d'instance RDS • Étiquettes standard	
Attachez l'instance au groupe de sécurité et effectuez des mises à jour de configuration.	1. Lancez une RFC manuelle intitulée Update Other pour associer l'instance de base de données Amazon RDS for Oracle que vous avez créée précédemment au groupe de sécurité VPC que vous avez créé précédemment. 2. Apportez des modifications supplémentaires à la configuration de l'instance de base de données Amazon RDS for Oracle.	AWS, AMS

Tâche	Description	Compétences requises
Testez l'instance de base de données.	Testez la connectivité du nouveau point de terminaison d'instance de base de données Amazon RDS for Oracle en vous connectant à une instance ou à un serveur d'applications hébergé sur le même groupe de sécurité et en utilisant Telnet pour vous connecter au port 1521. Pour plus d'informations, consultez la section Connexion à une instance de base de données Amazon RDS dans la documentation Amazon RDS. **Note** Si les informations de connexion de l'utilisateur principal sont disponibles, vous pouvez tester l'instance de base de données Amazon RDS for Oracle en vous connectant depuis n'importe quel client SQL (tel qu'Oracle SQL Developer).	AWS, BASE DE DONNÉES

Ressources connexes

- AWS Managed Services (documentation AWS)

- RFCs Fonctionnement (documentation AWS Managed Services)
- Partage d'instantanés chiffrés (Guide de l'utilisateur Amazon RDS)
- Comment puis-je partager un instantané de base de données Amazon RDS chiffré avec un autre compte ? (Centre de connaissances AWS)
- Qu'est-ce qu'Amazon Relational Database Service (Amazon RDS) ? (Guide de l'utilisateur Amazon RDS)
- Amazon RDS pour Oracle (Guide de l'utilisateur Amazon RDS)
- Utilisation des consoles AMS (documentation AWS Managed Services)

Informations supplémentaires

Annulation de la migration

Si vous souhaitez annuler la migration, procédez comme suit :

1. Émettez une RFC manuelle (Update Other) depuis le compte cible pour supprimer la pile de base de données créée dans le compte cible.
2. Mettez à jour la configuration de l'application pour qu'elle pointe vers l'instance de base de données Amazon RDS for Oracle dans le compte source.
3. Démarrez l'instance de base de données Amazon RDS for Oracle dans le compte source.

Migrer les variables de liaison Oracle OUT vers une base de données PostgreSQL

Créée par Bikash Chandra Rout (AWS) et Vinay Paladi (AWS)

Récapitulatif

Ce modèle montre comment migrer les variables de `OUT` liaison de base de données Oracle vers l'un des services de base de données AWS compatibles avec PostgreSQL suivants :

- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

PostgreSQL ne prend pas `OUT` en charge les variables de liaison. Pour obtenir les mêmes fonctionnalités dans vos instructions Python, vous pouvez créer une fonction PL/pgSQL personnalisée qui utilise plutôt les variables de **`SET`**package `GET` et. Pour appliquer ces variables, l'exemple de script de fonction wrapper fourni dans ce modèle utilise un pack d'extension AWS Schema Conversion Tool (AWS SCT).

> **Note**
>
> Si l'`EXECUTE IMMEDIATE`instruction Oracle est une `SELECT` instruction qui peut renvoyer une ligne au maximum, il est recommandé de procéder comme suit :

- Insérez des variables de `OUT` liaison (définitions) dans la `INTO` clause
- Insérez des variables de `IN` liaison dans la `USING` clause

Pour plus d'informations, consultez l'instruction EXECUTE IMMEDIATE dans la documentation Oracle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source Oracle Database 10g (ou plus récente) dans un centre de données sur site

- Une instance de base de données Amazon RDS pour PostgreSQL ou une instance de base de données compatible avec Aurora PostgreSQL

Architecture

Pile technologique source

- Base de données Oracle Database 10g (ou version ultérieure) sur site

Pile technologique cible

- Une instance de base de données Amazon RDS pour PostgreSQL ou une instance de base de données compatible avec Aurora PostgreSQL

Architecture cible

Le schéma suivant montre un exemple de flux de travail pour la migration des variables de 0UT liaison de base de données Oracle vers une base de données AWS compatible avec PostgreSQL.

Le schéma suivant illustre le flux de travail suivant :

1. AWS SCT convertit le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données AWS cible compatible avec PostgreSQL.
2. Tous les objets de base de données qui ne peuvent pas être convertis automatiquement sont signalés par la fonction PL/pgSQL. Les objets marqués sont ensuite convertis manuellement pour terminer la migration.

Outils

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.

- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Épopées

Migrez les variables de liaison Oracle OUT à l'aide d'une fonction PL/pgSQL personnalisée et d'AWS SCT

Tâche	Description	Compétences requises
Connectez-vous à votre base de données AWS compatible avec PostgreSQL.	Après avoir créé votre instance de base de données, vous pouvez utiliser n'importe quelle application client SQL standard pour vous connecter à une base de données de votre cluster de bases de données. Par exemple, vous pouvez utiliser pgAdmin pour vous connecter à votre instance de base de données. Pour plus d'informations, consultez l'une des rubriques suivantes : • Connexion à une instance de base de données Amazon RDS dans le guide de l'utilisateur Amazon RDS • Connexion à un cluster de base de données Amazon Aurora dans le guide de l'utilisateur Amazon Aurora	Ingénieur en migration

Tâche	Description	Compétences requises
Ajoutez l'exemple de script de fonction wrapper issu de ce modèle au schéma principal de la base de données cible.	Copiez l'exemple de script de fonction wrapper PL/pgSQL depuis la section Informations supplémentaires de ce modèle. Ajoutez ensuite la fonction au schéma principal de la base de données cible. Pour plus d'informations, consultez CREATE FUNCTION dans la documentation PostgreSQL.	Ingénieur en migration
(Facultatif) Mettez à jour le chemin de recherche dans le schéma principal de la base de données cible afin d'inclure le schéma Test_PG.	Pour améliorer les performances, vous pouvez mettre à jour la variable search_path de PostgreSQL afin qu'elle inclue le nom du schéma Test_PG. Si vous incluez le nom du schéma dans le chemin de recherche, il n'est pas nécessaire de le spécifier chaque fois que vous appelez la fonction PL/pgSQL. Pour plus d'informations, consultez la section 5.9.3 Le chemin de recherche du schéma dans la documentation de PostgreSQL.	Ingénieur en migration

Ressources connexes

- Outil de conversion de schéma AWS
- Variables de liaison OUT (documentation Oracle)

- Améliorez les performances des requêtes SQL en utilisant des variables de liaison (Oracle Blog)

Informations supplémentaires

Exemple de fonction PL/pgSQL

```
/* Oracle */

CREATE or replace PROCEDURE test_pg.calc_stats_new1 (
                                                a NUMBER,
                                                b NUMBER,
                                                result out NUMBER
                                               )

IS
BEGIN
result:=a+b;
END;
/
/* Testing */
set serveroutput on
DECLARE
  a NUMBER := 4;
  b NUMBER := 7;
  plsql_block VARCHAR2(100);
  output number;
BEGIN
  plsql_block := 'BEGIN test_pg.calc_stats_new1(:a, :b,:output); END;';
  EXECUTE IMMEDIATE plsql_block USING a, b,out output;  -- calc_stats(a, a, b, a)
  DBMS_OUTPUT.PUT_LINE('output:'||output);
END;

output:11


PL/SQL procedure successfully completed.

--Postgres--

/* Example : 1 */
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new1(
                                                    w integer,
                                                    x integer
```

```
                                                    )
RETURNS integer
AS
$BODY$
begin
      return w + x ;
end;
$BODY$
LANGUAGE  plpgsql;


CREATE OR REPLACE FUNCTION aws_oracle_ext.set_package_variable(
                                                                  package_name name,
                                                                  variable_name name,
                                                                  variable_value
 anyelement
                                                                )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
begin
    perform set_config
      ( format( '%s.%s',package_name, variable_name )
      , variable_value::text
      , false );
  end;
$BODY$;

CREATE OR REPLACE FUNCTION aws_oracle_ext.get_package_variable_record(
                                                                    package_name
 name,
                                                                    record_name name
                                                                  )
RETURNS text
LANGUAGE 'plpgsql'
    COST 100
    VOLATILE
AS $BODY$
begin
    execute 'select ' || package_name || '$Init()';
```

```
    return aws_oracle_ext.get_package_variable
        (
         package_name := package_name
        , variable_name := record_name || '$REC' );
end;
$BODY$;

--init()--
CREATE OR REPLACE FUNCTION test_pg.init()
RETURNS void
AS
$BODY$
BEGIN
if aws_oracle_ext.is_package_initialized('test_pg' ) then
      return;
    end if;
    perform aws_oracle_ext.set_package_initialized
      ('test_pg' );
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_output', NULL::INTEGER);
PERFORM aws_oracle_ext.set_package_variable('test_pg', 'v_status', NULL::text);
END;
$BODY$
LANGUAGE  plpgsql;

/* callable for 1st Example */

DO $$
declare
v_sql text;
v_output_loc int;
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
--raise notice 'v_sql %',v_sql;
execute 'do $a$ declare v_output_l int; begin select * from test_pg.calc_stats_new1('||
a||','||b||') into v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
 end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
raise notice 'v_output_loc %',v_output_loc;
END ;
$$
```

```
/*In above Postgres example we have set the value of v_output using v_output_l in the
 dynamic anonymous block to mimic the
  behaviour of oracle out-bind variable .*/

--Postgres Example : 2 --
CREATE OR REPLACE FUNCTION test_pg.calc_stats_new2(
 w integer,
 x integer,
inout status text,
 out result integer)
AS
$BODY$
DECLARE
begin
result :=  w + x ;
status := 'ok';
end;
$BODY$
LANGUAGE  plpgsql;

/* callable for 2nd Example */
DO $$
declare
v_sql text;
v_output_loc int;
v_staus text:= 'no';
a integer :=1;
b integer :=2;
BEGIN
perform  test_pg.init();
execute 'do $a$ declare v_output_l int; v_status_l text; begin select * from
 test_pg.calc_stats_new2('||a||','||b||','''||v_staus||''') into v_status_l,v_output_l;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_output'', v_output_l) ;
PERFORM aws_oracle_ext.set_package_variable(''test_pg'', ''v_status'', v_status_l) ;
end; $a$'  ;
v_output_loc := aws_oracle_ext.get_package_variable('test_pg', 'v_output');
v_staus := aws_oracle_ext.get_package_variable('test_pg', 'v_status');
raise notice 'v_output_loc %',v_output_loc;
raise notice 'v_staus %',v_staus;
END ;
$$
```

Migrez SAP HANA vers AWS à l'aide de SAP HSR avec le même nom d'hôte

Créée par Pradeep Puliyampatta (AWS)

Récapitulatif

Les migrations de SAP HANA vers Amazon Web Services (AWS) peuvent être effectuées à l'aide de plusieurs options, notamment la sauvegarde et la restauration, l'exportation et l'importation, ainsi que la réplication du système SAP HANA (HSR). Le choix d'une option particulière dépend de la connectivité réseau entre les bases de données SAP HANA source et cible, de la taille de la base de données source, des considérations relatives aux temps d'arrêt et d'autres facteurs.

L'option SAP HSR pour la migration des charges de travail SAP HANA vers AWS fonctionne bien lorsqu'il existe un réseau stable entre les systèmes source et cible et que l'intégralité de la base de données (instantané de réplication de base de données SAP HANA) peut être complètement répliquée en un jour, comme stipulé par SAP pour les exigences de débit réseau pour SAP HSR. Les exigences d'indisponibilité associées à cette approche se limitent à la prise de contrôle de l' AWS environnement cible, à la sauvegarde de la base de données SAP HANA et aux tâches post-migration.

SAP HSR prend en charge l'utilisation de différents noms d'hôte (noms d'hôtes mappés à différentes adresses IP) pour le trafic de réplication entre les systèmes principal, ou source, et secondaire, ou cible. Vous pouvez le faire en définissant ces ensembles spécifiques de noms d'hôtes dans `global.ini` la `[system_replication_hostname_resolution]` section de. Dans cette section, tous les hôtes des sites principal et secondaire doivent être définis sur chaque hôte. Pour connaître les étapes de configuration détaillées, consultez la documentation SAP.

L'un des principaux points à retenir de cette configuration est que les noms d'hôtes du système principal doivent être différents de ceux du système secondaire. Dans le cas contraire, les erreurs suivantes peuvent être observées.

- `"each site must have a unique set of logical hostnames"`
- `"remoteHost does not match with any host of the source site. All hosts of source and target site must be able to resolve all hostnames of both sites correctly"`

Cependant, le nombre d'étapes post-migration peut être réduit en utilisant le même nom d'hôte de base de données SAP HANA sur l'environnement cible. AWS

Ce modèle fournit une solution permettant d'utiliser le même nom d'hôte sur les environnements source et cible lors de l'utilisation de l'option SAP HSR. Avec ce modèle, vous pouvez utiliser l'option SAP HANA Hostname Rename. Vous attribuez un nom d'hôte temporaire à la base de données SAP HANA cible afin de faciliter l'unicité du nom d'hôte pour SAP HSR. Une fois que la migration a atteint l'étape de prise de contrôle dans l'environnement SAP HANA cible, vous pouvez rétablir le nom d'hôte du système cible en nom d'hôte du système source.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Un cloud privé virtuel (VPC) doté d'un point de terminaison de réseau privé virtuel (VPN) ou d'un routeur.
- AWS Client VPN ou AWS Direct Connect configuré pour transférer des fichiers de la source vers la cible.
- Bases de données SAP HANA dans l'environnement source et dans l'environnement cible. Le niveau de correctif de base de données SAP HANA cible doit être égal ou supérieur au niveau de correctif de base de données SAP HANA source, dans la même édition de SAP HANA Platform. Par exemple, la réplication ne peut pas être configurée entre les systèmes HANA 1.0 et HANA 2.0. Pour plus d'informations, reportez-vous à la question 15 de la note SAP : 1999880 — FAQ : réplication du système SAP HANA.
- Serveurs d'applications SAP dans l'environnement cible.
- Volumes Amazon Elastic Block Store (Amazon EBS) dans l'environnement cible.

Limites

La liste suivante de documents SAP couvre les problèmes connus liés à cette solution de contournement, notamment les contraintes relatives à la hiérarchisation dynamique de SAP HANA et aux migrations évolutives :

- 2956397 — Le changement de nom du système de base de données SAP HANA a échoué

- 2222694 — Lorsque vous essayez de renommer le système HANA, le message d'erreur suivant apparaît : « Les fichiers source ne sont pas la propriété de l'utilisateur sidadm d'origine (uid = xxxx) »
- 2607227 — hdblcm : register_rename_system : échec du changement de nom de l'instance SAP HANA
- 2630562 — Le changement de nom d'hôte HANA a échoué et HANA ne démarre pas
- 2935639 — sr_register n'utilise pas le nom d'hôte spécifié sous system_replication_hostname_resolution dans la section global.ini
- 2710211 — Erreur : les noms d'hôtes logiques du système source et du système cible se chevauchent
- 2693441 — Impossible de renommer un système SAP HANA en raison d'une erreur
- 2519672 — Le système HANA (primaire et secondaire) possède des données et une clé (SSFS) différentes du système (PKI) ou est incapable de vérifier
- 2457129 — Le changement de nom d'hôte du système SAP HANA n'est pas autorisé lorsque la hiérarchisation dynamique fait partie du paysage
- 2473002 — Utilisation de la réplication du système HANA pour migrer un système évolutif (SAP n'impose aucune restriction quant à l'utilisation de cette approche de changement de nom d'hôte pour les systèmes SAP HANA évolutifs). Cependant, la procédure doit être répétée sur chaque hôte individuel. D'autres limites liées à la migration progressive s'appliquent également à cette approche.)

Versions du produit

- Cette solution s'applique aux éditions 1.0 et 2.0 de la plateforme SAP HANA DB.

Architecture

Configuration de la source

Une base de données SAP HANA est installée sur l'environnement source. Toutes les connexions au serveur d'applications SAP et les interfaces de base de données utilisent le même nom d'hôte pour les connexions client. Le schéma suivant montre l'exemple de nom d'hôte source `hdbhost` et l'adresse IP correspondante.

Configuration de la cible

L'environnement AWS Cloud cible utilise le même nom d'hôte pour exécuter une base de données SAP HANA. L'environnement cible sur AWS inclut les éléments suivants :

- Base de données SAP HANA
- Serveurs d'applications SAP
- Volumes EBS

Configuration intermédiaire

Dans le schéma suivant, le nom d'hôte de l'environnement AWS cible est renommé temporairement `temp-host` afin que les noms d'hôte de la source et de la cible soient uniques. Une fois que la migration a atteint l'étape de prise de contrôle sur l'environnement cible, le nom d'hôte virtuel du système cible est renommé en utilisant le nom d'origine,`hdbhost`.

La configuration intermédiaire inclut l'une des options suivantes :

- AWS Client VPN avec un point de terminaison Client VPN
- AWS Direct Connect connexion à un routeur

Les serveurs d'applications SAP sur l'environnement AWS cible peuvent être installés soit avant la configuration de la réplication, soit après le rachat. Cependant, l'installation des serveurs d'applications avant la configuration de la réplication peut contribuer à réduire les temps d'arrêt lors de l'installation, de la configuration de la haute disponibilité et des sauvegardes.

Outils

Services AWS

- AWS Client VPNest un service VPN géré basé sur le client qui vous permet d'accéder en toute sécurité aux AWS ressources et aux ressources de votre réseau sur site.
- AWS Direct Connectrelie votre réseau interne à un AWS Direct Connect emplacement via un câble à fibre optique Ethernet standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement destinées au public Services AWS, en contournant les fournisseurs de services Internet sur votre chemin réseau.

- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon EC2). Les volumes EBS se comportent comme des périphériques de stockage en mode bloc bruts non formatés. Vous pouvez monter ces volumes en tant qu'appareils sur vos instances.

Autres outils

- Serveurs d'applications SAP : les serveurs d'applications SAP fournissent aux programmeurs un moyen d'exprimer la logique métier. Le serveur d'applications SAP effectue le traitement des données en fonction de la logique métier. Les données réelles sont stockées dans une base de données, qui constitue un composant distinct.
- SAP HANA Cockpit et SAP HANA Studio : SAP HANA Cockpit et SAP HANA Studio fournissent tous deux une interface administrative à la base de données SAP HANA. Dans SAP HANA Studio, la console d'administration SAP HANA est la vue système qui fournit le contenu pertinent pour l'administration des bases de données SAP HANA.
- Réplication du système SAP HANA — La réplication du système SAP HANA (SAP HSR) est la procédure standard fournie par SAP pour répliquer les bases de données SAP HANA. Les exécutables requis pour SAP HSR font partie du noyau du serveur SAP HANA lui-même.

Épopées

Préparation des environnements source et cible

Tâche	Description	Compétences requises
Installez et configurez les bases de données SAP HANA.	Dans les environnements source et cible, assurez-v ous que la base de données SAP HANA est installée et configurée conformément aux meilleures pratiques de SAP HANA. Pour plus d'informa tions, consultez SAP HANA sur AWS.	Administration de SAP Basis

Tâche	Description	Compétences requises
Mappez l'adresse IP.	Dans l'environnement cible, assurez-vous que le nom d'hôte temporaire est attribué à une adresse IP interne. 1. Attribuez une IPv4 adresse secondaire à l' EC2 instance sur la console de gestion AWS en accédant à Instance EC2, Actions, Mise en réseau, Gérer l'adresse IP, Attribuer une nouvelle adresse IP. 2. Pour attribuer la même adresse à l'adaptateur EC2 réseau (NIC), depuis le système d'exploitation, en tant qu'utilisateur root, exécutez la commande `ip addr add <IP>/32 dev eth0` en la `<IP>` remplaçant par l'adresse IP de l'étape 1.	Administration d'AWS
Résolvez les noms d'hôtes cibles.	Sur la base de données SAP HANA secondaire, vérifiez que les deux noms d'hôte (`hdbhostettemp-host`) sont résolus pour les réseaux de réplication SAP HANA en mettant à jour les noms d'hôte pertinents dans le fichier. `/etc/hosts`	Administration de Linux

Tâche	Description	Compétences requises
Sauvegardez les bases de données SAP HANA source et cible.	Utilisez SAP HANA Studio ou le cockpit SAP HANA pour effectuer des sauvegardes sur les bases de données SAP HANA.	Administration de SAP Basis
Certificats PKI du système Exchange.	(S'applique uniquement à SAP HANA 2.0 et versions ultérieures) Échangez des certificats dans le magasin sécurisé de l'infrastructure à clés publiques (PKI) du système de fichiers (SSFS) entre les bases de données principale et secondaire. Pour plus d'informations, consultez la note SAP 2369981 — Étapes de configuration requises pour l'authentification avec SAP HANA System Replication.	Administration de SAP Basis

Renommez la base de données SAP HANA cible

Tâche	Description	Compétences requises
Arrêtez les connexions des clients cibles.	Dans l'environnement cible, arrêtez les serveurs d'applications SAP et les autres connexions client.	Administration de SAP Basis
Renommez la base de données SAP HANA cible avec le nom d'hôte temporaire.	1. En tant qu'utilisateur root, renommez le nom d'hôte de la base de données SAP HANA cible en nom d'hôte	Administration de SAP Basis

Tâche	Description	Compétences requises

	temporaire en utilisant resident. `hdblcm`
	
	`root $> cd /hana/shared/<SID/hdblcm`
	`root $> ./hdblcm`
	
	2. Choisissez l'option9 `| rename_system | Rename the SAP HANA Database System`.
	3. Entrez le nouveau nom : `temp-host` .
	4. Vous pouvez valider d'autres options selon vos besoins. Veillez toutefois à ne pas confondre le changement de nom d'hôte avec un changement de SID (Note SAP 2598814 — hdblcm : échec du changement de nom du SID).
	
	L'arrêt et le démarrage de la base de données SAP HANA seront contrôlés par`hdblcm`.	

Tâche	Description	Compétences requises
Attribuez des réseaux de réplication.	Dans le `global.ini` fichier du système source, sous l'`[system_replication_hostname_resolution]` en-tête, fournissez les détails du réseau de réplication source et cible. Copiez ensuite les entrées dans le `global.ini` fichier sur le système cible.	Administration de SAP Basis
Activez la réplication sur le serveur principal.	Pour activer la réplication sur la base de données SAP HANA source, exécutez la commande suivante. `hdbnsutil -sr_enable --name=siteA`	Administration de SAP Basis

Tâche	Description	Compétences requises

Enregistrez la base de données SAP HANA cible en tant que système secondaire.	Pour enregistrer la base de données SAP HANA cible en tant que système secondaire à utiliser comme source pour SAP HSR, choisissez la réplication asynchrone.
	`(sid)adm $> HDB stop`
	`(sid)adm $> hdbnsutil -sr_register –name=siteB –remotehost=hdbhost /`
	`--remoteInstance=00 –replicationMode=async –operationMode=logreplay`
	`(sid)adm $> HDB start`
	Vous pouvez également choisir l'`–online`option d'enregistrement. Dans ce cas, il n'est pas nécessaire d'arrêter et de démarrer la base de données SAP HANA.
		Administration de SAP Basis

Tâche	Description	Compétences requises

Validez la synchronisation.	Sur la base de données SAP HANA source, vérifiez que tous les journaux sont appliqués au système cible (car il s'agit d'une réplication asynchrone).
	
	Pour vérifier la réplication, exécutez les commandes suivantes sur la source.
	
	`(sid)adm $> cdpy`
	`(sidadm $> python systemReplicationStatus.py`
		Administration de SAP Basis

Arrêtez l'application SAP source et la base de données SAP HANA.	Pendant le passage à la migration, arrêtez le système source (l'application SAP et la base de données SAP HANA).	Administration de SAP Basis
Effectuez une prise de contrôle sur la cible.	Pour effectuer une prise de contrôle sur la cible sur AWS, exécutez la commande`hdbnsutil -sr_takeover` .	Administration de SAP Basis

Tâche	Description	Compétences requises
Sur la base de données SAP HANA cible, désactivez la réplication.	Pour effacer les métadonnées de réplication, arrêtez la réplication sur le système cible en exécutant la commande`hdbnsutil -sr_disable` . **Note** Ceci est conforme à la note SAP 2693441 — Impossible de renommer un système SAP HANA en raison d'une erreur.	Administration de SAP Basis
Sauvegardez la base de données SAP HANA cible.	Une fois le rachat réussi, nous vous recommandons d'effectuer une sauvegarde complète de la base de données SAP HANA.	Administration de SAP Basis

Revenir au nom d'hôte d'origine dans le système cible

Tâche	Description	Compétences requises
Rétablissez le nom d'hôte de la base de données SAP HANA cible à l'original.	1. Pour rétablir le nom d'hôte de la base de données SAP HANA cible au nom d'hôte virtuel d'origine, utilisez resident. `hdblcm` `root $> cd /hana/shared/<SID>/hdblcm`	Administration de SAP Basis

Tâche	Description	Compétences requises
	`root $> ./hdblcm` 2. Choisissez l'option9 | `rename_system` | `Rename the SAP HANA Database System`. 3. Entrez le nouveau nom :`hdbhost`. Vous pouvez valider d'autres options selon vos besoins. Veillez toutefois à ne pas confondre le changemen t de nom d'hôte avec un changement de SID (Note SAP 2598814 — hdblcm : échec du changement de nom du SID).	
Ajustez hdbuserstore.	Adaptez les `hdbuserst ore` détails pointant vers les `schema/user` détails de la source. Pour connaître les étapes détaillées, consultez la documentation SAP. Pour valider cette étape, exécutez la commande`R3trans -d`. Le résultat doit refléter une connexion réussie à la base de données SAP HANA.	Administration de SAP Basis

Tâche	Description	Compétences requises
Démarrez les connexions client.	Dans l'environnement cible, démarrez les serveurs d'applications SAP et les autres connexions client.	Administration de SAP Basis

Ressources connexes

Références SAP

Les références de documentation SAP sont fréquemment mises à jour par SAP. Pour rester à jour, consultez la note SAP 2407186 intitulée Guides pratiques et livres blancs pour la haute disponibilité de SAP HANA.

Remarques SAP supplémentaires

- 2550327 — Comment renommer un système SAP HANA
- 1999880 — FAQ : réplication du système SAP HANA
- 2078425 — Note de dépannage concernant l'outil de gestion du cycle de vie de la plateforme SAP HANA hdblcm
- 2592227 — Modification du suffixe FQDN dans les systèmes HANA
- 2048681 — Exécution de tâches d'administration de gestion du cycle de vie de la plateforme SAP HANA sur des systèmes à hôtes multiples sans informations d'identification SSH ou root

Documents SAP

- Connexion réseau de réplication du système
- Résolution du nom d'hôte pour la réplication du système

AWS références

- Migration de SAP HANA depuis d'autres plateformes vers AWS

Informations supplémentaires

Les modifications effectuées dans le `hdblcm` cadre de l'activité de changement de nom d'hôte sont consolidées dans le journal détaillé suivant.

Migrer SQL Server vers AWS à l'aide de groupes de disponibilité distribués

Créée par Praveen Marthala (AWS)

Récapitulatif

Les groupes de disponibilité Microsoft SQL Server Always On fournissent une solution de haute disponibilité (HA) et de reprise après sinistre (DR) pour SQL Server. Un groupe de disponibilité se compose d'une réplique principale qui accepte le trafic de lecture/écriture et d'un maximum de huit répliques secondaires qui acceptent le trafic de lecture. Un groupe de disponibilité est configuré sur un cluster Windows Server Failover (WSFC) comportant deux nœuds ou plus.

Les groupes de disponibilité distribués Microsoft SQL Server Always On fournissent une solution pour configurer deux groupes de disponibilité distincts entre deux groupes indépendants WFSCs. Les groupes de disponibilité qui font partie du groupe de disponibilité distribué ne doivent pas nécessairement se trouver dans le même centre de données. L'un des groupes de disponibilité peut se trouver sur site, tandis que l'autre groupe de disponibilité peut se trouver sur le cloud Amazon Web Services (AWS) sur des instances Amazon Elastic Compute Cloud (Amazon EC2) d'un domaine différent.

Ce modèle décrit les étapes d'utilisation d'un groupe de disponibilité distribué pour migrer des bases de données SQL Server locales faisant partie d'un groupe de disponibilité existant vers SQL Server avec des groupes de disponibilité configurés sur Amazon EC2. En suivant ce modèle, vous pouvez migrer les bases de données vers le cloud AWS avec un temps d'arrêt minimal lors de la transition. Les bases de données sont hautement disponibles sur AWS immédiatement après le passage. Vous pouvez également utiliser ce modèle pour faire passer le système d'exploitation sous-jacent sur site à AWS tout en conservant la même version de SQL Server.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- AWS Direct Connect ou AWS Site-to-Site VPN
- La même version de SQL Server installée sur site et sur les deux nœuds d'AWS

Versions du produit

- SQL Server version 2016 et versions ultérieures

- SQL Server Enterprise Edition

Architecture

Pile technologique source

- Base de données Microsoft SQL Server avec groupes de disponibilité Always On sur site

Pile technologique cible

- Base de données Microsoft SQL Server avec groupes de disponibilité Always On sur Amazon EC2 sur le cloud AWS

Architecture de migration

Terminologie

- WSFC 1 — WSFC sur site
- WSFC 2 — WSFC sur le cloud AWS
- AG 1 — Premier groupe de disponibilité, qui se trouve dans WSFC 1
- AG 2 — Deuxième groupe de disponibilité, qui se trouve dans WSFC 2
- Réplique principale de SQL Server : nœud dans AG 1 considéré comme le principal global pour toutes les écritures
- Redirecteur SQL Server : nœud dans AG 2 qui reçoit des données de manière asynchrone à partir de la réplique principale de SQL Server
- Réplique secondaire de SQL Server : nœuds d'AG 1 ou AG 2 qui reçoivent des données de manière synchrone en provenance de la réplique principale ou du redirecteur

Outils

- AWS Direct Connect — AWS Direct Connect relie votre réseau interne à un site AWS Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les services AWS publics, en contournant les fournisseurs de services Internet sur votre chemin réseau.

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que vous le souhaitez, et vous pouvez les étendre ou les intégrer.
- Site-to-SiteVPN AWS — Le Site-to-Site VPN AWS prend en charge la création d'un réseau privé site-to-site virtuel (VPN). Vous pouvez configurer le VPN pour transmettre le trafic entre les instances que vous lancez sur AWS et votre propre réseau distant.
- Microsoft SQL Server Management Studio — Microsoft SQL Server Management Studio (SSMS) est un environnement intégré de gestion de l'infrastructure SQL Server. Il fournit une interface utilisateur et un groupe d'outils dotés d'éditeurs de script riches qui interagissent avec SQL Server.

Épopées

Configuration d'un deuxième groupe de disponibilité sur AWS

Tâche	Description	Compétences requises
Créez un WSFC sur AWS.	Créez des EC2 instances WSFC 2 sur Amazon avec deux nœuds pour HA. Vous utiliserez ce cluster de basculement pour créer le deuxième groupe de disponibilité (AG 2) sur AWS.	Administrateur système, SysOps administrateur
Créez le deuxième groupe de disponibilité sur WSFC 2.	À l'aide de SSMS, créez AG 2 sur deux nœuds dans WSFC 2. Le premier nœud de WSFC 2 agira en tant que redirecteur. Le deuxième nœud de WSFC 2 servira de réplique secondaire d'AG 2. À ce stade, aucune base de données n'est disponible dans AG 2. Il s'agit du point de départ pour configure	DBA, Développeur

Tâche	Description	Compétences requises
	r le groupe de disponibilité distribué.	
Créez des bases de données sans option de restauration sur AG 2.	Sauvegardez les bases de données du groupe de disponibilité sur site (AG 1). Restaurez les bases de données à la fois sur le redirecteur et sur la réplique secondaire d'AG 2 sans option de restauration. Lors de la restauration des bases de données, spécifiez un emplacement avec suffisamment d'espace disque pour les fichiers de données de base de données et les fichiers journaux. À ce stade, les bases de données sont en état de restauration. Ils ne font pas partie de l'AG 2 ou du groupe de disponibilité distribuée, et ils ne se synchronisent pas.	DBA, Développeur

Configuration du groupe de disponibilité distribué

Tâche	Description	Compétences requises
Créez le groupe de disponibilité distribué sur AG 1.	Pour créer le groupe de disponibilité distribué sur AG 1, utilisez l'`DISTRIBUTED` option `CREATE`	DBA, Développeur

Tâche	Description	Compétences requises
	`AVAILABILITY GROUP` avec. 1. Utilisez les adresses de point de `LISTENER_URL` terminaison pour AG 1 et AG 2. 2. À utiliser pour `AVAILABILITY-MODE ASYNCHRONOUS_COMMIT` éviter la latence du réseau, le cas échéant. Cela n'aura aucun impact sur les performances de la base de données. 3. Pour `FAILOVER_MODE` , utilisez `MANUAL`. Il s'agit du seul mode de disponibilité qui fonctionne avec les groupes de disponibilité distribués. 4. Pour restaurer les bases de données manuellement sur AG 2 et avoir un meilleur contrôle sur les bases de données plus volumineuses, utilisez `MANUAL` pour`SEEDING_MODE` .	

Tâche	Description	Compétences requises
Créez le groupe de disponibilité distribuée sur AG 2.	Pour créer le groupe de disponibilité distribué sur AG 2, utilisez-le `ALTER AVAILABILITY GROUP` avec l'`DISTRIBUTED` option. 1. Utilisez les adresses de point de `LISTENER_URL` terminaison pour AG 1 et AG 2. 2. À utiliser pour `AVAILABILITY-MODE ASYNCHRONOUS_COMMIT` éviter la latence du réseau, le cas échéant. Cela n'aura aucun impact sur les performances de la base de données. 3. Pour `FAILOVER_MODE` , utilisez `MANUAL`. Il s'agit du seul mode de disponibilité qui fonctionne avec les groupes de disponibilité distribués. 4. Pour restaurer les bases de données manuellement sur AG 2 et avoir un meilleur contrôle sur les bases de données plus volumineuses, utilisez `MANUAL` pour`SEEDING_MODE` .	DBA, Développeur

Tâche	Description	Compétences requises
	Le groupe de disponibilité distribuée est créé entre AG 1 et AG 2. Les bases de données d'AG 2 ne sont pas encore configuré es pour participer au flux de données d'AG 1 vers AG 2.	
Ajoutez des bases de données au redirecteur et à la réplique secondaire sur AG 2.	Ajoutez les bases de données au groupe de disponibi lité distribuée en utilisant l'`SET HADRAVAILABIL ITY GROUP` option `ALTER DATABASE` à la fois dans le redirecteur et dans la réplique secondaire sur AG 2. Cela lance un flux de données asynchrone entre les bases de données sur AG 1 et AG 2. Le primaire global prend des écritures, envoie des données de manière synchrone à la réplique secondaire sur AG 1 et envoie des données de manière asynchrone au redirecteur sur AG 2. Le redirecteur sur AG 2 envoie des données de manière synchrone à la réplique secondaire sur AG 2.	DBA, Développeur

Surveillez le flux de données asynchrone entre AG 1 et AG 2

Tâche	Description	Compétences requises
DMVs Journaux d'utilisation et de SQL Server.	Surveillez l'état du flux de données entre deux groupes de disponibilité à l'aide de vues de gestion dynamiques (DMVs) et de journaux SQL Server. DMVs qui présentent un intérêt pour le suivi incluent `sys.dm_hadr_availability_replica_states` et `sys.dm_hadr_automatic_seeding`. Pour connaître l'état de la synchronisation du redirecteur, surveillez l'état synchronisé dans le journal SQL Server du redirecteur.	DBA, Développeur

Réaliser des activités de transition pour la migration finale

Tâche	Description	Compétences requises
Arrêtez tout le trafic vers le réplica principal.	Arrêtez le trafic entrant vers le réplica principal dans AG 1 afin qu'aucune activité d'écriture ne se produise sur les bases de données et que celles-ci soient prêtes pour la migration.	Propriétaire de l'application, développeur

Tâche	Description	Compétences requises
Modifiez le mode de disponibilité du groupe de disponibilité distribué sur AG 1.	Sur le réplica principal , définissez le mode de disponibilité du groupe de disponibilité distribué sur synchrone. Une fois que vous avez changé le mode de disponibilité en mode synchrone, les données sont envoyées de manière synchrone depuis la réplique principale dans AG 1 vers le redirecteur dans AG 2.	DBA, Développeur
Vérifiez le LSNs dans les deux groupes de disponibilité.	Vérifiez les derniers numéros de séquence log (LSNs) dans AG 1 et AG 2. Aucune écriture n'ayant lieu dans le réplica principal d'AG 1, les données sont synchronisées et les derniers groupes LSNs de disponibilité doivent correspondre.	DBA, Développeur
Mettez AG 1 à jour avec le rôle secondaire.	Lorsque vous mettez à jour AG 1 vers le rôle secondaire, AG 1 perd le rôle de réplique principal et n'accepte pas les écritures, et le flux de données entre deux groupes de disponibilité s'arrête.	DBA, Développeur

Basculer vers le deuxième groupe de disponibilité

Tâche	Description	Compétences requises
Basculez manuellement vers AG 2.	Sur le redirecteur d'AG 2, modifiez le groupe de disponibilité distribuée pour permettre la perte de données. Comme vous avez déjà vérifié et confirmé que les dernières données LSNs sur AG 1 et AG 2 correspondent, la perte de données n'est pas un problème. Lorsque vous autorisez la perte de données sur le transitaire dans AG 2, les rôles de AG 1 et AG 2 changent : • AG 2 devient le groupe de disponibilité avec la réplique principale et la réplique secondaire. • AG 1 devient le groupe de disponibilité avec le redirecteur et la réplique secondaire.	DBA, Développeur
Modifiez le mode de disponibilité du groupe de disponibilité distribué sur AG 2.	Sur la réplique principale dans AG 2, passez le mode de disponibilité en mode asynchrone. Cela fait passer le mouvement des données d'AG 2 à AG 1, de synchrone à asynchrone. Cette étape est nécessair	DBA, Développeur

Tâche	Description	Compétences requises
	e pour éviter le temps de latence du réseau entre AG 2 et AG 1, le cas échéant, et n'aura aucun impact sur les performances de la base de données.	
Commencez à envoyer du trafic vers le nouveau réplica principal.	Mettez à jour la chaîne de connexion pour utiliser le point de terminaison URL de l'écouteur sur AG 2 pour envoyer du trafic aux bases de données. AG 2 accepte désormais les écritures et envoie des données au redirecteur dans AG 1, ainsi que l'envoi de données vers sa propre réplique secondaire dans AG 2. Les données se déplacent de manière asynchrone de l'AG 2 à l'AG 1.	Propriétaire de l'application, développeur

Réaliser des activités après le passage au poste

Tâche	Description	Compétences requises
Supprimez le groupe de disponibilité distribuée sur AG 2.	Surveillez la migration pendant la durée prévue. Supprimez ensuite le groupe de disponibilité distribué sur AG 2 pour supprimer la configuration du groupe de disponibilité distribué entre AG 2 et AG 1.	DBA, Développeur

Tâche	Description	Compétences requises
	Cela supprime la configura tion du groupe de disponibilité distribué et le flux de données entre AG 2 et AG 1 s'arrête. À ce stade, AG 2 est hautement disponible sur AWS, avec une réplique principale qui prend des écritures et une réplique secondaire dans le même groupe de disponibilité.	
Mettez hors service les serveurs locaux.	Mettez hors service les serveurs locaux de WSFC 1 qui font partie d'AG 1.	Administrateur système, SysOps administrateur

Ressources connexes

- Groupes de disponibilité distribués
- SQL Docs : groupes de disponibilité distribués
- SQL Docs : Groupes de disponibilité Always On : une solution de haute disponibilité et de reprise après sinistre

Migrez d'Oracle 8i ou 9i vers Amazon RDS for Oracle à l'aide d'AWS DMS SharePlex

Créée par Ramu Jagini (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Oracle 8i ou 9i sur site vers une base de données Amazon Relational Database Service (Amazon RDS) pour Oracle. Vous pouvez utiliser ce modèle pour terminer votre migration en réduisant les temps d'arrêt en utilisant Quest SharePlex pour la réplication synchrone.

Vous devez utiliser une instance de base de données Oracle intermédiaire pour votre migration car AWS Database Migration Service (AWS DMS) ne prend pas en charge Oracle 8i ou 9i en tant qu'environnement source. Vous pouvez utiliser la version SharePlex 7.6.3 pour effectuer une réplication à partir de versions de base de données Oracle précédentes vers des versions ultérieures de base de données Oracle. L'instance de base de données Oracle intermédiaire est compatible en tant que cible pour la version SharePlex 7.6.3 et prise en charge en tant que source pour AWS DMS ou les versions plus récentes de. SharePlex Cette prise en charge permet la réplication ultérieure des données vers l'environnement cible Amazon RDS for Oracle.

Sachez que plusieurs types de données et fonctionnalités obsolètes peuvent avoir un impact sur la migration d'Oracle 8i ou 9i vers la dernière version d'Oracle Database. Pour atténuer cet impact, ce modèle utilise Oracle 11.2.0.4 comme version de base de données intermédiaire afin d'optimiser le code du schéma avant la migration vers l'environnement cible Amazon RDS for Oracle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle 8i ou 9i source dans un environnement sur site
- Oracle Database 12c version 2 (12CR2) pour le staging sur Amazon Elastic Compute Cloud (Amazon EC2)
- Quest SharePlex 7.6.3 (version commerciale)

Limites

- Limites de RDS pour Oracle

Versions du produit

- Oracle 8i ou 9i pour la base de données source
- Oracle 12 CR2 pour la base de données intermédiaire (doit correspondre à la version Amazon RDS for Oracle)
- Oracle 12 CR2 ou version ultérieure pour la base de données cible (Amazon RDS for Oracle)

Architecture

Pile technologique source

- Base de données Oracle 8i ou 9i
- SharePlex

Pile technologique cible

- Amazon RDS for Oracle

Architecture de migration

Le schéma suivant montre comment migrer une base de données Oracle 8i ou 9i d'un environnement sur site vers une instance de base de données Amazon RDS for Oracle dans le cloud AWS.

Le schéma suivant illustre le flux de travail suivant :

1. Activez la base de données source Oracle avec le mode journal d'archivage, la journalisation forcée et la journalisation supplémentaire.
2. Restaurez la base de données intermédiaire Oracle à partir de la base de données source Oracle en utilisant Recovery Manager (RMAN) point-in-time Recovery et FLASHBACK_SCN.
3. Configurez SharePlex pour lire les journaux de journalisation à partir de la base de données source Oracle en utilisant `FLASHBACK_SCN` (utilisé dans RMAN).
4. Lancez SharePlex la réplication pour synchroniser les données de la base de données source Oracle vers la base de données intermédiaire Oracle.

5. Restaurez la base de données cible Amazon RDS for Oracle en utilisant EXPDP et IMPDP avec. `FLASHBACK_SCN`
6. Configurez AWS DMS et ses tâches sources en tant que base de données intermédiaire Oracle et Amazon RDS for Oracle en tant que base de données cible `FLASHBACK_SCN` en utilisant (utilisé dans EXPDP).
7. Lancez des tâches AWS DMS pour synchroniser les données de la base de données intermédiaire Oracle avec la base de données cible Oracle.

Outils

- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- SharePlexQuest est un outil de réplication de Oracle-to-Oracle données permettant de déplacer des données avec un minimum de temps d'arrêt et sans perte de données.
- Recovery Manager (RMAN) est un client de base de données Oracle qui effectue des tâches de sauvegarde et de restauration sur vos bases de données. Il simplifie considérablement la sauvegarde, la restauration et la restauration des fichiers de base de données.
- Data Pump Export vous permet de télécharger des données et des métadonnées dans un ensemble de fichiers du système d'exploitation appelé ensemble de fichiers de vidage. L'ensemble de fichiers de vidage ne peut être importé que par l'utilitaire Data Pump Import ou le package DBMS_DATAPUMP.

Épopées

Configuration SharePlex et base de données de préparation Oracle sur Amazon EC2

Tâche	Description	Compétences requises
Créez une EC2 instance.	1. Créez une EC2 instance. 2. Installez Oracle 12 CR2 sur l' EC2 instance pour qu'elle serve de base de données intermédiaire Oracle.	Administration d'Oracle

Tâche	Description	Compétences requises
Préparez la base de données de préparation.	Préparez la base de données intermédiaire Oracle pour la restauration en tant que mise à niveau sur Oracle 12 CR2 en utilisant la sauvegarde RMAN depuis l'environnement source de base de données Oracle 8i ou 9i. Pour plus d'informations, consultez le guide de l'utilisateur d'Oracle 9i Recovery Manager et le guide de l'utilisateur de Database Backup and Recovery dans la documentation Oracle.	Administration d'Oracle
Configurez SharePlex.	Configurez la SharePlex source en tant que base de données Oracle 8i ou 9i sur site, et configurez la cible en tant que base de données intermédiaire Oracle 12 CR2 hébergée sur Amazon. EC2	SharePlex, administration d'Oracle

Configurez Amazon RDS for Oracle comme environnement cible

Tâche	Description	Compétences requises
Créez une instance de base de données Oracle.	Créez une base de données Amazon RDS for Oracle, puis connectez Oracle CR2 12 à la base de données.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez Création d'une instance de base de données Oracle et connexion à une base de données sur une instance de base de données Oracle dans la documentation Amazon RDS.	
Restaurez Amazon RDS for Oracle à partir de la base de données intermédiaire.	1. Effectuez une sauvegarde EXPDP depuis le serveur de base de données intermédiaire Oracle en utilisant`FLASHBACK_SCN` . 2. Restaurez Amazon RDS for Oracle à partir de la base de données intermédiaire. Pour plus d'informations, consultez la section 54 DBMS_DATAPUMP dans la documentation Oracle.	DBA

Configuration d'AWS DMS

Tâche	Description	Compétences requises
Créez des points de terminaison pour les bases de données.	Créez un point de terminaison source pour la base de données intermédiaire Oracle et un point de terminaison cible pour la base de données Amazon RDS for Oracle.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez Comment créer des points de terminaison source ou cible à l'aide d'AWS DMS ? dans le centre de connaissances AWS.	
Créez une instance de réplication.	Utilisez AWS DMS pour lancer une instance de réplication de la base de données intermédiaire Oracle vers la base de données Amazon RDS for Oracle. Pour plus d'informations, consultez Comment créer une instance de réplication AWS DMS ? dans le centre de connaissances AWS.	DBA
Créez et lancez des tâches de réplication.	Créez des tâches de réplication AWS DMS pour la capture des données de modification (CDC) `FLASHBACK_SCN` à l'aide de from EXPDP (puisque le chargement complet a déjà été effectué via EXPDP). Pour plus d'informations, consultez la section Création d'une tâche dans la documentation AWS DMS.	DBA

Passez à Amazon RDS for Oracle

Tâche	Description	Compétences requises
Arrêtez la charge de travail de l'application.	Arrêtez les serveurs d'applications et leurs applications pendant la période de transition planifiée.	Développeur d'applications, DBA
Validez la synchronisation de la base de données intermédiaire Oracle locale avec l' EC2 instance.	Vérifiez que tous les messages relatifs aux tâches de réplication ont été publiés depuis l'instance de SharePlex réplication vers la base de données intermédiaire Oracle sur Amazon en EC2 effectuant quelques changements de journal sur la base de données source locale. Pour plus d'informations, reportez-vous à la section 6.4.2 Changer de fichier journal dans la documentation Oracle.	DBA
Validez la synchronisation de la base de données intermédiaire Oracle avec la base de données Amazon RDS for Oracle.	Vérifiez que toutes vos tâches AWS DMS ne présentent aucun décalage ni aucune erreur, puis vérifiez l'état de validation des tâches.	DBA
Arrêtez la réplication SharePlex d'Amazon RDS.	Si les réplications SharePlex et AWS DMS ne présentent aucune erreur, arrêtez les deux réplications.	DBA

Tâche	Description	Compétences requises
Remappez l'application sur Amazon RDS.	Partagez les détails du point de terminaison Amazon RDS for Oracle avec le serveur d'applications et ses applications, puis démarrez l'application pour reprendre les activités commerciales.	Développeur d'applications, DBA

Testez l'environnement cible d'AWS

Tâche	Description	Compétences requises
Testez l'environnement de base de données intermédiaire Oracle sur AWS.	1. Testez la SharePlex réplication et vérifiez qu'il n'y a aucune interruption de synchronisation ou erreur de réplication dans la base de données intermédiaire Oracle. 2. Vérifiez que l'application se comporte comme prévu grâce aux benchmarks définis dans l'environnement sur site.	SharePlex, administration d'Oracle
Testez l'environnement Amazon RDS.	1. Vérifiez que toutes les données propagées vers Amazon RDS après la réplication sont exemptes d'erreur. 2. Dirigez une autre application vers l'instance de base de données Amazon RDS, puis exécutez des tests de	Administration d'Oracle

Tâche	Description	Compétences requises
	performances pour vérifier le comportement attendu. Pour plus d'informations, consultez Amazon RDS pour Oracle dans la documentation Amazon RDS.	

Ressources connexes

- Migrez en toute confiance
- Amazon EC2
- Amazon RDS for Oracle
- AWS Database Migration Service
- Débogage de vos migrations AWS DMS : que faire en cas de problème (partie 1)
- Débogage de vos migrations AWS DMS : que faire en cas de problème (partie 2)
- Débogage de vos migrations AWS DMS : que faire en cas de problème ? (Partie 3)
- SharePlex pour la réplication de bases de données
- SharePlex: réplication de base de données pour tous les environnements

Surveillez Amazon Aurora pour détecter les instances sans chiffrement

Créée par Mansi Suratwala (AWS)

Récapitulatif

Ce modèle fournit un CloudFormation modèle Amazon Web Services (AWS) que vous pouvez déployer pour configurer des notifications automatiques lorsqu'une instance Amazon Aurora est créée sans que le chiffrement soit activé.

Aurora est un moteur de base de données relationnelle entièrement géré compatible avec MySQL et PostgreSQL. Avec certaines charges de travail, Aurora peut offrir un débit jusqu'à cinq fois supérieur à celui de MySQL et jusqu'à trois fois supérieur à celui de PostgreSQL sans qu'il soit nécessaire de modifier la plupart de vos applications existantes.

Le CloudFormation modèle crée un événement Amazon CloudWatch Events et une fonction AWS Lambda. L'événement utilise AWS CloudTrail pour surveiller la création d'une instance Aurora ou la restauration ponctuelle d'une instance existante. L'événement Cloudwatch Events lance la fonction Lambda, qui vérifie si le chiffrement est activé. Si le chiffrement n'est pas activé, la fonction Lambda envoie une notification Amazon Simple Notification Service (Amazon SNS) vous informant de la violation.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

Limites

- Ce contrôle de service fonctionne uniquement avec les instances Amazon Aurora. Il ne prend pas en charge les autres instances Amazon Relational Database Service (Amazon RDS).
- Le CloudFormation modèle doit être déployé pour `CreateDBInstance` et `RestoreDBClusterToPointInTim` e uniquement.

Versions du produit

- Versions de PostgreSQL prises en charge dans Amazon Aurora

- Versions de MySQL prises en charge dans Amazon Aurora

Architecture

Pile technologique cible

- Amazon Aurora
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Vous pouvez utiliser le CloudFormation modèle plusieurs fois pour différentes régions et différents comptes. Vous ne devez l'exécuter qu'une seule fois dans chaque région ou compte.

Outils

Outils

- Amazon Aurora — Amazon Aurora est un moteur de base de données relationnelle entièrement géré compatible avec MySQL et PostgreSQL.
- AWS CloudTrail — AWS vous CloudTrail aide à gérer la gouvernance, la conformité, ainsi que l'audit opérationnel et des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un near-real-time flux d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif que vous pouvez utiliser pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages via Lambda, HTTP, e-mail, notifications push mobiles et messages texte (SMS) mobiles.

Code

Un fichier .zip du projet est disponible en pièce jointe.

Épopées

Créez le compartiment S3 pour le script Lambda

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Ouvrez la console Amazon S3 et choisissez ou créez un compartiment S3. Ce compartiment S3 hébergera le fichier .zip du code Lambda. Votre compartiment S3 doit se trouver dans la même région qu'Aurora. Le nom du compartiment S3 ne peut pas contenir de barres obliques en tête.	Architecte du cloud

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda.	Téléchargez le fichier .zip de code Lambda fourni dans la section Pièces jointes dans	Architecte du cloud

Tâche	Description	Compétences requises
	le compartiment S3 que vous avez défini.	

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Sur la CloudFormation console, déployez le `RDS_Aurora_Encryption_At_Rest.yml` CloudFormation modèle fourni en pièce jointe à ce modèle. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou choisi dans le premier épisode épique.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,). `<directory>/<file-name>.zip`	Architecte du cloud

Tâche	Description	Compétences requises
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événement s d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail fournie. Pour recevoir des notifications, vous devez confirmer cet abonnement par e-mail.	Architecte du cloud

Ressources connexes

- Création d'un compartiment S3

- Téléchargement de fichiers dans un compartiment S3
- Création d'un cluster de base de données Amazon Aurora
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Surveillez GoldenGate les journaux Oracle à l'aide d'Amazon CloudWatch

Créée par Chithra Krishnamurthy (AWS)

Récapitulatif

Oracle GoldenGate assure la réplication en temps réel entre Amazon Relational Database Service (Amazon RDS) pour les bases de données Oracle ou entre les bases de données Oracle hébergées sur Amazon Elastic Compute Cloud (Amazon EC2). Il prend en charge la réplication unidirectionnelle et bidirectionnelle.

Lorsque vous l'utilisez GoldenGate pour la réplication, la surveillance est essentielle pour vérifier que le GoldenGate processus est opérationnel et que les bases de données source et cible sont synchronisées.

Ce modèle explique les étapes à suivre pour implémenter la CloudWatch surveillance GoldenGate d'un journal des erreurs par Amazon et comment configurer des alarmes pour envoyer des notifications en cas d'événements spécifiques, par exemple pour que `STOP` vous `ABEND` puissiez prendre les mesures appropriées pour reprendre rapidement la réplication.

Conditions préalables et limitations

Prérequis

- GoldenGate installé et configuré sur une EC2 instance, afin que vous puissiez configurer la CloudWatch surveillance de ces EC2 instances. Si vous souhaitez surveiller la réplication bidirectionnelle dans toutes les GoldenGate régions AWS, vous devez installer l' CloudWatch agent dans chaque EC2 instance où le GoldenGate processus est en cours d'exécution.

Limites

- Ce modèle explique comment surveiller le GoldenGate processus à l'aide de CloudWatch. CloudWatch ne surveille pas le retard de réplication ni les problèmes de synchronisation des données pendant la réplication. Vous devez exécuter des requêtes SQL distinctes pour surveiller le retard de réplication ou les erreurs liées aux données, comme expliqué dans la GoldenGate documentation.

Versions du produit

- Ce document est basé sur l'implémentation d'Oracle GoldenGate 19.1.0.0.4 pour Oracle sous Linux x86-64. Toutefois, cette solution est applicable à toutes les versions majeures de GoldenGate.

Architecture

Pile technologique cible

- GoldenGate binaires pour Oracle installés sur une instance EC2
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)

Architecture cible

Outils

Services AWS

- Amazon CloudWatch est un service de surveillance utilisé dans ce modèle pour surveiller les journaux GoldenGate d'erreurs.
- Amazon SNS est un service de notification par messages utilisé dans ce modèle pour envoyer des e-mails de notification.

Autres outils

- Oracle GoldenGate est un outil de réplication de données que vous pouvez utiliser pour les bases de données Amazon RDS for Oracle ou les bases de données Oracle hébergées sur Amazon EC2.

Étapes d'implémentation de haut niveau

1. Créez un rôle AWS Identity and Access Management (IAM) pour l' CloudWatch agent.
2. Attachez le rôle IAM à l' EC2 instance où les journaux GoldenGate d'erreurs sont générés.
3. Installez l' CloudWatch agent sur l' EC2 instance.
4. Configurez les fichiers de configuration de l' CloudWatch agent : `awscli.conf` et `awslogs.conf`.

5. Démarrez l' CloudWatch agent.
6. Créez des filtres métriques dans le groupe de journaux.
7. Configurez Amazon SNS.
8. Créez une alarme pour les filtres métriques. Amazon SNS envoie des alertes par e-mail lorsque ces filtres capturent des événements.

Pour des instructions détaillées, reportez-vous à la section suivante.

Épopées

Étape 1. Création d'un rôle IAM pour l'agent CloudWatch

Tâche	Description	Compétences requises
Créez le rôle IAM.	L'accès aux ressources AWS nécessite des autorisations. Vous devez donc créer des rôles IAM pour inclure les autorisations nécessaires à l'exécution de l' CloudWatch agent par chaque serveur. Pour créer le rôle IAM, procédez comme suit : 1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/. 2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle. 3. Pour le type d'entité de confiance, choisissez le service AWS.	AWS en général

Tâche	Description	Compétences requises
	4. Pour les cas d'utilisation courants, choisissez EC2, puis cliquez sur Suivant. 5. Dans la liste des politiques, cochez la case située à côté de CloudWatchAgentServerPolicy. Si nécessaire, utilisez la zone de recherche pour trouver la politique. 6. Choisissez Suivant. 7. Pour Role name (Nom du rôle), entrez un nom pour votre nouveau rôle, par exemple `goldengate-cw-monitoring-role` ou autre, en fonction de vos préférences. 8. (Facultatif) Pour Role description (Description du rôle), entrez une description. 9. Vérifiez que cela CloudWatchAgentServerPolicyapparaît sous le nom de la politique. 10. (Facultatif) Ajoutez une ou plusieurs balises (paires clé-valeur) pour organiser, suivre ou contrôler l'accès à ce rôle, puis choisissez Créer un rôle.	

Étape 2. Attachez le rôle IAM à l'instance GoldenGate EC2

Tâche	Description	Compétences requises
Attachez le rôle IAM à l' EC2 instance où les journaux GoldenGate d'erreurs sont générés.	Les journaux d'erreurs générés par GoldenGat e doivent être renseignés CloudWatch et surveillés. Vous devez donc associer le rôle IAM que vous avez créé à l'étape 1 à l' EC2 instance sur laquelle elle GoldenGate est exécutée. Pour associer un rôle IAM à une instance : 1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/. 2. Dans le volet de navigation, choisissez Instances, puis recherchez l'instance sur laquelle elle GoldenGate est exécutée. 3. Sélectionnez l'instance, puis choisissez Actions, Sécurité, Modifier le rôle IAM. 4. Sélectionnez le rôle IAM créé lors de la première étape à associer à votre instance, puis choisissez Enregistrer.	AWS en général

Étapes 3 à 5. Installation et configuration de l' CloudWatch agent sur l'instance de Goldengate EC2

Tâche	Description	Compétences requises
Installez l' CloudWatch agent sur l' GoldenGate EC2 instance.	Pour installer l'agent, exécutez la commande suivante : `sudo yum install -y awslogs`	AWS en général

Modifiez les fichiers de configuration de l'agent.	1. Exécutez la commande suivante.
	`sudo su -`
	2. Modifiez ce fichier pour mettre à jour la région AWS si nécessaire.
	`cat /etc/awslogs/conf [plugins] cwlogs = cwlogs [default] region = us-east-1`
	3. Modifiez le `/etc/awslogs/awslogs.conf` fichier pour mettre à jour le nom du fichier, le nom du groupe de journaux et le date/time format. You must specify the date/time pour qu'il corresponde au format de date `ggserror.log` ; sinon, le flux de journal ne sera pas transféré CloudWatch. Par exemple :
		AWS en général

Tâche	Description	Compétences requises

	`datetime_format = %Y-%m-%dT%H:%M:%S%z`
	`file = /u03/oracle/oragg/ggserr.log`
	`log_group_name = goldengate_monitor`	

Démarrez l' CloudWatch agent.	Pour démarrer l'agent, utilisez la commande suivante. `$ sudo service awslogsd start` Après avoir démarré l'agent, vous pouvez consulter le groupe de journaux dans la CloudWatch console. Le flux du journal contiendra le contenu du fichier.	AWS en général

Étape 6. Création de filtres métriques pour le groupe de journaux

Tâche	Description	Compétences requises
Créez des filtres métriques pour les mots clés ABEND et STOPPED.	Lorsque vous créez des filtres métriques pour le groupe de journaux, chaque fois que les filtres sont identifiés dans le journal des erreurs, celui-ci déclenche une alarme et envoie une notification par e-mail en fonction de la configuration Amazon SNS.	CloudWatch

Tâche	Description	Compétences requises
	Pour créer des filtres métriques, procédez comme suit : 1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/. 2. Choisissez le nom du groupe de journaux. 3. Choisissez Actions, puis Create metric filter (Créer un filtre de métrique). 4. Pour le modèle de filtre, spécifiez un modèle tel queABEND. 5. Sélectionnez Next (Suivant), puis saisissez un nom pour le filtre de métrique. 6. Sous Détails de la métrique, pour l'espace de noms métrique, entrez le nom de l'espace de CloudWatch noms dans lequel la métrique sera publiée. Si l'espace réservé au nom n'existe pas encore, assurez-vous que l'option Create new (Créer un nouveau) est sélectionnée. 7. Pour Valeur métrique, entrez1, car votre filtre métrique compte les	

Tâche	Description	Compétences requises
	occurrences des mots clés contenus dans le filtre. 8. Réglez l'unité sur Aucune. 9. Choisissez Créer un filtre de métriques. Vous pouvez trouver le filtre de métrique que vous avez créé à partir du panneau de navigation. 10. Créez un autre filtre métrique pour le `STOPPED` modèle. Au sein d'un même groupe de journaux, vous pouvez créer plusieurs filtres métriques et définir des alarmes individue llement.	

Étape 7. Configurer Amazon SNS

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Au cours de cette étape, vous configurez Amazon SNS pour créer des alarmes pour les filtres métriques. Pour créer une rubrique SNS, procédez comme suit : 1. Connectez-vous à la console Amazon SNS chez https://console.aws.amazon.com/sns/ vous.	Amazon SNS

Tâche	Description	Compétences requises
	2. Dans la zone Créer un sujet, entrez un nom de sujet tel que `goldengate-alert` , puis choisissez Étape suivante. 3. Pour Type, choisissez Standard. 4. Faites défiler la page jusqu'en bas et choisissez Créer une rubrique. La console ouvre la page Détails de la nouvelle rubrique.	

Tâche	Description	Compétences requises
Créez un abonnement.	Pour créer un abonnement à la rubrique, procédez comme suit : 1. Dans le volet de navigation de gauche, choisissez Abonnements. 2. Sur la page Abonnements, choisissez Créer un abonnement. 3. Sur la page Créer un abonnement, choisissez le champ ARN du sujet pour voir la liste des sujets de votre compte AWS. 4. Choisissez la rubrique que vous avez créée à l'étape précédente. 5. Pour Protocole, choisissez E-mail. 6. Pour Point de terminaison, entrez une adresse e-mail qui peut recevoir les notifications. 7. Choisissez Créer un abonnement. La console ouvre la page Détails du nouvel abonnement. 8. Vérifiez si votre boîte de réception contient un message provenant d'AWS Notifications, puis choisisse	Amazon SNS

Tâche	Description	Compétences requises
	z Confirmer l'abonnement dans l'e-mail. Amazon SNS ouvre votre navigateur web et affiche une confirmation d'abonnement avec votre ID d'abonnement.	

Étape 8. Créez une alarme pour envoyer des notifications pour les filtres métriques

Tâche	Description	Compétences requises
Créez une alarme pour la rubrique SNS.	Pour créer une alarme basée sur un filtre métrique de groupe de logs : 1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/. 2. Dans le panneau de navigation, choisissez Logs (Journaux), puis Log groups (Groupes de journaux). 3. Sélectionnez le groupe de journaux qui comprend votre filtre de métrique. 4. Sélectionnez Metric filters (Filtres de métrique). 5. Dans l'onglet Filtres métriques, cochez la case correspondant au filtre métrique sur lequel vous	CloudWatch

Tâche	Description	Compétences requises
	souhaitez baser votre alarme. 6. Sélectionnez Créer une alerte. 7. Pour Conditions, spécifiez les éléments suivants dans chaque section : • Pour Threshold type (Type de seuil), choisissez Static (Statique). • Pour Whenever, c'est... <metric-name> , choisissez Greater. • Pour que... , spécifiez 0. 8. Choisissez Suivant. 9. Sous Notification : • Pour Alarm state trigger (Déclencheur de l'état d'alarme), choisissez In alarm (En alarme). • Pour Envoyer une notification à la rubrique SNS suivante, choisissez Sélectionner une rubrique existante. • Dans la boîte e-mail, sélectionnez la rubrique Amazon SNS que vous avez créée à l'étape précédente. 10. Choisissez Suivant.	

Tâche	Description	Compétences requises
	11. Pour Name and description (Nom et description), saisissez un nom et une description pour votre alarme. **Note** Pour la description, vous pouvez spécifier le nom de l'instance afin que l'e-mail de notification soit descriptif. 12. Pour Prévisualiser et créer, vérifiez que votre configuration est correcte, puis choisissez Créer une alarme. Après ces étapes, chaque fois que ces modèles sont détectés dans le fichier journal des GoldenGate erreurs (`ggserr.log`) que vous surveillez, vous recevez une notification par e-mail.	

Résolution des problèmes

Problème	Solution
Le flux du journal des GoldenGate erreurs n'entre pas dans CloudWatch.	Vérifiez le `/etc/awslogs/awslogs.conf` fichier pour vérifier que le nom du fichier, le nom du groupe de journaux et date/time format. You must specify the date/time qu'ils correspon dent au format de date utiliséggserror.log . Dans le cas contraire, le flux de log ne sera pas acheminé vers CloudWatch.

Ressources connexes

- CloudWatch Documentation Amazon
- Collecte de métriques et de journaux avec l' CloudWatch agent
- Documentation Amazon SNS

Replateformage d'Oracle Database Enterprise Edition vers l'édition Standard 2 sur Amazon RDS for Oracle

Créée par Lanre (Lan-Ray) showunmi (AWS) et Tarun Chawla (AWS)

Récapitulatif

Oracle Database Enterprise Edition (EE) est un choix populaire pour exécuter des applications dans de nombreuses entreprises. Dans certains cas, toutefois, les applications n'utilisent que peu ou pas de fonctionnalités d'Oracle Database EE, de sorte qu'il n'est pas justifié d'engager des coûts de licence énormes. Vous pouvez réaliser des économies en rétrogradant ces bases de données vers Oracle Database Standard Edition 2 (SE2) lorsque vous migrez vers Amazon RDS.

Ce modèle décrit comment rétrograder d'Oracle Database EE à Oracle Database SE2 lors d'une migration sur site vers Amazon RDS for Oracle. Les étapes présentées dans ce modèle s'appliquent également si votre base de données EE Oracle est déjà exécutée sur Amazon RDS ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2).

Pour plus d'informations, consultez le guide AWS Prescriptive Guidance sur la façon d'évaluer la rétrogradation des bases de données Oracle vers l'édition Standard 2 sur AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Oracle Database Enterprise Edition
- Outil client, tel qu'Oracle SQL Developer ou SQL*Plus, permettant de se connecter à une base de données Oracle et d'exécuter des commandes SQL sur celle-ci
- Utilisateur de la base de données pour effectuer l'évaluation ; par exemple, l'un des éléments suivants :
  - Utilisateur disposant de privilèges suffisants pour exécuter l'évaluation AWS Schema Conversion Tool (AWS SCT)
  - Utilisateur disposant de privilèges suffisants pour exécuter des requêtes SQL sur les tables du dictionnaire de base de données Oracle
- Utilisateur de base de données pour effectuer la migration de base de données ; par exemple, l'un des éléments suivants :

- Utilisateur disposant de privilèges suffisants pour exécuter AWS Database Migration Service (AWS DMS)
- Utilisateur disposant de privilèges suffisants pour effectuer l'exportation et l'importation d'Oracle Data Pump
- Utilisateur disposant de privilèges suffisants pour exécuter Oracle GoldenGate

Limites

- Amazon RDS for Oracle dispose d'une taille de base de données maximale. Pour plus d'informations, consultez Stockage d'instance de base de données Amazon RDS.

Versions du produit

La logique générale décrite dans ce document s'applique aux versions d'Oracle 9i et ultérieures. Pour connaître les versions prises en charge des bases de données autogérées et Amazon RDS for Oracle, consultez la documentation AWS DMS.

Pour identifier l'utilisation des fonctionnalités dans les cas où AWS SCT n'est pas pris en charge, exécutez des requêtes SQL sur la base de données source. Pour effectuer une migration depuis des versions antérieures d'Oracle dans lesquelles AWS DMS et Oracle Data Pump ne sont pas pris en charge, utilisez les utilitaires Oracle Export and Import.

Pour obtenir la liste actuelle des versions et éditions prises en charge, consultez Oracle sur Amazon RDS dans la documentation AWS. Pour plus de détails sur la tarification et les classes d'instances prises en charge, veuillez consulter Tarification d'Amazon RDS for Oracle.

Architecture

Pile technologique source

- Oracle Database Enterprise Edition s'exécutant sur site ou sur Amazon EC2

Cibler la pile technologique à l'aide d'outils Oracle natifs

- Amazon RDS pour Oracle exécutant une base de données Oracle SE2

1. Exportez les données à l'aide d'Oracle Data Pump.
2. Copiez les fichiers de vidage sur Amazon RDS via un lien de base de données.
3. Importez des fichiers de vidage sur Amazon RDS à l'aide d'Oracle Data Pump.

Cibler la pile technologique à l'aide d'AWS DMS

- Amazon RDS pour Oracle exécutant une base de données Oracle SE2
- AWS DMS

1. Exportez les données à l'aide d'Oracle Data Pump avec FLASHBACK_SCN.
2. Copiez les fichiers de vidage sur Amazon RDS via un lien de base de données.
3. Importez des fichiers de vidage sur Amazon RDS à l'aide d'Oracle Data Pump.
4. Utilisez la capture des données de modification (CDC) d'AWS DMS.

Outils

Services AWS

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS. Ce modèle utilise Amazon RDS for Oracle.
- AWS SCT fournit une interface utilisateur basée sur un projet pour évaluer, convertir et copier automatiquement le schéma de base de données de votre base de données Oracle source dans un format compatible avec Amazon RDS for Oracle. AWS SCT vous permet d'analyser les économies potentielles qui peuvent être réalisées en modifiant le type de licence d'Oracle pour passer de l'édition Enterprise à l'édition Standard. La section Évaluation des licences et support cloud du rapport AWS SCT fournit des informations détaillées sur les fonctionnalités Oracle utilisées afin que vous puissiez prendre une décision éclairée lors de la migration vers Amazon RDS for Oracle.

Autres outils

- Les utilitaires natifs d'importation et d'exportation Oracle prennent en charge le transfert des données Oracle vers et depuis les bases de données Oracle. Oracle propose deux types d'utilitaires d'importation et d'exportation de bases de données : Original Export and Import (pour les versions antérieures) et Oracle Data Pump Export and Import (disponible dans Oracle Database 10g versions 1 et ultérieures).
- Oracle GoldenGate propose des fonctionnalités de réplication en temps réel qui vous permettent de synchroniser votre base de données cible après un chargement initial. Cette option permet de réduire les temps d'arrêt des applications lors de la mise en service.

Épopées

Réaliser une évaluation préalable à la migration

Tâche	Description	Compétences requises
Validez les exigences de base de données pour vos applications.	Assurez-vous que vos applications sont certifiées pour fonctionner sur Oracle Database SE2. Consultez directement le fournisseur du logiciel, le développeur ou la documentation de l'application.	Développeur d'applications, DBA, propriétaire de l'application
Étudiez l'utilisation des fonctionnalités EE directement dans la base de données.	Pour déterminer l'utilisation des fonctionnalités EE, effectuez l'une des opérations suivantes : • Générez un rapport d'évaluation AWS SCT pour votre base de données Oracle EE. Le rapport indique quelles fonctionnalités de votre base de données EE actuelle doivent être supprimées si vous	Propriétaire de l'application, DBA, développeur d'applications

Tâche	Description	Compétences requises
	souhaitez modifier les types de licence. • Si vous possédez un compte Oracle Support, procurez-vous et exécutez le script figurant `options_packs_usage_statistics.sql` dans le document de support 1317265.1 pour générer un rapport des options et fonctionnalités utilisées sur votre base de données Oracle. • Interrogez DBA_FEATURE_USAGE_STATISTICS pour afficher les détails de toutes les fonctionnalités utilisées.	

Tâche	Description	Compétences requises
Identifier l'utilisation des fonctionnalités EE pour les activités opérationnelles.	Les administrateurs de bases de données ou d'applications s'appuient parfois sur des fonctionnalités d'EE uniquement pour leurs activités opérationnelles. Les exemples courants incluent les activités de maintenance en ligne (reconstruction d'index, déplacement de tables) et l'utilisation du parallélisme par des tâches par lots. Ces dépendances peuvent être atténuées en modifiant vos opérations dans la mesure du possible. Identifiez l'utilisation de ces fonctionnalités et prenez une décision basée sur les coûts par rapport aux avantages. Utilisez le tableau de comparaison entre Oracle Database EE et les SE2 fonctionnalités comme guide pour identifier les fonctionnalités disponibles dans Oracle Database SE2.	Développeur d'applications, DBA, propriétaire de l'application

Tâche	Description	Compétences requises
Passez en revue les modèles de charge de travail de la base de données EE Oracle.	Oracle Database limite SE2 automatiquement l'utilisation à un maximum de 16 threads CPU à tout moment. Si votre base de données Oracle EE est autorisée à utiliser le pack de diagnosti c Oracle, utilisez l'outil Automatic Workload Repositor y (AWR), ou les vues DBA_HIST_*, pour analyser les modèles de charge de travail de la base de données afin de déterminer si la limite maximale de 16 threads CPU aura un impact négatif sur les niveaux de service en cas de rétrogradation vers. SE2 Assurez-vous que votre évaluation couvre les périodes de pointe, telles que le traitement en fin de journée, de mois ou d'année.	Propriétaire de l'application, DBA, développeur d'applica tions

Préparer l'infrastructure cible sur AWS

Tâche	Description	Compétences requises
Déployez et configurez l'infrast ructure réseau.	Créez un cloud privé virtuel (VPC) ainsi que des sous-rése aux, des groupes de sécurité	Administrateur AWS, architect e cloud, administrateur réseau, DevOps ingénieur

Tâche	Description	Compétences requises
	et des listes de contrôle d'accès réseau.	
Approvisionnez la base de données Amazon RDS for SE2 Oracle.	Provisionnez la base de données Amazon RDS for SE2 Oracle cible afin de répondre aux exigences de performance, de disponibilité et de sécurité de vos applications. Nous recommandons une configuration multi-AZ pour les charges de travail de production. Toutefois, pour améliorer les performances de migration, vous pouvez différer l'activation de Multi-AZ jusqu'à la fin de la migration des données.	Administrateur cloud, architecte cloud, DBA, DevOps ingénieur, administrateur AWS
Personnalisez l'environnement Amazon RDS.	Configurez des paramètres et options personnalisés et activez une surveillance supplémentaire. Pour plus d'informations, consultez la section Meilleures pratiques pour la migration vers Amazon RDS for Oracle.	Administrateur AWS, administrateur système AWS, administrateur cloud, DBA, architecte cloud

Effectuer les tests de migration, de fonctionnement à sec et d'application

Tâche	Description	Compétences requises
Migrez les données (essai à sec).	Migrez les données de la base de données Oracle EE source vers l'instance de base	DBA

Tâche	Description	Compétences requises
	de données Amazon RDS for SE2 Oracle en utilisant l'approche la mieux adaptée à votre environnement spécifique. Sélectionnez une stratégie de migration en fonction de facteurs tels que la taille, la complexité et la période d'indisponibilité disponible. Utilisez l'une ou plusieurs des options suivantes : • Des outils Oracle natifs tels qu'Oracle Data Pump (recommandé), les utilitaires Oracle Import-Export et Oracle. GoldenGate • AWS DMS, utilisant le chargement complet avec réplication continue via le CDC.	
Validez la base de données cible.	Effectuez la validation après la migration du stockage de la base de données et des objets de code. Consultez les journaux de migration et corrigez les problèmes identifiés. Pour plus d'informations, consultez le guide Migration des bases de données Oracle vers le cloud AWS.	DBA

Tâche	Description	Compétences requises
Testez les applications.	Les administrateurs d'applications et de bases de données doivent effectuer des tests fonctionnels, de performance et opérationnels, le cas échéant. Pour plus d'informations, consultez la section Meilleures pratiques pour la migration vers Amazon RDS for Oracle. Enfin, obtenez l'approbation des résultats des tests par les parties prenantes.	Développeur d'applications, propriétaire de l'application, DBA, ingénieur de migration, responsable de la migration

Découper

Tâche	Description	Compétences requises
Actualisez les données depuis Oracle Database EE.	Sélectionnez une approche d'actualisation des données en fonction des exigences de disponibilité des applications. Pour plus d'informations, consultez les méthodes de migration dans la section Stratégies de migration des bases de données Oracle vers AWS. Par exemple, vous pouvez atteindre un temps d'arrêt quasi nul en utilisant des outils tels qu'Oracle GoldenGate ou AWS DMS avec réplicati	Propriétaire de l'application, responsable du transfert, administrateur de base de données, ingénieur de migration, responsable de la migration

Tâche	Description	Compétences requises
	on continue. Si la période d'indisponibilité le permet, vous pouvez effectuer le transfert final des données à l'aide de méthodes hors ligne telles que les utilitaires Oracle Data Pump ou Original Export-Import.	
Pointez les applications vers l'instance de base de données cible.	Mettez à jour les paramètre s de connexion dans les applications et les autres clients pour qu'ils pointent vers la base de données Amazon RDS for SE2 Oracle.	Développeur d'applications, propriétaire de l'applica tion, ingénieur de migration, responsable de la migration, responsable du transfert
Effectuez des activités après la migration.	Effectuez des tâches après la migration des données, telles que l'activation du multi-AZ, la validation des données et d'autres vérifications.	DBA, ingénieur en migration
Effectuez une surveillance après le passage.	Utilisez des outils tels qu'Amazon CloudWatch et Amazon RDS Performance Insights pour surveiller la base de données Amazon RDS for SE2 Oracle.	Développeur d'applications, propriétaire de l'application, administrateur AWS, DBA, ingénieur de migration

Ressources connexes

Recommandations AWS

- Migration de bases de données Oracle vers le cloud AWS (guide)
- Évaluer la rétrogradation des bases de données Oracle vers l'édition Standard 2 sur AWS (guide)

- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle (modèle)
- Migrate an on-premises Oracle database to Amazon RDS for Oracle using Oracle Data Pump (modèle)

Billets de blogs

- Migration de bases de données Oracle avec un temps d'arrêt quasi nul à l'aide d'AWS DMS
- Analyse de la gestion des performances dans Oracle SE à l'aide d'Amazon RDS for Oracle
- Gestion de votre plan SQL dans Oracle SE avec Amazon RDS for Oracle
- Implémentation du partitionnement des tables dans Oracle Standard Edition : partie 1

Répliquez des bases de données mainframe sur AWS à l'aide de Precisely Connect

Créée par Lucio Pereira (AWS), Balaji Mohan (AWS) et Sayantan Giri (AWS)

Récapitulatif

Ce modèle décrit les étapes à suivre pour répliquer les données des bases de données mainframe vers les magasins de données Amazon en temps quasi réel à l'aide de Precisely Connect. Il met en œuvre une architecture basée sur les événements avec Amazon Managed Streaming for Apache Kafka (Amazon MSK) et des connecteurs de base de données personnalisés dans le cloud afin d'améliorer l'évolutivité, la résilience et les performances.

Precisely Connect est un outil de réplication qui capture les données des systèmes mainframe existants et les intègre dans des environnements cloud. Les données sont répliquées des mainframes vers AWS par le biais de la capture des données de modification (CDC) en utilisant des flux de messages en temps quasi réel avec des pipelines de données hétérogènes à faible latence et à haut débit.

Ce modèle couvre également une stratégie de reprise après sinistre pour des pipelines de données résilients avec réplication des données multirégions et routage sur incident.

Conditions préalables et limitations

Prérequis

- Une base de données mainframe existante, par exemple IBM DB2, IBM Information Management System (IMS) ou Virtual Storage Access Method (VSAM), que vous souhaitez répliquer dans le cloud AWS
- Un compte AWS actif
- AWS Direct Connect ou réseau privé virtuel AWS (AWS VPN) entre votre environnement d'entreprise et AWS
- Un cloud privé virtuel doté d'un sous-réseau accessible par votre ancienne plateforme

Architecture

Pile technologique source

Un environnement mainframe qui inclut au moins l'une des bases de données suivantes :

- Base de données IBM IMS
- Base de DB2 données IBM
- fichiers VSAM

Pile technologique cible

- Amazon MSK
- Amazon Elastic Kubernetes Service (Amazon EKS) et Amazon EKS Anywhere
- Docker
- Une base de données relationnelle ou NoSQL AWS telle que la suivante :
  - Amazon DynamoDB
  - Amazon Relational Database Service (Amazon RDS) pour Oracle, Amazon RDS pour PostgreSQL ou Amazon Aurora
  - Amazon ElastiCache pour Redis
  - Amazon Keyspaces (pour Apache Cassandra)

Architecture cible

Réplication des données du mainframe vers des bases de données AWS

Le schéma suivant illustre la réplication des données du mainframe vers une base de données AWS telle que DynamoDB, Amazon RDS, Amazon ou Amazon Keyspaces ElastiCache. La réplication s'effectue en temps quasi réel à l'aide de Precisely Capture et Publisher dans votre environnement mainframe sur site, de Precisely Dispatcher sur Amazon EKS Anywhere dans votre environnement distribué sur site, et de Precisely Apply Engine et des connecteurs de base de données dans le cloud AWS.

Le schéma suivant illustre le flux de travail suivant :

1. Precisely Capture extrait les données du mainframe à partir des journaux du CDC et les conserve dans un stockage transitoire interne.
2. Precisely Publisher écoute les modifications apportées au stockage interne des données et envoie les enregistrements CDC à Precisely Dispatcher via une connexion TCP/IP.

3. Precisely Dispatcher reçoit les enregistrements CDC de Publisher et les envoie à Amazon MSK. Dispatcher crée des clés Kafka en fonction de la configuration utilisateur et de plusieurs tâches de travail pour envoyer des données en parallèle. Dispatcher envoie un accusé de réception à Publisher lorsque les enregistrements ont été stockés dans Amazon MSK.
4. Amazon MSK détient les dossiers du CDC dans l'environnement cloud. La taille de partition des sujets dépend des exigences de débit de votre système de traitement des transactions (TPS). La clé Kafka est obligatoire pour toute transformation ultérieure et pour la commande de transactions.
5. Le moteur Precisely Apply écoute les enregistrements CDC d'Amazon MSK et transforme les données (par exemple, par filtrage ou mappage) en fonction des exigences de la base de données cible. Vous pouvez ajouter une logique personnalisée aux scripts Precisely SQD. (SQD est le langage propriétaire de Precisely.) Le moteur Precisely Apply transforme chaque enregistrement CDC au format Apache Avro ou JSON et le distribue à différents sujets en fonction de vos besoins.
6. Les rubriques Kafka cibles contiennent des enregistrements CDC dans plusieurs rubriques en fonction de la base de données cible, et Kafka facilite l'ordre des transactions en fonction de la clé Kafka définie. Les clés de partition s'alignent sur les partitions correspondantes pour permettre un processus séquentiel.
7. Les connecteurs de base de données (applications Java personnalisées) écoutent les enregistrements CDC d'Amazon MSK et les stockent dans la base de données cible.
8. Vous pouvez sélectionner une base de données cible en fonction de vos besoins. Ce modèle prend en charge à la fois les bases de données NoSQL et relationnelles.

Reprise après sinistre

La continuité des activités est essentielle au succès de votre entreprise. Le cloud AWS fournit des fonctionnalités de haute disponibilité (HA) et de reprise après sinistre (DR), et prend en charge les plans de reprise et de secours de votre organisation. Ce modèle suit une stratégie de reprise après sinistre active/passive et fournit des conseils de haut niveau pour la mise en œuvre d'une stratégie de reprise après sinistre qui répond à vos exigences en matière de RTO et de RPO.

Le schéma suivant illustre le flux de travail DR.

Le diagramme décrit les éléments suivants :

1. Un basculement semi-automatique est nécessaire en cas de panne dans la région 1 d'AWS. En cas de panne dans la région 1, le système doit initier les modifications de routage pour connecter Precisely Dispatcher à la région 2.

2. Amazon MSK réplique les données par le biais de la mise en miroir entre les régions. C'est pourquoi, lors du basculement, le cluster Amazon MSK de la région 2 doit être promu en tant que principal leader.
3. Le moteur Precisely Apply et les connecteurs de base de données sont des applications sans état qui peuvent fonctionner dans n'importe quelle région.
4. La synchronisation des bases de données dépend de la base de données cible. Par exemple, DynamoDB peut utiliser des tables globales ElastiCache et des banques de données globales.

Traitement à faible latence et haut débit via des connecteurs de base de données

Les connecteurs de base de données sont des composants essentiels de ce modèle. Les connecteurs suivent une approche basée sur les écouteurs pour collecter les données d'Amazon MSK et envoyer des transactions à la base de données via un traitement à haut débit et à faible latence pour les applications critiques (niveaux 0 et 1). Le schéma suivant illustre ce processus.

Ce modèle permet le développement d'une application personnalisée consommant un seul thread grâce à un moteur de traitement multithread.

1. Le thread principal du connecteur consomme les enregistrements CDC d'Amazon MSK et les envoie au pool de threads pour traitement.
2. Les threads du pool de threads traitent les enregistrements CDC et les envoient à la base de données cible.
3. Si tous les threads sont occupés, les enregistrements CDC sont conservés par la file d'attente des threads.
4. Le thread principal attend que tous les enregistrements soient effacés de la file d'attente des threads et valide les offsets dans Amazon MSK.
5. Les threads enfants gèrent les défaillances. En cas d'échec pendant le traitement, les messages d'échec sont envoyés à la rubrique DLQ (file d'attente de lettres mortes).
6. Les threads enfants initient les mises à jour conditionnelles (voir Expressions de condition dans la documentation DynamoDB), en fonction de l'horodatage du mainframe, afin d'éviter toute duplication ou mise à jour dans la base de données. out-of-order

Pour plus d'informations sur la mise en œuvre d'une application client Kafka dotée de fonctionnalités multithreading, consultez le billet de blog intitulé Multi-Threaded Message Consumption with the Apache Kafka Consumer sur le site Web de Confluent.

Outils

Services AWS

- Amazon Managed Streaming for Apache Kafka (Amazon MSK) est un service entièrement géré qui vous permet de créer et d'exécuter des applications utilisant Apache Kafka pour traiter les données de streaming.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Amazon EKS Anywhere vous aide à déployer, utiliser et gérer des clusters Kubernetes exécutés dans vos propres centres de données.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon vous ElastiCache aide à configurer, à gérer et à faire évoluer des environnements de cache en mémoire distribués dans le cloud AWS.
- Amazon Keyspaces (pour Apache Cassandra) est un service de base de données géré qui vous aide à migrer, exécuter et dimensionner vos charges de travail Cassandra dans le cloud AWS.

Autres outils

- Precisely Connect intègre les données des systèmes mainframe existants tels que les ensembles de données VSAM ou les bases de données mainframe IBM dans des plateformes cloud et de données de nouvelle génération.

Bonnes pratiques

- Trouvez la meilleure combinaison de partitions Kafka et de connecteurs multithread pour trouver le meilleur équilibre entre performances et coûts. Plusieurs instances de Precisely Capture et Dispatcher peuvent augmenter les coûts en raison de la consommation plus élevée de MIPS (millions d'instructions par seconde).
- Évitez d'ajouter une logique de manipulation et de transformation des données aux connecteurs de base de données. Pour ce faire, utilisez le moteur Precisely Apply, qui fournit les temps de traitement en microsecondes.

- Créez des appels périodiques de demande ou de vérification de l'état de la base de données (pulsations cardiaques) dans les connecteurs de base de données afin de réchauffer fréquemment la connexion et de réduire le temps de latence.
- Implémentez une logique de validation du pool de threads pour comprendre les tâches en attente dans la file d'attente des threads et attendez que tous les threads soient terminés avant le prochain sondage Kafka. Cela permet d'éviter la perte de données en cas de panne d'un nœud, d'un conteneur ou d'un processus.
- Exposez les mesures de latence via les points de terminaison de santé afin d'améliorer les capacités d'observabilité grâce à des tableaux de bord et à des mécanismes de suivi.

Épopées

Préparation de l'environnement source (sur site)

Tâche	Description	Compétences requises
Configurez le processus du mainframe (batch ou utilitaire en ligne) pour démarrer le processus CDC à partir des bases de données du mainframe.	1. Identifiez l'environnement du mainframe. 2. Identifiez les bases de données mainframe qui seront impliquées dans le processus du CDC. 3. Dans l'environnement mainframe, développez un processus qui lance l'outil CDC pour capturer les modifications apportées à la base de données source. Pour obtenir des instructions, consultez la documentation de votre ordinateur central. 4. Documentez le processus du CDC, y compris la configuration.	Ingénieur mainframe

Tâche	Description	Compétences requises
	5. Déployez le processus dans les environnements de test et de production.	
Activez les flux de journaux de la base de données mainframe.	1. Configurez les flux de journaux dans l'environ nement mainframe pour capturer les journaux CDC. Pour obtenir des instructions, consultez la documentation de votre ordinateur central. 2. Testez les flux de journaux pour vous assurer qu'ils capturent les données nécessaires. 3. Déployez les flux de journaux dans les environne ments de test et de production.	Spécialiste des bases de données mainframe

Tâche	Description	Compétences requises
Utilisez le composant Capture pour capturer les enregistrements CDC.	1. Installez et configurez le composant Precisely Capture dans l'environnement mainframe. Pour obtenir des instructions, consultez la documentation Precisely. 2. Testez la configuration pour vous assurer que le composant Capture fonctionne correctement. 3. Configurez un processus de réplication pour répliquer les enregistrements CDC capturés via le composant Capture. 4. Documentez la configuration de capture pour chaque base de données source. 5. Développez un système de surveillance pour garantir que le composant Capture collecte correctement les journaux au fil du temps. 6. Déployez l'installation et les configurations dans les environnements de test et de production.	Ingénieur mainframe, Precisely Connect SME

Tâche	Description	Compétences requises
Configurez le composant Publisher pour écouter le composant Capture.	1. Installez et configurez le composant Precisely Publisher dans l'environnement mainframe. Pour obtenir des instructions, consultez la documentation Precisely. 2. Testez la configuration pour vous assurer que le composant Publisher fonctionne correctement. 3. Configurez un processus de réplication pour publier les enregistrements CDC sur le composant Precisely Dispatcher à partir de Publisher. 4. Documentez la configuration de Publisher. 5. Développez un système de surveillance pour garantir le bon fonctionnement du composant Publisher au fil du temps. 6. Déployez l'installation et les configurations dans les environnements de test et de production.	Ingénieur mainframe, Precisely Connect SME

Tâche	Description	Compétences requises
Provisionnez Amazon EKS Anywhere dans l'environnement distribué sur site.	1. Installez Amazon EKS Anywhere sur l'infrastructure sur site et assurez-vous qu'elle est correctement configurée. Pour obtenir des instructions, consultez la documentation Amazon EKS Anywhere. 2. Configurez un environnement réseau sécurisé pour le cluster Kubernetes, y compris des pare-feux. 3. Implémentez et testez l'exemple de déploiement de l'application sur le cluster Amazon EKS Anywhere. 4. Mettez en œuvre des fonctionnalités de dimensionnement automatique pour le cluster. 5. Développez et mettez en œuvre des procédures de sauvegarde et de reprise après sinistre.	DevOps ingénieur

Tâche	Description	Compétences requises
Déployez et configurez le composant Dispatcher dans l'environnement distribué pour publier les rubriques dans le cloud AWS.	1. Configurez et conteneur isez le composant Precisely Dispatcher. Pour obtenir des instructions, consultez la documentation Precisely. 2. Déployez l'image Dispatche r Docker dans l'environ nement Amazon EKS Anywhere sur site. 3. Configurez une connexion sécurisée entre le cloud AWS et Dispatcher. 4. Développez un système de surveillance pour garantir le bon fonctionnement du composant Dispatcher au fil du temps. 5. Déployez l'installation et les configurations dans les environnements de test et de production.	DevOps ingénieur, Precisely Connect PME

Préparation de l'environnement cible (AWS)

Tâche	Description	Compétences requises
Provisionnez un cluster Amazon EKS dans la région AWS désignée.	1. Connectez-vous à votre compte AWS et configure z-le pour vous assurer que les autorisations nécessair es sont en place pour créer et gérer le cluster Amazon EKS.	DevOps ingénieur, administr ateur réseau

Tâche	Description	Compétences requises
	2. Créez un cloud privé virtuel (VPC) et des sous-réseaux dans la région AWS sélectionnée. Pour obtenir des instructions, consultez la documentation Amazon EKS. 3. Créez et configurez les groupes de sécurité réseau nécessaires pour permettre les communications entre le cluster Amazon EKS et les autres ressources du VPC. Pour plus d'informations, consultez la documentation Amazon EKS. 4. Créez le cluster Amazon EKS et configurez-le avec la taille de groupe de nœuds et les types d'instances appropriés. 5. Validez le cluster Amazon EKS en déployant un exemple d'application.	

Tâche	Description	Compétences requises
Provisionnez un cluster MSK et configurez les rubriques Kafka applicables.	1. Configurez votre compte AWS pour vous assurer que les autorisations nécessaires sont en place pour créer et gérer le cluster MSK. 2. Créez et configurez les groupes de sécurité réseau nécessaires pour permettre les communications entre le cluster MSK et les autres ressources du VPC. Pour plus d'informations, consultez la documentation Amazon VPC. 3. Créez le cluster MSK et configurez-le pour inclure les sujets Kafka qui seront utilisés par l'application. Pour plus d'informations, consultez la documentation Amazon MSK.	DevOps ingénieur, administrateur réseau

Tâche	Description	Compétences requises
Configurez le composant Apply Engine pour écouter les sujets Kafka répliqués.	1. Configurez et conteneur isez le composant Precisely Apply Engine. 2. Déployez l'image Docker d'Apply Engine dans le cluster Amazon EKS de votre compte AWS. 3. Configurez le moteur d'application pour écouter les sujets MSK. 4. Développez et configure z un script SQD dans le moteur Apply pour gérer le filtrage et la transformation. Pour plus d'informations, consultez la documentation Precisely. 5. Déployez le moteur Apply dans des environnements de test et de production.	Precisely Connect PME

Tâche	Description	Compétences requises
Provisionnez des instances de base de données dans le cloud AWS.	1. Configurez votre compte AWS pour vous assurer que les autorisations nécessaires sont en place pour créer et gérer des clusters et des tables de base de données. Pour obtenir des instructions, consultez la documentation AWS relative au service de base de données AWS que vous souhaitez utiliser. (Voir la section Ressources pour les liens.) 2. Créez un VPC et des sous-réseaux dans la région AWS sélectionnée. 3. Créez et configurez les groupes de sécurité réseau nécessaires pour permettre les communications entre les instances de base de données et les autres ressources du VPC. 4. Créez les bases de données et configurez-les pour inclure les tables que l'application utilisera. 5. Concevez et validez les schémas de base de données.	Ingénieur de données, DevOps ingénieur

Tâche	Description	Compétences requises
Configurez et déployez des connecteurs de base de données pour écouter les rubriques publiées par le moteur Apply.	1. Concevez des connecteurs de base de données pour connecter les rubriques Kafka aux bases de données AWS que vous avez créées au cours des étapes précédentes. 2. Développez les connecteurs en fonction de la base de données cible. 3. Configurez les connecteurs pour écouter les sujets Kafka publiés par le moteur Apply. 4. Déployez les connecteurs dans le cluster Amazon EKS.	Développeur d'applications, Architecte cloud, Ingénieur de données

Configurez la continuité des activités et la reprise après sinistre

Tâche	Description	Compétences requises
Définissez des objectifs de reprise après sinistre pour vos applications professionnelles.	1. Définissez les objectifs de RPO et de RTO pour les pipelines CDC en fonction des besoins de votre entreprise et de l'analyse d'impact. 2. Définissez les procédures de communication et de notification pour vous assurer que toutes les parties prenantes sont	Architecte cloud, ingénieur des données, propriétaire de l'application

Tâche	Description	Compétences requises
	informées du plan de reprise après sinistre. 3. Déterminez le budget et les ressources nécessaires pour mettre en œuvre le plan de reprise après sinistre. 4. Documentez les objectifs de reprise après sinistre, y compris les objectifs RPO et RTO.	

Tâche	Description	Compétences requises
Concevez des stratégies de reprise après sinistre basées sur un RTO/RPO défini.	1. Déterminez les stratégies de reprise après sinistre les plus appropriées pour les pipelines CDC en fonction de votre criticité et de vos exigences en matière de reprise. 2. Définissez l'architecture et la topologie de reprise après sinistre. 3. Définissez les procédures de basculement et de retour en arrière pour les pipelines CDC afin de garantir leur basculement rapide et fluide vers la région de sauvegarde. 4. Documentez les stratégies et procédures de reprise après sinistre et assurez-vous que toutes les parties prenantes ont une compréhension claire de la conception.	Architecte cloud, ingénieur de données

Tâche	Description	Compétences requises
Provisionnez des clusters et des configurations de reprise après sinistre.	1. Provisionnez une région AWS secondaire pour la reprise après sinistre. 2. Dans la région AWS secondaire, créez un environnement identique à la région AWS principale. 3. Configurez Apache Kafka MirrorMaker entre les régions principale et secondaire. Pour plus d'informations, consultez la documentation Amazon MSK. 4. Configurez les applications de secours dans la région secondaire. 5. Configurez les réplications de base de données entre les régions principale et secondaire.	DevOps ingénieur, administrateur réseau, architecte cloud

Tâche	Description	Compétences requises
Testez le pipeline du CDC pour la reprise après sinistre.	1. Définissez la portée et les objectifs du test de reprise après sinistre pour le pipeline CDC, y compris les scénarios de test et le RTO à atteindre. 2. Identifiez l'environnement de test et l'infrastructure pour effectuer le test de reprise après sinistre. 3. Préparez les ensembles de données de test et le script pour simuler des scénarios de défaillance. 4. Vérifiez l'intégrité et la cohérence des données pour éviter toute perte de données.	Propriétaire de l'application, ingénieur de données, architecte cloud

Ressources connexes

Ressources AWS

- Amazon DynamoDB
- Expressions de condition avec Amazon DynamoDB
- Amazon EKS
- Amazon EKS Anywhere
- Amazon ElasticCache
- Amazon Keyspaces
- Amazon MSK
- Amazon RDS et Amazon Aurora
- Amazon VPC

Ressources Precisely Connect

- Présentation de Precisely Connect
- Changez la capture de données avec Precisely Connect

Ressources de Confluent

- Consommation de messages multithread avec Apache Kafka Consumer

Planifiez des tâches pour Amazon RDS for PostgreSQL et Aurora PostgreSQL à l'aide de Lambda et Secrets Manager

Créée par Yaser Raja (AWS)

Récapitulatif

Pour les bases de données locales et les bases de données hébergées sur des instances Amazon Elastic Compute Cloud (Amazon EC2), les administrateurs de base de données utilisent souvent l'utilitaire cron pour planifier les tâches.

Par exemple, une tâche d'extraction de données ou une tâche de purge de données peuvent être facilement planifiées à l'aide de cron. Pour ces tâches, les informations d'identification de base de données sont généralement codées en dur ou stockées dans un fichier de propriétés. Toutefois, lorsque vous migrez vers Amazon Relational Database Service (Amazon RDS) ou Amazon Aurora PostgreSQL Compatible Edition, vous ne pouvez plus vous connecter à l'instance hôte pour planifier des tâches cron.

Ce modèle décrit comment utiliser AWS Lambda et planifier des tâches pour AWS Secrets Manager les bases de données compatibles Amazon RDS for PostgreSQL et Aurora PostgreSQL après la migration.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une base de données compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL

Limites

- Une tâche doit être terminée dans les 15 minutes, ce qui correspond au délai d'expiration de la fonction Lambda. Pour les autres limites, consultez la AWS Lambda documentation.
- Le code du job doit être écrit dans un langage compatible avec Lambda.

Architecture

Pile technologique source

Cette pile contient des jobs écrits dans des langages tels que Bash, Python et Java. Les informations d'identification de la base de données sont stockées dans le fichier de propriétés et la tâche est planifiée à l'aide de Linux cron.

Pile technologique cible

Cette pile possède une fonction Lambda qui utilise les informations d'identification stockées dans Secrets Manager pour se connecter à la base de données et effectuer l'activité. La fonction Lambda est lancée à l'intervalle planifié à l'aide d'Amazon CloudWatch Events.

Architecture cible

Outils

- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources. À l'aide de règles simples que vous pouvez configurer rapidement, vous pouvez associer des événements et les acheminer vers une ou plusieurs fonctions ou flux cibles. CloudWatch Events prend conscience des changements opérationnels au fur et à mesure qu'ils se produisent. Il répond à ces changements opérationnels et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état. Vous pouvez également utiliser les CloudWatch événements pour planifier des actions automatisées qui se déclenchent automatiquement à certains moments à l'aide d'expressions cron ou rate.
- AWS Lambda est un service informatique qui vous permet d’exécuter un code sans demander la mise en service ou la gestion des serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous ne payez que pour le temps de calcul que vous consommez ; aucun frais n'est facturé lorsque votre code n'est pas en cours d'exécution. Avec Lambda, vous pouvez exécuter du code pour pratiquement n'importe quel type d'application ou de service principal sans aucune administration. Lambda exécute votre code sur une infrastructure informatique à haute disponibilité et gère toutes les ressources de calcul, y compris la maintenance des serveurs et des systèmes d'exploitation, le provisionnement des capacités et le dimensionnement automatique, la surveillance du code et la journalisation. Il vous suffit de fournir votre code dans l'un des langages pris en charge par Lambda.
- AWS Secrets Managervous aide à protéger les secrets d'accès à vos applications, services et ressources informatiques. Vous pouvez facilement faire pivoter, gérer et récupérer les informations

d'identification de base de données, les clés d'API et d'autres secrets tout au long de leur cycle de vie. Les utilisateurs et les applications récupèrent les secrets en appelant Secrets Manager APIs, ce qui élimine le besoin de coder en dur les informations sensibles en texte brut. Secrets Manager propose une rotation secrète avec intégration intégrée à Amazon RDS, Amazon Redshift et Amazon DocumentDB. Le service est extensible à d'autres types de secrets, notamment les clés d'API et les OAuth jetons. Secrets Manager vous permet de contrôler l'accès aux secrets à l'aide d'autorisations détaillées et d'auditer la rotation des secrets de manière centralisée pour les ressources dans les AWS Cloud services tiers et sur site.

Épopées

Stocker les informations d'identification de la base de données dans Secrets Manager

Tâche	Description	Compétences requises
Créez un utilisateur de base de données pour la fonction Lambda.	Il est recommandé d'utiliser des utilisateurs de base de données distincts pour les différentes parties de votre application. S'il existe déjà un utilisateur de base de données distinct pour vos tâches cron, utilisez-le. Sinon, créez un nouvel utilisateur de base de données. Pour plus d'informations, consultez Gestion des utilisateurs et des rôles PostgreSQLAWS (article de blog).	DBA
Stockez les informations d'identification de la base de données sous forme de secret dans Secrets Manager.	Suivez les instructions de la section Créer un secret de base de données (documentation Secrets Manager).	DBA, DevOps

Créez le code de la fonction Lambda

Tâche	Description	Compétences requises
Choisissez un langage de programmation compatible avec Lambda.	Pour obtenir la liste des langages pris en charge, consultez les environnements d'exécution Lambda (documentation Lambda).	Developer
Écrivez la logique pour récupérer les informations d'identification de la base de données depuis Secrets Manager.	Pour un exemple de code, voir Comment fournir en toute sécurité des informations d'identification de base de données aux fonctions Lambda en utilisant AWS Secrets Manager (article de AWS blog).	Developer
Écrivez la logique pour exécuter l'activité de base de données planifiée.	Migrez votre code existant pour la tâche de planification que vous utilisez sur site vers la fonction Lambda. Pour plus d'informations, consultez Déploiement de fonctions Lambda (documentation Lambda).	Developer

Déployez le code et créez la fonction Lambda

Tâche	Description	Compétences requises
Créez le package de déploiement de la fonction Lambda.	Ce paquet contient le code et ses dépendances. Pour plus d'informations, consultez	Developer

Tâche	Description	Compétences requises
	Packages de déploiement (documentation Lambda).	
Créez la fonction Lambda.	Dans la console Lambda, choisissez Create function, entrez un nom de fonction, choisissez l'environnement d'exécution, puis choisissez Create function.	DevOps
Charger un package de déploiement	Choisissez la fonction Lambda que vous avez créée pour ouvrir sa configuration. Vous pouvez écrire votre code directement dans la section du code ou télécharger votre package de déploiement. Pour télécharger votre package, accédez à la section Code de fonction, choisissez le type d'entrée de code pour télécharger un fichier .zip, puis sélectionnez le package.	DevOps
Configurez la fonction Lambda selon vos besoins.	Par exemple, vous pouvez définir le paramètre Timeout sur la durée prévue pour votre fonction Lambda. Pour plus d'informations, consultez Configuration des options de fonction (documentation Lambda).	DevOps

Tâche	Description	Compétences requises
Définissez les autorisations pour le rôle de fonction Lambda afin d'accéder à Secrets Manager.	Pour obtenir des instructions, consultez la section Utiliser des secrets dans AWS Lambda les fonctions (documentation Secrets Manager).	DevOps
Testez la fonction Lambda.	Lancez la fonction Lambda manuellement pour vous assurer qu'elle fonctionne comme prévu.	DevOps

Planifiez la fonction Lambda à l'aide d'Events CloudWatch

Tâche	Description	Compétences requises
Créez une règle pour exécuter votre fonction Lambda selon une planification.	Planifiez la fonction Lambda à l'aide CloudWatch d'Events. Pour obtenir des instructions, voir Planifier des fonctions Lambda à l'aide d' CloudWatch événements (didacticiel sur CloudWatch les événements).	DevOps

Ressources connexes

- AWS Secrets Manager
- Commencer à utiliser Lambda
- Création d'une règle d' CloudWatch événements qui déclenche un événement
- AWS Lambda Restrictions
- Interrogez votre AWS base de données depuis votre application sans serveur (article de blog)

Envoyer des notifications pour une instance de base de données Amazon RDS for SQL Server à l'aide d'un serveur SMTP sur site et de Database Mail

Créée par Nishad Mankar (AWS)

Récapitulatif

Database Mail (documentation Microsoft) envoie des messages électroniques, tels que des notifications ou des alertes, à partir d'une base de données Microsoft SQL Server à l'aide d'un serveur SMTP (Simple Mail Transfer Protocol). La documentation Amazon Relational Database Service (Amazon RDS) pour Microsoft SQL Server fournit des instructions pour utiliser Amazon Simple Email Service (Amazon SES) comme serveur SMTP pour le courrier de base de données. Pour plus d'informations, consultez Utilisation de Database Mail sur Amazon RDS pour SQL Server. Comme configuration alternative, ce modèle explique comment configurer Database Mail pour envoyer des e-mails depuis une instance de base de données (DB) Amazon RDS for SQL Server en utilisant un serveur SMTP sur site comme serveur de messagerie.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance de base de données Amazon RDS exécutant une édition Standard ou Enterprise de SQL Server
- Adresse IP ou nom d'hôte du serveur SMTP local
- Règle de groupe de sécurité entrant qui autorise les connexions à l'instance de base de données Amazon RDS for SQL Server à partir de l'adresse IP du serveur SMTP
- Une connexion, telle qu'une connexion AWS Direct Connect, entre votre réseau sur site et le cloud privé virtuel (VPC) qui contient l'instance de base de données Amazon RDS

Limites

- Les éditions Express de SQL Server ne sont pas prises en charge.
- Pour plus d'informations sur les limitations, consultez la section Limitations relatives à l'utilisation de Database Mail sur Amazon RDS for SQL Server dans la documentation Amazon RDS.

Versions du produit

- Éditions Standard et Enterprise des versions de SQL Server prises en charge par RDS

Architecture

Pile technologique cible

- Instance de base de données Amazon RDS for SQL Server
- Règle de transfert Amazon Route 53
- Messagerie de base de données
- Serveur SMTP sur site
- Microsoft SQL Server Management Studio (SSMS)

Architecture cible

L'image suivante montre l'architecture cible pour ce modèle. Lorsqu'un événement ou une action déclenche une notification ou une alerte concernant l'instance de base de données, Amazon RDS for SQL Server utilise Database Mail pour envoyer une notification par e-mail. Database Mail utilise le serveur SMTP local pour envoyer le courrier électronique.

Outils

Services AWS

- Amazon Relational Database Service (Amazon RDS) pour Microsoft SQL Server vous aide à configurer, exploiter et dimensionner une base de données relationnelle SQL Server dans le cloud AWS.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.

Autres outils

- Database Mail est un outil qui envoie des messages électroniques, tels que des notifications et des alertes, depuis le moteur de base de données SQL Server aux utilisateurs.
- Microsoft SQL Server Management Studio (SSMS) est un outil de gestion de SQL Server, y compris l'accès, la configuration et l'administration des composants de SQL Server. Dans ce

modèle, vous utilisez SSMS pour exécuter les commandes SQL afin de configurer Database Mail sur une instance de base de données Amazon RDS for SQL Server.

Épopées

Activez la connectivité réseau avec le serveur SMTP local

Tâche	Description	Compétences requises
Supprimez Multi-AZ de l'instance de base de données RDS.	Si vous utilisez une instance de base de données RDS multizone, convertissez-la en instance mono-AZ. Lorsque vous aurez terminé de configurer Database Mail, vous reconvertirez l'instance de base de données en déploiement multi-AZ. La configuration Database Mail fonctionne alors à la fois dans les nœuds principal et secondaire. Pour obtenir des instructions, consultez la section Suppression de Multi-AZ d'une instance de base de données Microsoft SQL Server.	DBA
Créez une liste d'autorisations pour le point de terminaison ou l'adresse IP Amazon RDS sur le serveur SMTP local.	Le serveur SMTP se trouve en dehors du réseau AWS. Sur le serveur SMTP local, créez une liste d'autorisation qui permet au serveur de communiquer avec le point de terminaison sortant ou l'adresse IP de l'instance Amazon RDS ou de l'instance Amazon Elastic	DBA

Tâche	Description	Compétences requises
	Compute Cloud (Amazon EC2) hébergée sur Amazon RDS. Cette procédure varie d'une organisation à l'autre. Pour plus d'informations sur le point de terminaison de l'instance de base de données, consultez Trouver le point de terminaison et le numéro de port de l'instance de base de données.	

Tâche	Description	Compétences requises
Supprimez les restrictions du port 25.	Par défaut, AWS limite le port 25 aux EC2 instances. Pour supprimer la restriction du port 25, procédez comme suit : 1. Connectez-vous avec votre compte AWS, puis ouvrez le formulaire de demande de suppression des restrictions d'envoi d'e-mails. 2. Entrez votre adresse e-mail afin qu'AWS Support puisse vous contacter pour vous tenir au courant de votre demande. 3. Fournissez les informations requises dans le champ Description du cas d'utilisation. 4. Sélectionnez Envoyer. **Note** • Si vous avez des instances dans plusieurs régions AWS, soumettez une demande distincte pour chaque région. • Le traitement de votre demande peut prendre jusqu'à 48 heures.	AWS général

Tâche	Description	Compétences requises
Ajoutez une règle Route 53 pour résoudre les requêtes DNS pour le serveur SMTP.	Utilisez Route 53 pour résoudre les requêtes DNS entre vos ressources AWS et le serveur SMTP sur site. Vous devez créer une règle qui transfère les requêtes DNS au domaine du serveur SMTP, telle que `example.com`. Pour obtenir des instructions, consultez la section Création de règles de transfert dans la documentation de Route 53.	Administrateur réseau

Configurer Database Mail sur l'instance de base de données Amazon RDS for SQL Server

Tâche	Description	Compétences requises
Activez Database Mail.	Créez un groupe de paramètres pour Database Mail, définissez le `database mail xps` paramètre sur`1`, puis associez le groupe de paramètres Database Mail à l'instance de base de données RDS cible. Pour obtenir des instructions, consultez la section Enabling Database Mail dans la documentation Amazon RDS. Ne passez pas à la section Configuration du courrier de base de données dans ces instructions. La configuration du serveur	DBA

Tâche	Description	Compétences requises
	SMTP sur site est différente de celle d'Amazon SES.	
Connectez-vous à l'instance de base de données.	Depuis un hôte Bastion, utilisez Microsoft SQL Server Management Studio (SSMS) pour vous connecter à l'instance de base de données Amazon RDS for SQL Server. Pour obtenir des instructions, voir Connexion à une instance de base de données exécutant le moteur de base de données Microsoft SQL Server. Si vous rencontrez des erreurs, consultez les références de résolution des problèmes de connexion dans la section Ressources associées.	DBA

Tâche	Description	Compétences requises
Créez le profil.	Dans SSMS, entrez l'instruction SQL suivante pour créer le profil de messagerie de base de données. Remplacez les valeurs suivantes : • Pour`profile_name`, entrez un nom pour le nouveau profil. • Pour`description`, entrez une brève description du nouveau profil. Pour plus d'informations sur cette procédure stockée et ses arguments, consultez sysmail_add_profile_sp dans la documentation Microsoft. `EXECUTE msdb.dbo.sysmail_add_profile_sp @profile_name = 'SQL Alerts profile', @description = 'Profile used for sending outgoing notifications using OM SMTP Server.';`	DBA

Tâche	Description	Compétences requises
Ajoutez des directeurs au profil.	Entrez l'instruction SQL suivante pour ajouter des entités publiques ou privées au profil Database Mail. Un principal est une entité qui peut demander des ressources SQL Server. Remplacez les valeurs suivantes : • Pour`profile_name`, entrez le nom du profil que vous avez créé précédemment. • Pour`principal_name`, entrez le nom de l'utilisateur ou du rôle de base de données. Cette valeur doit être mappée à un utilisateur d'authentification SQL Server, à un utilisateur d'authentification Windows ou à un groupe d'authentification Windows. Pour plus d'informations sur cette procédure stockée et ses arguments, consultez sysmail_add_principalprofile_sp dans la documentation Microsoft. `EXECUTE msdb.dbo.sysmail_add_principalprofile_sp`	DBA

Tâche	Description	Compétences requises
	`@profile_name = 'SQL Alerts profile', @principal_name = 'public', @is_default = 1 ;`	

Tâche	Description	Compétences requises
Créez le compte.	Entrez l'instruction SQL suivante pour créer le compte Database Mail. Remplacez les valeurs suivantes : • Pour `account_name`, entrez un nom pour le nouveau compte. • Pour `description`, entrez une brève description du nouveau compte. • Pour `email_address`, entrez l'adresse e-mail à partir de laquelle envoyer les messages de base de données. • Pour `display_address`, entrez un nom d'affichage à utiliser pour les messages sortants de ce compte, par exemple `SQL Server Automated Notification`. Vous pouvez également utiliser la valeur que vous avez saisie `email_address`. • Pour `mailserver_name`, entrez le nom ou l'adresse IP du serveur de messagerie SMTP. • Pour `port`, laissez la valeur de `25`.	DBA

Tâche	Description	Compétences requises

	• Pour`enable_ssl` , laissez la valeur à 1 ou entrez-la `0` si vous ne souhaitez pas que Database Mail chiffre les communications à l'aide du protocole SSL.
	• Pour`username`, entrez le nom d'utilisateur pour vous connecter au serveur de messagerie SMTP. Si le serveur ne nécessite pas d'authentification, entrez`NULL`.
	• Pour`password`, entrez le mot de passe de connexion au serveur de messageri e SMTP. Si le serveur ne nécessite pas d'authent ification, entrez`NULL`.
	
	Pour plus d'informations sur cette procédure stockée et ses arguments, consultez sysmail_add_account_sp dans la documentation Microsoft.
	
	`EXECUTE msdb.dbo.`
	`sysmail_add_accoun`
	`t_sp`
	` @account_name = 'SQL`
	` Alerts account',`
	` @description =`
	` 'Database Mail account`
	` for sending outgoing`
	` notifications.',`	

Tâche	Description	Compétences requises
	`@email_address = 'xyz@example.com', @display_name = 'xyz@example.com', @mailserver_name = 'test_smtp.example.com', @port = 25, @enable_ssl = 1, @username = 'SMTP-username', @password = 'SMTP-password';`	

Tâche	Description	Compétences requises
Ajoutez le compte au profil.	Entrez l'instruction SQL suivante pour ajouter le compte Database Mail au profil Database Mail. Remplacez les valeurs suivantes : • Pour`profile_name` , entrez le nom du profil que vous avez créé précédemment. • Pour`account_name` , entrez le nom du compte que vous avez créé précédemment. Pour plus d'informations sur cette procédure stockée et ses arguments, consultez sysmail_add_profileaccount_sp dans la documentation Microsoft. `EXECUTE msdb.dbo.sysmail_add_profileaccount_sp @profile_name = 'SQL Alerts profile', @account_name = 'SQL Alerts account', @sequence_number = 1;`	DBA

Tâche	Description	Compétences requises
(Facultatif) Ajoutez Multi-AZ à l'instance de base de données RDS.	Si vous souhaitez ajouter le mode multi-AZ avec mise en miroir de base de données (DBM) ou les groupes de disponibilité Always On (AGs), consultez les instructions de la section Ajout du mode multi-AZ à une instance de base de données Microsoft SQL Server.	DBA

Ressources connexes

- Utilisation de Database Mail sur Amazon RDS for SQL Server (documentation Amazon RDS)
- Utilisation des pièces jointes (documentation Amazon RDS)
- Résolution des problèmes de connexion à votre instance de base de données SQL Server (documentation Amazon RDS)
- Impossible de se connecter à l'instance de base de données Amazon RDS (documentation Amazon RDS)

Configuration de la reprise après sinistre pour SAP sur IBM Db2 on AWS

Créée par Ambarish Satarkar (AWS) et Debasis Sahoo (AWS)

Récapitulatif

Ce modèle décrit les étapes à suivre pour configurer un système de reprise après sinistre (DR) pour les charges de travail SAP avec IBM Db2 comme plate-forme de base de données, exécuté sur le cloud Amazon Web Services (AWS). L'objectif est de fournir une solution peu coûteuse pour assurer la continuité des activités en cas de panne.

Le motif utilise l'approche de la veilleuse. En implémentant Pilot Light DR sur AWS, vous pouvez réduire les temps d'arrêt et maintenir la continuité des activités. L'approche pilote met l'accent sur la mise en place d'un environnement de reprise après sinistre minimal dans AWS, comprenant un système SAP et une base de données DB2 de secours, synchronisé avec l'environnement de production.

Cette solution est évolutive. Vous pouvez l'étendre à un environnement de reprise après sinistre à grande échelle selon vos besoins.

Conditions préalables et limitations

Prérequis

- Une instance SAP exécutée sur une instance Amazon Elastic Compute Cloud (Amazon EC2)
- Une base de données IBM Db2
- Système d'exploitation pris en charge par la matrice de disponibilité des produits SAP (PAM)
- Différents noms d'hôte de base de données physiques pour les hôtes de base de données de production et de secours
- Un compartiment Amazon Simple Storage Service (Amazon S3) dans chaque région AWS avec la réplication entre régions (CRR) activée

Versions du produit

- IBM Db2 Database version 11.5.7 ou ultérieure

Architecture

Pile technologique cible

- Amazon EC2
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (peering VPC)
- Amazon Route 53
- IBM Db2 High Availability Disaster Recovery (HADR)

Architecture cible

Cette architecture met en œuvre une solution de reprise après sinistre pour les charges de travail SAP avec Db2 comme plate-forme de base de données. La base de données de production est déployée dans la région AWS 1 et une base de données de secours est déployée dans une deuxième région. La base de données de secours est appelée système DR. La base de données DB2 prend en charge plusieurs bases de données de secours (jusqu'à trois). Il utilise Db2 HADR pour configurer la base de données DR et automatiser l'envoi des journaux entre les bases de données de production et de secours.

En cas de sinistre rendant la région 1 indisponible, la base de données de secours de la région DR prend le rôle de base de données de production. Les serveurs d'applications SAP peuvent être créés à l'avance ou à l'aide d'AWS Elastic Disaster Recovery ou d'une Amazon Machine Image (AMI) pour répondre aux exigences relatives aux objectifs de temps de restauration (RTO). Ce modèle utilise une AMI.

Db2 HADR implémente une configuration de veille de production, dans laquelle la production agit en tant que serveur principal et où tous les utilisateurs y sont connectés. Toutes les transactions sont écrites dans des fichiers journaux, qui sont transférés vers le serveur de secours à l'aide du protocole TCP/IP. Le serveur de secours met à jour sa base de données locale en reportant les enregistrements du journal transférés, ce qui permet de garantir sa synchronisation avec le serveur de production.

Le peering VPC est utilisé pour que les instances de la région de production et de la région DR puissent communiquer entre elles. Amazon Route 53 dirige les utilisateurs finaux vers des applications Internet.

1. Créez une AMI du serveur d'applications dans la région 1 et copiez-la dans la région 2. Utilisez l'AMI pour lancer des serveurs dans la région 2 en cas de sinistre.

2. Configurez la réplication Db2 HADR entre la base de données de production (dans la région 1) et la base de données de secours (dans la région 2).
3. Modifiez le type d' EC2 instance pour qu'il corresponde à l'instance de production en cas de sinistre.
4. Dans la région 1, `LOGARCHMETH1` est défini sur`db2remote: S3 path`.
5. Dans la région 2, `LOGARCHMETH1` est défini sur`db2remote: S3 path`.
6. La réplication entre régions est effectuée entre les compartiments S3.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS. Ce modèle utilise le peering VPC.

Bonnes pratiques

- Le réseau joue un rôle clé dans le choix du mode de réplication HADR. Pour la reprise après sinistre dans les régions AWS, nous vous recommandons d'utiliser le mode DB2 HADR ASYNC ou SUPERASYNC.
- Pour plus d'informations sur les modes de réplication pour Db2 HADR, consultez la documentation IBM.
- Vous pouvez utiliser la console de gestion AWS ou l'interface de ligne de commande AWS (AWS CLI) pour créer une nouvelle AMI de votre système SAP existant. Vous pouvez ensuite utiliser l'AMI pour récupérer votre système SAP existant ou pour créer un clone.
- AWS Systems Manager Automation peut vous aider à effectuer les tâches courantes de maintenance et de déploiement des EC2 instances et des autres ressources AWS.

- AWS fournit plusieurs services natifs pour surveiller et gérer votre infrastructure et vos applications sur AWS. Des services tels qu'Amazon CloudWatch et AWS CloudTrail peuvent être utilisés pour surveiller votre infrastructure sous-jacente et vos opérations d'API, respectivement. Pour plus de détails, consultez SAP on AWS — IBM Db2 HADR with Pacemaker.

Épopées

Préparez l'environnement

Tâche	Description	Compétences requises
Vérifiez le système et les journaux.	1. Vérifiez que le système de production SAP on Db2 est configuré. 2. Vérifiez que la sauvegarde des journaux est activée et configurée pour enregistrer les journaux dans le compartiment S3. Cela peut être vérifié par le paramètre `LOGARCHMETH1` Db2. 3. Créez une AMI du serveur d'applications supplémentaire.	Administrateur AWS, administrateur SAP Basis

Configuration des serveurs et de la réplication

Tâche	Description	Compétences requises
Créez le SAP et les serveurs de base de données.	1. Pour déployer l'infrastructure pour la région DR, utilisez un CloudFormation script AWS ou une AMI de l'instance de production. Dans le cadre de l'approche pilote, vous pouvez	Administrateur SAP Basis

Tâche	Description	Compétences requises
	utiliser une EC2 instance plus petite appartenant à la même famille que l'instance de production. Par exemple, si le type de votre instance de productio n est `r6i.12xlarge` , vous pouvez utiliser le type d'`r6i.xlarge` instance pour le build DR. Assurez-vous toutefois d'allouer la même capacité de stockage sur l'instance DR pour restaurer la sauvegarde de la base de données de production. 2. Créez des points de montage Amazon Elastic File System (Amazon EFS) pour `/sapmnt/<SID>/` le système principal et assurez-vous qu'il est configuré pour être répliqué depuis le système principal. 3. Effectuez une sauvegarde COMPLÈTE de la base de données (en ligne ou hors ligne) depuis le système de production. Vous utiliserez cette sauvegarde pour créer la base de données DR. 4. Dans le système DR, utilisez la méthode de copie du système SAP Software	

Tâche	Description	Compétences requises
	Provisioning Manager (SWPM) avec Utilisation de la copie du système dans le backup/restore for HA/DR but de créer le système DR SAP. 5. À la demande de SWPM, restaurez la base de données dans DR avec la sauvegarde que vous avez prise lors de la productio n. La base de données DR sera dans l'état en attente de reconduction. L'état en attente de report est défini par défaut une fois la sauvegarde complète restaurée. L'état en attente de report indique que la base de données est en cours de restauration et que certaines modifications devront peut-être être appliquées. Pour plus d'informations, consultez la documentation IBM.	

Tâche	Description	Compétences requises
Vérifiez la configuration.	1. Pour configurer l'archivage des journaux pour HADR, les bases de données de production et de reprise après sinistre doivent être en mesure de récupérer les journaux automatiquement à partir de tous les emplacements d'archivage des journaux. Vérifiez que le `LOGARCHMETH1` paramètre de la base de données DR est défini au même emplacement que dans la base de données de production. Si le même emplacement n'est pas accessible en raison de limitations régionales, assurez-vous que le système DR peut récupérer automatiquement les journaux depuis le système principal. 2. Pour activer les ports TCP/IP afin de permettre la réplication de base de données, modifiez les hôtes de production et de reprise après sinistre `/etc/services` en ajoutant les deux entrées suivantes. Dans le code, `<SID>` fait référence à l'ID système (SID) de la	Administrateur AWS, administrateur SAP Basis

Tâche	Description	Compétences requises

	base de données DB2 (par exemple,PR1).
	
	`<SID>_HADR_1 55001/tcp # DB2 HADR Port1`
	`<SID>_HADR_2 55002/tcp # DB2 HADR Port2`
	
	Vérifiez que les deux ports autorisent le trafic entrant et sortant entre le port principal et le port de secours.
	3. Vérifiez `/etc/hosts` les hôtes de production et de reprise après sinistre pour vérifier que les noms d'hôtes de production et de secours pointent vers les adresses IP correctes.	

Tâche	Description	Compétences requises

Configurez la réplication de la base de données de productio n vers la base de données DR (en utilisant le mode ASYNC).	1. Dans la base de données de production, exécutez les commandes suivantes pour mettre à jour les paramètre s.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	2. Dans la base de données DR, exécutez les
		Administrateur SAP Basis

Tâche	Description	Compétences requises

	commandes suivantes pour mettre à jour les paramètres.
	
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_HOST HOST2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_LOCAL_SVC <SID>_HADR_2`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_HOST HOST1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_SVC <SID>_HADR_1`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_REMOTE_INST db2<sid>`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_TIMEOUT 120`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SYNCMODE ASYNC`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_SPOOL_LIMIT 1000`
	`db2 UPDATE DB CFG FOR <SID> USING HADR_PEER_WINDOW 240`
	`db2 UPDATE DB CFG FOR <SID> USING indexrec RESTART logindexbuild ON`
	
	Ces paramètres sont nécessaires pour fournir des informations relatives au HADR aux deux bases	

Tâche	Description	Compétences requises

	de données. Dans la base de données DB2, le HADR est activé en fonction des valeurs de chacun des paramètres définis précédemment. Pour plus d'informations sur ces paramètres, consultez la documentation IBM.
	3. Démarrez d'abord HADR sur la base de données de secours nouvellement créée à l'aide de la commande suivante.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as standby`
	4. Démarrez HADR sur la base de données de production à l'aide de la commande suivante.
	`db2 deactivate db <SID>`
	`db2 start hadr on db <SID> as primary`
	5. Vérifiez si les bases de données DB2 de production et de secours sont synchronisées et si l'expédition des journaux est en cours.	

Tâche	Description	Compétences requises
	Pour surveiller l'état de réplication HADR, utilisez la db2pd commande suivante. `db2pd -d <SID> -hadr` Pour plus d'informations sur la surveillance du HADR, consultez la documentation IBM.	

Tester les tâches de reprise après sinistre

Tâche	Description	Compétences requises
Planifiez les interruptions de production pour le test de reprise après sinistre.	Assurez-vous de planifier les interruptions de service requises dans l'environnement de production pour tester le scénario de reprise après sinistre.	Administrateur SAP Basis
Créez un utilisateur de test.	Créez un utilisateur de test (ou toute modification de test) qui peut être validé sur l'hôte DR pour confirmer la réplication du journal après le basculement de DR.	Administrateur SAP Basis
Sur la console, arrêtez les EC2 instances de production.	Un arrêt indécent est initié au cours de cette étape pour imiter un scénario de catastrophe.	Administrateur système AWS

Tâche	Description	Compétences requises
Augmentez la taille de l' EC2 instance DR en fonction des exigences.	Sur la EC2 console, modifiez le type d'instance dans la région DR. 1. Arrêter l'instance : si l'instance est en cours d'exécution, vous devez l'arrêter avant de pouvoir modifier son type d'instance. Sur la EC2 console, sélectionnez l'instance, puis cliquez sur Stop. 2. Modifiez le type d'instance : sur la EC2 console, sélectionnez l'instance, puis choisissez Actions, Paramètres de l'instance, Modifier le type d'instance. Sélectionnez le type d'instance qui correspond à l'instance principale, puis choisissez Appliquer. 3. Démarrez l'instance : une fois le changement de type d'instance terminé, démarrez l'instance depuis la EC2 console en sélectionnant l'instance puis en choisissant Start. 4. Pour démarrer la base de données DB2, utilisez la commande suivante. `db2start`	Administrateur SAP Basis

Tâche	Description	Compétences requises
	db2 start HADR on db <SID> as standby	

Tâche	Description	Compétences requises

Initiez le rachat.	À partir du système DR (`host2`), lancez le processus de prise de contrôle et affichez la base de données DR en tant que base de données principale.
	
	`db2 takeover hadr on database <SID> by force`
	
	Vous pouvez éventuellement définir les paramètres suivants pour ajuster automatiquement l'allocation de mémoire de la base de données en fonction du type d'instance. La `INSTANCE_MEMORY` valeur peut être décidée en fonction de la portion de mémoire dédiée à allouer à la base de données Db2.
	
	`db2 update db cfg for <SID> using INSTANCE_MEMORY <FIXED VALUE> IMMEDIATE;`
	`db2 get db cfg for <SID> | grep -i DATABASE_MEMORY AUTOMATIC IMMEDIATE;`
	`db2 update db cfg for <SID> using self_tuning_mem ON IMMEDIATE;`
	
	Vérifiez la modification à l'aide des commandes suivantes.
		Administrateur SAP Basis

Tâche	Description	Compétences requises
	`db2 get db cfg for <SID> | grep -i MEMORY` `db2 get db cfg for <SID> | grep -i self_tuning_mem`	
Lancez le serveur d'applications pour SAP dans la région DR.	À l'aide de l'AMI que vous avez créée pour le système de production, lancez un nouveau serveur d'applications supplémentaire dans la région DR.	Administrateur SAP Basis
Effectuez la validation avant de démarrer l'application SAP.	1. Validez les `/etc/fstab` entrées `/etc/hosts` et. 2. `/sapmnt/<SID>/` À monter sur le système DR. 3. Vérifiez que le système de fichiers DR `/sapmnt/<SID>/` est synchronisé avec la production `/sapmnt/<SID>/` . 4. Connectez-vous à `<sid>adm` l'utilisateur`R3trans -d`, exécutez et vérifiez le résultat dans le `trans.log` fichier. Le `trans.log` fichier est généré au même endroit où vous avez exécuté la `R3trans -d` commande.	Administrateur AWS, administrateur SAP Basis

Tâche	Description	Compétences requises

Démarrez l'application SAP sur le système DR.	Démarrez l'application SAP sur le système DR en utilisant `<sid>adm` user. Utilisez le code suivant, qui XX représente le numéro d'instance de votre serveur SAP ABAP SAP Central Services (ASCS) et YY le numéro d'instance de votre serveur d'applications SAP.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
		Administrateur SAP Basis

Effectuez la validation SAP.	Ceci est effectué sous forme de test DR pour fournir des preuves ou pour vérifier le succès de la réplication des données dans la région DR.	Ingénieur de test

Réaliser des tâches de reprise après sinistre

Tâche	Description	Compétences requises
Démarrez le SAP de production et les serveurs de base de données.	Sur la console, démarrez les EC2 instances qui hébergent SAP et la base de données	Administrateur SAP Basis

Tâche	Description	Compétences requises
	dans le système de productio n.	

Tâche	Description	Compétences requises

Démarrez la base de données de production et configurez HADR.	Connectez-vous au système de production (`host1`) et vérifiez que la base de données est en mode de restauration à l'aide de la commande suivante.
	`db2start`
	`db2 start HADR on db P3V as standby`
	`db2 connect to <SID>`
	Vérifiez que le statut HADR est`connected` . L'état de réplication doit être`peer`.
	`db2pd -d <SID> -hadr`
	Si la base de données n'est pas incohérente `connected` et n'est pas en `peer` état, une sauvegarde et une restauration peuvent être nécessaires pour synchroniser la base de données avec la base de données actuellement active (`host2`dans la région DR). `host1` Dans ce cas, restaurez la sauvegarde de base de données de la base de données de la région `host2` DR vers la base de données de la région `host1` de production.
		Administrateur SAP Basis

Tâche	Description	Compétences requises
Replacez la base de données dans la région de production.	Dans un business-as-usual scénario normal, cette étape est exécutée lors d'un arrêt planifié. Les applications exécutées sur le système DR sont arrêtées et la base de données est renvoyée dans la région de production (région 1) pour reprendre les opérations depuis la région de production. 1. Connectez-vous au serveur d'applications SAP dans la région DR et arrêtez l'application SAP. 2. Démontez `/sapmnt/<SID>` du système DR en vous assurant que les modifications sont répliquées à l'envers dans le système `/sapmnt/<SID>` de production. 3. Connectez-vous au serveur de base de données (`host1`) dans la région de production et effectuez la prise de contrôle. `db2 takeover hadr on database <SID>` 4. Vérifiez l'état du HADR : `HADR_ROLE` il doit être `PRIMARY` activé `host1` et `StandBy` activé`host2`.	Administrateur SAP Basis

Tâche	Description	Compétences requises
	`db2pd -d <SID> -hadr`	
Effectuez la validation avant de démarrer l'application SAP.	1. Validez les `/etc/fstab` entrées `/etc/hosts` et. 2. Monter `/sapmnt/<SID>/` sur le système de production. 3. Assurez-vous qu'il est synchronisé avec le système DR`/sapmnt/<SID>/` . 4. Connectez-vous à `<sid>adm` l'utilisateur`R3trans -d`, exécutez et vérifiez le résultat dans le `trans.log` fichier. Le `trans.log` fichier est généré au même endroit où vous avez exécuté la `R3trans -d` commande.	Administrateur AWS, administrateur SAP Basis

Tâche	Description	Compétences requises

Démarrez l'application SAP.	1. Démarrez l'application SAP sur le système de production à l'aide de `<sid>adm` l'utilisateur. Utilisez le code suivant, qui XX représente le numéro d'instance de votre serveur SAP ASCS et YY le numéro d'instance de votre serveur d'applications SAP.
	`sapconrol -nr XX -function StartService <SID>`
	`sapconrol -nr XX -function StartSystem`
	`sapconrol -nr YY -function StartService <SID>`
	`sapconrol -nr YY -function StartSystem`
	2. Pour vérifier que les serveurs d'applications sont disponibles, connectez-vous à SAP et effectuez des vérifications à l'aide du SICK et SM51 des transactions.
		Administrateur SAP Basis

Résolution des problèmes

Problème	Solution
Fichiers journaux et commandes clés pour résoudre les problèmes liés au HADR	• `db2 get db cfg | grep -i hadr`

Problème	Solution
	• `db2pd -d sid -hadr` • `Db2diag.log` (Ce fichier se trouve généralement dans le `db2dump` répertoir e et le `db2dump` chemin est défini par le paramètre`DIAGPATH`.)
Note SAP pour la résolution des problèmes HADR sur Db2 UDB	Reportez-vous à la note SAP 1154013 - DB6 : Problèmes de base de données dans l'environnement HADR. (Vous avez besoin des informations d'identification du portail SAP pour accéder à cette note.)

Ressources connexes

- Approches de reprise après sinistre pour les bases de données DB2 sur AWS (article de blog)
- SAP on AWS — IBM DB2 HADR avec stimulateur cardiaque
- Procédure étape par étape pour configurer la réplication HADR entre les bases de données DB2
- Wiki DHR DB2

Informations supplémentaires

À l'aide de ce modèle, vous pouvez configurer un système de reprise après sinistre pour un système SAP exécuté sur la base de données DB2. En cas de sinistre, l'entreprise doit être en mesure de poursuivre ses activités dans les limites de vos objectifs de temps de reprise (RTO) et de point de reprise (RPO) définis :

- Le RTO est le délai maximum acceptable entre l'interruption du service et le rétablissement du service. Elle détermine ce qui est considéré comme étant un créneau de temps acceptable d’indisponibilité du service.
- Le RPO est la durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l’interruption du service.

Pour en FAQs savoir plus sur le HADR, consultez la note SAP #1612105 - DB6 : FAQ sur Db2 High Availability Disaster Recovery (HADR). (Vous avez besoin des informations d'identification du portail SAP pour accéder à cette note.)

Configurer un pipeline CI/CD pour la migration de base de données à l'aide de Terraform

Créée par le Dr Rahul Sharad Gaikwad (AWS), Aarti Rajput (AWS), Ashish Bhatt (AWS), Aniket Dekate (AWS), Naveen Suthar (AWS), Nadeem Rahaman (AWS), Ruchika Modi (AWS) et Tamilselvan P (AWS)

Récapitulatif

Ce modèle consiste à établir un pipeline d'intégration et de déploiement continus (CI/CD) pour gérer les migrations de bases de données de manière fiable et automatisée. Il couvre le processus de mise en service de l'infrastructure nécessaire, de migration des données et de personnalisation des modifications de schéma à l'aide de Terraform, un outil d'infrastructure en tant que code (IaC).

Plus précisément, le modèle met en place un pipeline CI/CD pour migrer une base de données Microsoft SQL Server sur site vers Amazon Relational Database Service (Amazon RDS) sur. AWS Vous pouvez également utiliser ce modèle pour migrer une base de données SQL Server située sur une machine virtuelle (VM) ou dans un autre environnement cloud vers Amazon RDS.

Ce modèle permet de relever les défis suivants liés à la gestion et au déploiement de bases de données :

- Les déploiements manuels de bases de données prennent du temps, sont sujets aux erreurs et manquent de cohérence entre les environnements.
- La coordination du provisionnement de l'infrastructure, des migrations de données et des modifications de schéma peut s'avérer complexe et difficile à gérer.
- Garantir l'intégrité des données et minimiser les temps d'arrêt lors des mises à jour des bases de données est crucial pour les systèmes de production.

Ce modèle offre les avantages suivants :

- Rationalise le processus de mise à jour et de déploiement des modifications de base de données en mettant en œuvre un pipeline CI/CD pour les migrations de bases de données. Cela réduit le risque d'erreurs, garantit la cohérence entre les environnements et minimise les temps d'arrêt.
- Contribue à améliorer la fiabilité, l'efficacité et la collaboration. Permet d'accélérer la mise sur le marché et de réduire les temps d'arrêt lors des mises à jour des bases de données.
- Vous aide à adopter DevOps des pratiques modernes de gestion de base de données, ce qui améliore l'agilité, la fiabilité et l'efficacité de vos processus de livraison de logiciels.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Terraform 0.12 ou version ultérieure installé sur votre machine locale (pour les instructions, consultez la documentation Terraform)
- Terraform AWS Provider version 3.0.0 ou ultérieure à partir de HashiCorp (voir le GitHub référentiel de ce fournisseur)
- Politique de moindre privilège AWS Identity and Access Management (IAM) (voir le billet de blog Techniques de rédaction de politiques IAM de moindre privilège)

Architecture

Ce modèle implémente l'architecture suivante, qui fournit l'infrastructure complète pour le processus de migration de base de données.

Dans cette architecture :

- La base de données source est une base de données SQL Server installée sur site, sur une machine virtuelle (VM) ou hébergée par un autre fournisseur de cloud. Le schéma suppose que la base de données source se trouve dans un centre de données local.
- Le centre de données sur site est connecté via un VPN ou une AWS Direct Connect connexion. AWS Cela garantit des communications sécurisées entre la base de données source et l' AWS infrastructure.
- La base de données cible est une base de données Amazon RDS hébergée dans le cloud privé virtuel (VPC) à l'aide d'un AWS pipeline de provisionnement de base de données.
- AWS Database Migration Service (AWS DMS) réplique votre base de données locale vers. AWS Il est utilisé pour configurer la réplication de la base de données source vers la base de données cible.

Le schéma suivant montre l'infrastructure configurée à différents niveaux du processus de migration de base de données, qui implique le provisionnement, la AWS DMS configuration et la validation.

Dans le cadre de ce processus :

- Le pipeline de validation valide toutes les vérifications. Le pipeline intégré passe à l'étape suivante lorsque toutes les validations nécessaires sont terminées.
- Le pipeline de provisionnement de base de données comprend différentes AWS CodeBuild étapes qui exécutent des actions Terraform sur le code Terraform fourni pour la base de données. Lorsque ces étapes sont terminées, il déploie les ressources dans la cible Compte AWS.
- Le AWS DMS pipeline comprend différentes CodeBuild étapes qui effectuent des tests, puis fournissent l' AWS DMS infrastructure pour effectuer la migration à l'aide d'IaC.

Outils

Services AWS et outils

- AWS CodeBuildest un service d'intégration continue entièrement géré qui compile le code source, exécute des tests et produit des ready-to-deploy progiciels.
- AWS CodePipelineest un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le. AWS Cloud
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre évolutivité, disponibilité des données, sécurité et performances.
- AWS Database Migration Service (AWS DMS) vous aide à migrer les banques de données vers AWS Cloud ou entre des combinaisons de configurations cloud et sur site.

Autres services

- Terraform est un outil IaC HashiCorp qui vous aide à créer et à gérer des ressources sur site et dans le cloud.

Référentiel de code

Le code de ce modèle est disponible dans le DevOps framework de migration de GitHub base de données à l'aide du référentiel d'exemples Terraform.

Bonnes pratiques

- Mettez en œuvre des tests automatisés pour la migration de votre base de données afin de vérifier l'exactitude des modifications de schéma et l'intégrité des données. Cela inclut les tests unitaires, les tests d'intégration et les end-to-end tests.
- Mettez en œuvre une stratégie de sauvegarde et de restauration robuste pour vos bases de données, en particulier avant la migration. Cela garantit l'intégrité des données et fournit une option de secours en cas de panne.
- Mettez en œuvre une stratégie de restauration robuste pour annuler les modifications apportées à la base de données en cas de défaillance ou de problème lors de la migration. Cela peut impliquer de revenir à un état de base de données antérieur ou de rétablir des scripts de migration individuels.
- Configurez des mécanismes de surveillance et de journalisation pour suivre la progression et l'état des migrations de bases de données. Cela vous permet d'identifier et de résoudre rapidement les problèmes.

Épopées

Configurez votre poste de travail local

Tâche	Description	Compétences requises
Installez et configurez Git sur votre poste de travail local.	Installez et configurez Git sur votre poste de travail local en suivant les instructions de la documentation Git.	DevOps ingénieur
Créez un dossier de projet et ajoutez les fichiers du GitHub référentiel.	1. Ouvrez le GitHub référentiel pour ce modèle. 2. Choisissez Code pour voir les options de clonage, puis copiez l'URL fournie dans l'onglet HTTPS. 3. Créez un dossier pour votre projet sur votre poste de travail.	DevOps ingénieur

Tâche	Description	Compétences requises

	4. Ouvrez un terminal et accédez à ce dossier.
	5. Clonez le GitHub dépôt :
	`git clone <github-repository-url>`
	où se `<github-repository-url>` trouve l'URL que vous avez copiée à l'étape 2.
	6. Lorsque le clonage est terminé, accédez au dépôt cloné dans le dossier de votre projet :
	`cd <folder-name>/aws-terraform-db-migration-framework-samples`
	7. Ouvrez ce projet dans un environnement de développement intégré (IDE) de votre choix.	

Provisionner l'architecture cible

Tâche	Description	Compétences requises
Mettez à jour les paramètres requis.	Le `ssm-parameters.sh` fichier enregistre tous les AWS Systems Manager paramètres requis. Vous pouvez configurer ces paramètres avec les	DevOps ingénieur

Tâche	Description	Compétences requises
	valeurs personnalisées de votre projet. Dans le `setup/db-ssm-params` dossier de votre station de travail locale, ouvrez le `ssm-parameters.sh` fichier et définissez ces paramètres avant d'exécuter le pipeline CI/CD.	
Initialisez la configuration Terraform.	Dans le `db-cicd-integration` dossier, entrez la commande suivante pour initialiser votre répertoire de travail contenant les fichiers de configuration Terraform : `terraform init`	DevOps ingénieur
Prévisualisez le plan Terraform.	Pour créer un plan Terraform, entrez la commande suivante : `terraform plan -var-file="terraform.sample"` Terraform évalue les fichiers de configuration pour déterminer l'état cible des ressources déclarées. Il compare ensuite l'état cible à l'état actuel et crée un plan.	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez le plan.	Passez en revue le plan et confirmez qu'il configure l'architecture requise dans votre cible Compte AWS.	DevOps ingénieur
Déployez la solution.	1. Entrez la commande suivante pour appliquer le plan : `terraform apply -var-file="terraform.sample"` 2. Saisissez `yes` pour confirmer. Terraform crée, met à jour ou détruit l'infrastructure pour atteindre l'état cible déclaré dans les fichiers de configuration. Pour plus d'informations sur la séquence, consultez la section Architecture de ce modèle.	DevOps ingénieur

Vérification du déploiement

Tâche	Description	Compétences requises
Validez le déploiement.	Vérifiez l'état du `db-cicd-integration` pipeline pour confirmer que la migration de la base de données est terminée.	DevOps ingénieur

Tâche	Description	Compétences requises
	1. Connectez-vous à la AWS CodePipeline console AWS Management Console, puis ouvrez-la. 2. Dans le volet de navigation, sélectionnez Pipelines. 3. Choisissez le `db-cicd-integration` pipeline. 4. Vérifiez que l'exécution du pipeline s'est terminée avec succès.	

Nettoyer l'infrastructure après utilisation

Tâche	Description	Compétences requises
Nettoyez l'infrastructure.	1. Une fois votre projet terminé, nettoyez l'infrastructure que vous avez créée à l'aide de la commande : `terraform destroy --var-file=terraform.sample` 2. Saisissez `yes` pour confirmer.	DevOps ingénieur

Ressources connexes

AWS documentation

- Commencer à utiliser un produit Terraform

Documentation Terraform

- Installation de Terraform
- Configuration du backend Terraform
- Documentation du fournisseur Terraform AWS

Configuration d'une architecture HA/DR pour Oracle E-Business Suite sur Amazon RDS Custom avec une base de données de secours active

Créée par Simon Cunningham (AWS) et Nitin Saxena

Récapitulatif

Ce modèle décrit comment vous pouvez concevoir votre solution Oracle E-Business sur Amazon Relational Database Service (Amazon RDS) Custom pour la haute disponibilité (HA) et la reprise après sinistre (DR) en configurant une base de données de répliques en lecture personnalisée Amazon RDS dans une autre zone de disponibilité Amazon Web Services (AWS) et en la convertissant en base de données de secours active. La création de la réplique de lecture personnalisée Amazon RDS est entièrement automatisée via l'AWS Management Console.

Ce modèle ne décrit pas les étapes à suivre pour ajouter des niveaux d'application supplémentaires et des systèmes de fichiers partagés, qui peuvent également faire partie d'une architecture HA/DR. Pour plus d'informations sur ces sujets, consultez les notes de support Oracle suivantes : 1375769.1, 1375670.1 et 1383621.1 (section 5, Options de clonage avancées). (L'accès nécessite un compte Oracle Support.)

Pour migrer le système E-Business Suite vers une architecture mono-AZ à niveau unique sur Amazon Web Services (AWS), consultez le modèle Migrer Oracle E-Business Suite vers Amazon RDS Custom.

Oracle E-Business Suite est une solution de planification des ressources d'entreprise (ERP) permettant d'automatiser les processus à l'échelle de l'entreprise tels que les finances, les ressources humaines, les chaînes d'approvisionnement et la fabrication. Il possède une architecture à trois niveaux : client, application et base de données. Auparavant, vous deviez exécuter votre base de données E-Business Suite sur une instance Amazon Elastic Compute Cloud EC2 (Amazon) autogérée, mais vous pouvez désormais bénéficier d'Amazon RDS Custom.

Conditions préalables et limitations

Prérequis

- Une installation existante de E-Business Suite sur Amazon RDS Custom ; voir le modèle Migrer Oracle E-Business Suite vers Amazon RDS Custom

- Si vous souhaitez remplacer la réplique en lecture seule et l'utiliser pour transférer les rapports au serveur de secours, une licence de base de données Oracle Active Data Guard (voir la liste des prix commerciaux d'Oracle Technology)

Limites

- Limitations et configurations non prises en charge pour les bases de données Oracle sur Amazon RDS Custom
- Limitations associées aux répliques de lecture Amazon RDS Custom for Oracle

Versions du produit

Pour les versions de base de données Oracle et les classes d'instances prises en charge par Amazon RDS Custom, consultez Exigences et limites relatives à Amazon RDS Custom pour Oracle.

Architecture

Le schéma suivant illustre une architecture représentative de la suite E-Business sur AWS qui inclut plusieurs zones de disponibilité et niveaux d'application dans une configuration active/passive. La base de données utilise une instance de base de données Amazon RDS Custom et une réplique de lecture Amazon RDS Custom. La réplique en lecture utilise Active Data Guard pour se répliquer vers une autre zone de disponibilité. Vous pouvez également utiliser la réplique de lecture pour décharger le trafic de lecture sur la base de données principale et à des fins de création de rapports.

Pour plus d'informations, consultez la section Travailler avec des répliques de lecture pour Amazon RDS Custom pour Oracle dans la documentation Amazon RDS.

La réplique de lecture personnalisée Amazon RDS est créée par défaut telle qu'elle est montée. Toutefois, si vous souhaitez décharger certaines de vos charges de travail en lecture seule vers la base de données de secours afin de réduire la charge sur votre base de données principale, vous pouvez modifier manuellement le mode des répliques montées en lecture seule en suivant les étapes de la section Epics. Un cas d'utilisation typique consiste à exécuter vos rapports à partir de la base de données de secours. Le passage en lecture seule nécessite une licence de base de données de secours active.

Lorsque vous créez une réplique en lecture sur AWS, le système utilise le courtier Oracle Data Guard en guise de couverture. Cette configuration est automatiquement générée et configurée en mode Performances maximales comme suit :

```
DGMGRL> show configuration
Configuration - rds_dg
  Protection Mode: MaxPerformance
  Members:
  vis_a - Primary database
    vis_b - Physical standby database
Fast-Start Failover: DISABLED
Configuration Status:
SUCCESS   (status updated 58 seconds ago)
```

Outils

Services AWS

- Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents. Il automatise les tâches et les opérations d'administration des bases de données tout en vous permettant, en tant qu'administrateur de base de données, d'accéder à votre environnement de base de données et de votre système d'exploitation et de les personnaliser.

Autres outils

- Oracle Data Guard est un outil qui vous aide à créer et à gérer des bases de données de secours Oracle. Ce modèle utilise Oracle Data Guard pour configurer une base de données de secours active sur Amazon RDS Custom.

Épopées

Création d'un réplica en lecture

Tâche	Description	Compétences requises
Créez une réplique en lecture de l'instance de base de données personnalisée Amazon RDS.	Pour créer une réplique en lecture, suivez les instructions de la documentation Amazon RDS et utilisez l'instance de base de données personnal	DBA

Tâche	Description	Compétences requises
	isée Amazon RDS que vous avez créée (voir la section Conditions préalables) comme base de données source. Par défaut, la réplique de lecture personnalisée Amazon RDS est créée en tant que support physique et est à l'état monté. Cela est intentionnel pour garantir la conformité avec la licence Oracle Active Data Guard. Suivez les étapes suivantes pour convertir la réplique en lecture seule en mode lecture seule.	

Remplacez le réplica en lecture seule par un mode veille actif en lecture seule

Tâche	Description	Compétences requises
Connectez-vous à la réplique de lecture personnalisée Amazon RDS.	Utilisez les commandes suivantes pour convertir votre base de données de secours physique en base de données de secours active. ⚠ Important Ces commandes nécessitent une licence Oracle Active Standby. Pour obtenir une licence, contactez	DBA

Tâche	Description	Compétences requises

	votre représentant Oracle.
	
	`$ sudo su - rdsdb`
	`-bash-4.2$ sql`
	`SQL> select process,s`
	`tatus,sequence# from v`
	`$managed_standby;`
	
	`PROCESS STATUS`
	`SEQUENCE#`
	`--------- ------------`
	`----------`
	`ARCH CLOSING`
	`3956`
	`ARCH CONNECTED`
	`0`
	`ARCH CLOSING`
	`3955`
	`ARCH CLOSING`
	`3957`
	`RFS IDLE`
	`0`
	`RFS IDLE`
	`3958`
	`MRP0 APPLYING_LOG`
	`3958`
	`SQL> select name,`
	`database_role,`
	`open_mode from v`
	`$database;`
	
	`NAME DATABASE_`
	`ROLE OPEN_MODE`
	`--------- ---------`
	`------- ---------`
	`----------`
	`VIS PHYSICAL`
	`STANDBY MOUNTED`	

Tâche	Description	Compétences requises
	SQL> alter database recover managed standby database cancel; Database altered. Open the standby database SQL> alter database open; Database altered. SQL> select name, database_role, open_mode from v $database; NAME DATABASE_ ROLE OPEN_MODE --------- --------- ------- --------- ----------- VIS PHYSICAL STANDBY READ ONLY	

Tâche	Description	Compétences requises

Démarrez la restauration multimédia avec l'application du journal en temps réel.	Pour activer la fonctionn alité d'application du journal en temps réel, utilisez les commandes suivantes. Ils convertissent et valident la base de données de secours (réplique en lecture) en tant que base de données de secours active, afin que vous puissiez vous connecter et exécuter des requêtes en lecture seule.
	`SQL>  alter database recover managed standby database using current logfile disconnect from session;`
	`Database altered`
		DBA

Vérifiez l'état de la base de données.	Pour vérifier l'état de la base de données, utilisez la commande suivante.
	`SQL> select name, database_role, open_mode from v$database;`
	`NAME  DATABASE_ROLE  OPEN_MODE`
	`--------- ---------- ----------`
	`VIS  PHYSICAL  STANDBY READ ONLY WITH APPLY`
		DBA

Tâche	Description	Compétences requises

Cochez le mode Rétablir l'application.	Pour activer le mode Redo Apply, utilisez la commande suivante.
	
	`SQL> select process,s tatus,sequence# from v $managed_standby;`
	`PROCESS STATUS SEQUENCE#`
	`--------- ------------ ----------`
	`ARCH CLOSING 3956`
	`ARCH CONNECTED 0`
	`ARCH CLOSING 3955`
	`ARCH CLOSING 3957`
	`RFS IDLE 0`
	`RFS IDLE 3958`
	`MRP0 APPLYING_LOG 3958`
	
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`--------------------`
	`READ ONLY WITH APPLY`
		DBA

Ressources connexes

- Migrer la suite Oracle E-Business vers Amazon RDS Custom (AWS Prescriptive Guidance)
- Utilisation d'Amazon RDS Custom (documentation Amazon RDS)
- Utilisation de répliques de lecture pour Amazon RDS Custom pour Oracle (documentation Amazon RDS)

- Amazon RDS Custom pour Oracle — Nouvelles fonctionnalités de contrôle dans l'environnement de base de données (blog d'actualités AWS)
- Migration d'Oracle E-Business Suite sur AWS (livre blanc AWS)
- Architecture de la suite Oracle E-Business sur AWS (livre blanc AWS)

Configurer la réplication des données entre Amazon RDS for MySQL et MySQL sur EC2 Amazon à l'aide de GTID

Créée par Rajesh Madiwale (AWS)

Récapitulatif

Ce modèle décrit comment configurer la réplication de données sur le cloud Amazon Web Services (AWS) entre une instance de base de données Amazon Relational Database Service (Amazon RDS) pour MySQL et une base de données MySQL sur une instance Amazon Elastic Compute Cloud (EC2Amazon) en utilisant la réplication native de l'identifiant de transaction global (GTID) MySQL.

Avec GTIDs, les transactions sont identifiées et suivies lorsqu'elles sont validées sur le serveur d'origine et appliquées par des répliques. Il n'est pas nécessaire de consulter les fichiers journaux lorsque vous démarrez une nouvelle réplique lors d'un basculement.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance Amazon Linux déployée

Restrictions

- Cette configuration nécessite qu'une équipe interne exécute les requêtes en lecture seule.
- Les versions source et cible de MySQL doivent être identiques.
- La réplication est configurée dans la même région AWS et dans le même cloud privé virtuel (VPC).

Versions du produit

- Amazon RDS versions 5.7.23 et ultérieures, qui sont les versions qui prennent en charge le GTID

Architecture

Pile technologique source

- Amazon RDS for MySQL

Pile technologique cible

- MySQL sur Amazon EC2

Architecture cible

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Relational Database Service (Amazon RDS) pour MySQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle MySQL dans le cloud AWS.

Autres services

- Les identifiants de transaction globaux (GTIDs) sont des identifiants uniques générés pour les transactions MySQL validées.
- mysqldump est un utilitaire client permettant d'effectuer des sauvegardes logiques en produisant des instructions SQL qui peuvent être exécutées pour reproduire les définitions des objets de la base de données source et les données des tables.
- mysql est le client en ligne de commande de MySQL.

Épopées

Création et préparation de l'instance de base de données Amazon RDS for MySQL

Tâche	Description	Compétences requises
Créez l'instance RDS pour MySQL.	Pour créer l'instance RDS pour MySQL, suivez les étapes de la documentation Amazon RDS, en utilisant les valeurs des paramètre	DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	s abordées dans la tâche suivante.	
Activez les paramètres liés au GTID dans le groupe de paramètres de base de données.	Activez les paramètres suivants dans le groupe de paramètres de base de données Amazon RDS for MySQL. `enforce_gtid_consistency` Réglez sur on et réglez `gtid-mode` suron.	DBA
Redémarrez l'instance Amazon RDS for MySQL.	Un redémarrage est nécessaire pour que les modifications des paramètres soient prises en compte.	DBA

Créez un utilisateur et accordez-lui des autorisations de réplication.	Pour installer MySQL, utilisez les commandes suivantes.
	
	`CREATE USER 'repl'@'%' IDENTIFIED BY 'xxxx';`
	`GRANT REPLICATI ON slave ON *.* TO 'repl'@'%' ;`
	`FLUSH PRIVILEGES;`
		DBA

Installation et préparation de MySQL sur l' EC2 instance Amazon

Tâche	Description	Compétences requises

Installez MySQL sur Amazon Linux.	Pour installer MySQL, utilisez les commandes suivantes.
	`sudo yum update`
	`sudo wget https://dev.mysql.com/get/mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum localinstall mysql57-community-release-el7-11.noarch.rpm`
	`sudo yum install mysql-community-server`
	`sudo systemctl start mysqld`
		DBA

Connectez-vous à MySQL sur l' EC2 instance et créez la base de données.	Le nom de la base de données doit être identique à celui de la base de données dans Amazon RDS for MySQL. Dans l'exemple suivant, le nom de la base de données est`replication` . `create database replication;`	DBA
Modifiez le fichier de configuration MySQL et redémarrez la base de données.	Modifiez le `my.conf` fichier qui s'y trouve en `/etc/` ajoutant les paramètres suivants. `server-id=3`	DBA

Tâche	Description	Compétences requises

	`gtid_mode=ON enforce_gtid_consistency=ON replicate-ignore-db=mysql binlog-format=ROW log_bin=mysql-bin`
	
	Redémarrez ensuite le `mysqld` service.
	
	`systemctl mysqld restart`	

Configuration de la réplication

Tâche	Description	Compétences requises
Exportez le dump de données depuis la base de données Amazon RDS for MySQL.	Pour exporter le dump depuis Amazon RDS for MySQL, utilisez la commande suivante. `mysqldump --single-transaction -h mydb.xxxxxxx.amazonaws.com -uadmin -p --databases replication > replication-db.sql`	DBA
Restaurez le fichier de vidage .sql dans la base de données MySQL sur Amazon EC2.	Pour importer le dump dans la base de données MySQL sur Amazon EC2, utilisez la commande suivante.	DBA

Tâche	Description	Compétences requises
	`mysql -D replication -uroot -p < replication-db.sql`	

Configurez la base de données MySQL sur Amazon EC2 en tant que réplique.	Pour démarrer la réplication et vérifier l'état de la réplication, connectez-vous à la base de données MySQL sur Amazon EC2 et utilisez la commande suivante.
	`CHANGE MASTER TO MASTER_HOST="mydb.xxxxxxx.amazonaws.com", MASTER_USER="repl", MASTER_PASSWORD="rep123", MASTER_PORT=3306, MASTER_AUTO_POSITION = 1;`
	`START SLAVE;`
	`SHOW SLAVE STATUS\G`
		DBA

Ressources connexes

- Guide de EC2 l'utilisateur Amazon pour les instances Linux
- Installation de MySQL sous Linux à l'aide du référentiel MySQL Yum
- Réplication avec des identifiants de transaction globaux
- Utilisation de la réplication basée sur GTID pour Amazon RDS for MySQL

Rôles de transition pour une PeopleSoft application Oracle sur Amazon RDS Custom for Oracle

Créée par sampath kathirvel (AWS)

Récapitulatif

Pour exécuter la solution de planification des ressources PeopleSoft d'entreprise (ERP) Oracle sur Amazon Web Services (AWS), vous pouvez utiliser Amazon Relational Database Service (Amazon RDS) ou Amazon RDS Custom pour Oracle, qui prend en charge les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation (SE) et à l'environnement de base de données sous-jacents. Pour connaître les principaux facteurs à prendre en compte lors de la planification d'une migration, consultez les stratégies de migration des bases de données Oracle dans AWS Prescriptive Guidance.

Ce modèle se concentre sur les étapes à suivre pour effectuer un passage à Oracle Data Guard, ou une transition de rôle, pour une base de données d' PeopleSoft application exécutée sur Amazon RDS Custom en tant que base de données principale avec une base de données répliquée en lecture. Le modèle inclut des étapes pour configurer le basculement rapide (FSFO). Au cours de ce processus, les bases de données de la configuration Oracle Data Guard continuent de fonctionner dans leurs nouveaux rôles. Les cas d'utilisation typiques du passage à Oracle Data Guard sont les exercices de reprise après sinistre (DR), les activités de maintenance planifiée sur les bases de données et les patchs roulants Standby-First Patch Apply. Pour plus d'informations, consultez le billet de blog Réduire le temps d'arrêt de l'application de correctifs aux bases de données dans Amazon RDS Custom.

Conditions préalables et limitations

Prérequis

- Réalisation de l'opération personnalisée Ajouter HA à Oracle PeopleSoft sur Amazon RDS à l'aide d'un modèle de réplication de lecture.

Limites

- Limitations et configurations non prises en charge pour RDS Custom pour Oracle
- Limitations associées aux répliques de lecture Amazon RDS Custom for Oracle

Versions du produit

- Pour les versions de base de données Oracle prises en charge par Amazon RDS Custom, consultez RDS Custom pour Oracle.
- Pour les classes d'instance de base de données Oracle prises en charge par Amazon RDS Custom, consultez la section Support des classes d'instance de base de données pour RDS Custom pour Oracle.

Architecture

Pile technologique

- Amazon RDS Custom for Oracle

Architecture cible

Le schéma suivant montre une instance de base de données personnalisée Amazon RDS et une réplique de lecture personnalisée Amazon RDS. Oracle Data Guard assure la transition des rôles lors du basculement pour DR.

Pour une architecture représentative utilisant Oracle PeopleSoft sur AWS, voir Configurer une PeopleSoft architecture hautement disponible sur AWS.

Outils

Services AWS

- Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Dans ce modèle, vous pouvez récupérer les mots de passe des utilisateurs de base de données depuis Secrets Manager pour `RDS_DATAGUARD` lesquels le nom du secret est indiqué`do-not-delete-rds-custom-+<<RDS Resource ID>>+-dg`.

Autres services

- Oracle Data Guard vous aide à créer, maintenir, gérer et surveiller des bases de données de secours. Ce modèle utilise les performances maximales d'Oracle Data Guard pour la transition des rôles (passage à Oracle Data Guard).

Bonnes pratiques

Pour votre déploiement en production, nous vous recommandons de lancer l'instance d'observation dans une troisième zone de disponibilité, séparée du nœud principal et du nœud de réplication en lecture.

Épopées

Initier une transition de rôle

Tâche	Description	Compétences requises
Suspendez l'automatisation de la base de données pour la base de données principale et pour la réplique.	Bien que le framework d'automatisation RDS Custom n'interfère pas avec le processus de transition des rôles, il est recommandé de suspendre l'automatisation lors du passage à Oracle Data Guard. Pour suspendre et reprendre l'automatisation de la base de données RDS Custom, suivez les instructions de la section Suspension et reprise de l'automatisation RDS Custom.	Administrateur cloud, DBA
Vérifiez l'état d'Oracle Data Guard.	Pour vérifier l'état d'Oracle Data Guard, connectez-vous à la base de données principal e. Ce modèle inclut du code permettant d'utiliser une base de données de conteneurs	DBA

Tâche	Description	Compétences requises

	multilocataires (CDB) ou une instance non CDB.
	
	Non CDB
	
	`-bash-4.2$ dgmgrl RDS_DATAGUARD@RDS_CUSTOM_ORCL_A`
	`DGMGRL for Linux: Release 19.0.0.0.0 - Production on Mon Nov 28 20:55:50 2022`
	`Version 19.10.0.0.0`
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.`
	`Welcome to DGMGRL, type "help" for information.`
	`Password:`
	`Connected to "ORCL_A"`
	`Connected as SYSDG.`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 59 seconds ago)`
	`DGMGRL>`
	
	CDB	

Tâche	Description	Compétences requises

	CDB-bash-4.2$ dgmgrl
	 C##RDS_DATAGUARD@R
	DS_CUSTOM_RDSCDB_A
	DGMGRL for Linux:
	 Release 19.0.0.0.0 -
	 Production on Wed Jan
	 18 06:13:07 2023
	Version 19.16.0.0.0
	Copyright (c) 1982,
	 2019, Oracle and/or
	 its affiliates. All
	 rights reserved.
	Welcome to DGMGRL, type
	 "help" for informati
	on.
	Password:
	Connected to "RDSCDB_A
	"
	Connected as SYSDG.
	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	    rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 52 seconds ago)
	DGMGRL>	

Tâche	Description	Compétences requises
Vérifiez le rôle de l'instance.	Ouvrez la console de gestion AWS et accédez à la console Amazon RDS. Dans la section Réplication de la base de données, sous l'onglet Connectivité et sécurité, vérifiez le rôle de l'instance principale et de la réplique. Le rôle principal doit correspon dre à la base de données principale Oracle Data Guard, et le rôle de réplique doit correspondre à la base de données de secours physique Oracle Data Guard.	Administrateur cloud, DBA

Tâche	Description	Compétences requises

Effectuez le changement.	Pour effectuer le basculement, connectez-vous DGMGRL depuis le nœud principal.
	
	Non CDB
	
	`DGMGRL> switchover to orcl_d;`
	`Performing switchover NOW, please wait...`
	`Operation requires a connection to database "orcl_d"`
	`Connecting ...`
	`Connected to "ORCL_D"`
	`Connected as SYSDG.`
	`New primary database "orcl_d" is opening...`
	`Operation requires start up of instance "ORCL" on database "orcl_a"`
	`Starting instance "ORCL"...`
	`Connected to an idle instance.`
	`ORACLE instance started.`
	`Connected to "ORCL_A"`
	`Database mounted.`
	`Database opened.`
	`Connected to "ORCL_A"`
	`Switchover succeeded, new primary is "orcl_d"`
	`DGMGRL>`
	
	CDB
	
	`DGMGRL> switchover to rdscdb_b`
		DBA

Tâche	Description	Compétences requises
	Performing switchover NOW, please wait... New primary database "rdscdb_b" is opening... Operation requires start up of instance "RDSCDB" on database "rdscdb_a" Starting instance "RDSCDB"... Connected to an idle instance. ORACLE instance started. Connected to "RDSCDB_A " Database mounted. Database opened. Connected to "RDSCDB_A " Switchover succeeded , new primary is "rdscdb_b"	

Tâche	Description	Compétences requises

Vérifiez la connexion Oracle Data Guard.	Après le basculement, vérifiez la connexion Oracle Data Guard entre le nœud principal et. DGMGRL
	
	Non CDB
	
	`DGMGRL> show configura tion;`
	`Configuration - rds_dg`
	`Protection Mode:  MaxAvailability`
	`Members:`
	`orcl_d - Primary  database`
	`orcl_a - Physical  standby database`
	`Fast-Start Failover:  Disabled`
	`Configuration Status:`
	`SUCCESS (status updated  60 seconds ago)`
	`DGMGRL>`
	
	`DGMGRL> show configura tion lag;`
	`Configuration - rds_dg`
	`Protection Mode:  MaxAvailability`
	`Members:`
	`orcl_d - Primary  database`
	`orcl_a - Physical  standby database`
	`Transport Lag: 0  seconds (computed 0  seconds ago)`
	`Apply Lag: 0 seconds  (computed 0 seconds  ago)`
		DBA

Tâche	Description	Compétences requises
	Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 44 seconds ago) DGMGRL>	
	CDB DGMGRL> show configura tion DGMGRL> show configura tion Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_b - Primary database rdscdb_a - Physical standby database Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 52 seconds ago) DGMGRL> DGMGRL> show configura tion lag Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_b - Primary database rdscdb_a - Physical standby database Transport Lag: 0 seconds	

Tâche	Description	Compétences requises
	(computed 0 seconds ago) Apply Lag: 0 seconds (computed 0 seconds ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 53 seconds ago) DGMGRL>	
Vérifiez le rôle de l'instance sur la console Amazon RDS.	Après avoir effectué le changement de rôle, la console Amazon RDS affiche les nouveaux rôles dans la section Réplication de l'onglet Connectivité et sécurité sous Bases de données. La mise à jour de l'état de réplication de vide à Réplication peut prendre quelques minutes.	DBA

Configurer FSFO

Tâche	Description	Compétences requises
Réinitialisez le basculement.	Replacez le basculement sur le nœud principal.	DBA
Installez et démarrez l'observateur.	Un processus d'observation est un composant DGMGRL client qui s'exécute généralement sur une machine différente de celle	DBA

Tâche	Description	Compétences requises
	des bases de données principale et de secours. L'installation d'ORACLE HOME pour l'observateur peut être une installation Oracle Client Administrator, ou vous pouvez installer Oracle Database Enterprise Edition ou Personal Edition. Pour plus d'informations sur l'installation de l'observateur pour la version de votre base de données, voir Installation et démarrage de l'observateur. Pour configurer la haute disponibilité pour le processus d'observation, vous pouvez effectuer les opérations suivantes : • Activez EC2 la restauration automatique de l' EC2 instance qui exécute votre observateur. Vous devez automatiser le processus de démarrage de l'observateur dans le cadre du démarrage du système d'exploitation. • Déployez un observateur dans l' EC2 instance et configurez un groupe Amazon EC2 Auto Scaling de taille 1. En cas de défaillance d'une EC2 instance, le groupe de	

Tâche	Description	Compétences requises
	dimensionnement automatique lance automatiquement une autre EC2 instance. Pour Oracle 12c version 2 et versions ultérieures, vous pouvez déployer jusqu'à trois observateurs. L'un des observateurs est l'observateur principal et les autres sont des observateurs suppléants. Lorsque l'observateur principal échoue, l'un des observateurs suppléants prend le rôle principal.	

Tâche	Description	Compétences requises

Connectez-vous à DGMGRL depuis l'hôte observateur.	L'hôte observateur est configuré avec des `tnsnames.ora` entrées pour la connectivité à la base de données principale et de secours. Vous pouvez activer FSFO avec le mode de protection des performances maximales tant que la perte de données est conforme à la FastStartFailoverLagLimitconfiguration (valeur en secondes). Cependant, vous devez utiliser le mode de protection de disponibilité maximale pour atteindre zéro perte de données (RPO=0).
	
	Non CDB
	
	`DGMGRL> show configuration;`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`orcl_d - Physical standby database`
	`Fast-Start Failover: Disabled`
	`Configuration Status:`
	`SUCCESS (status updated 58 seconds ago)`
	`DGMGRL> show configuration lag`
	`Configuration - rds_dg`
		DBA

Tâche	Description	Compétences requises
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - Physical standby database Transport Lag: 0 seconds (computed 1 second ago) Apply Lag: 0 seconds (computed 1 second ago) Fast-Start Failover: Disabled Configuration Status: SUCCESS (status updated 5 seconds ago) DGMGRL>	
	CDB -bash-4.2$ dgmgrl C##RDS_DATAGUARD@R DS_CUSTOM_RDSCDB_A DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Jan 18 06:55:09 2023 Version 19.16.0.0.0 Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved. Welcome to DGMGRL, type "help" for informati on. Password: Connected to "RDSCDB_A " Connected as SYSDG.	

Tâche	Description	Compétences requises

	DGMGRL> show configura
	tion
	Configuration - rds_dg
	  Protection Mode:
	 MaxAvailability
	  Members:
	  rdscdb_a - Primary
	 database
	  rdscdb_b - Physical
	 standby database
	Fast-Start Failover:
	 Disabled
	Configuration Status:
	SUCCESS (status
	 updated 18 seconds ago)
	DGMGRL>	

Tâche	Description	Compétences requises

Modifiez la base de données de secours pour qu'elle soit la cible du basculement.	Connectez-vous depuis le nœud principal ou le nœud observateur à une base de données de secours. (Bien que votre configuration puisse comporter plusieurs bases de données de secours, vous ne devez vous connecter qu'à une seule pour le moment.)
	
	Non CDB
	
	`DGMGRL> edit database orcl_a set property FastStartFailoverTarget='orcl_d';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> edit database orcl_d set property FastStartFailoverTarget='orcl_a';`
	`Property "faststartfailovertarget" updated`
	`DGMGRL> show database orcl_a FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_d'`
	`DGMGRL> show database orcl_d FastStartFailoverTarget;`
	`FastStartFailoverTarget = 'orcl_a'`
	`DGMGRL>`
	
	CDB
		DBA

Tâche	Description	Compétences requises
	`DGMGRL> edit database orcl_a set property FastStartFailoverT arget='rdscdb_b'; Object "orcl_a" was not found DGMGRL> edit database rdscdb_a set property FastStartFailoverT arget='rdscdb_b'; Property "faststar tfailovertarget" updated DGMGRL> edit database rdscdb_b set property FastStartFailoverT arget='rdscdb_a'; Property "faststar tfailovertarget" updated DGMGRL> show database rdscdb_a FastStart FailoverTarget; FastStartFailoverT arget = 'rdscdb_b' DGMGRL> show database rdscdb_b FastStart FailoverTarget; FastStartFailoverT arget = 'rdscdb_a' DGMGRL>`	

Tâche	Description	Compétences requises
Configurez FastStartFailoverThreshold pour la connexion à DGMGRL.	La valeur par défaut est de 30 secondes dans Oracle 19c et la valeur minimale est de 6 secondes. Une valeur inférieure peut potentiellement raccourcir l'objectif de temps de restauration (RTO) lors du basculement. Une valeur plus élevée permet de réduire le risque d'erreurs transitoires inutiles liées au basculement sur la base de données principale. Le framework d'automatisation RDS Custom for Oracle surveille l'état de la base de données et effectue des actions correctives toutes les quelques secondes. Par conséquent, nous vous recommandons FastStartFailoverThreshold de définir une valeur supérieure à 10 secondes. L'exemple suivant configure la valeur de seuil à 35 secondes. Sans CBD ou CDB `DGMGRL> edit configuration set property FastStartFailoverThreshold=35;`	DBA

Tâche	Description	Compétences requises

	`Property "faststar tfailoverthreshold" updated`
	`DGMGRL> show configura tion FastStart FailoverThreshold;`
	`FastStartFailover Threshold = '35'`
	`DGMGRL>`	

Tâche	Description	Compétences requises

Activez FSFO en vous connectant à DGMGRL depuis le nœud principal ou le nœud observateur.	Si la base de données Flashback n'est pas activée, le message d'avertissement `ORA-16827` s'affiche. La base de données flashback facultative permet de rétablir automatiquement les bases de données principales défaillantes à un moment donné avant le basculement si la propriété de FastStartFailoverAutoReinstateconfiguration est définie sur `TRUE` (valeur par défaut).
	
	Non CDB
	
	`DGMGRL> enable fast_start failover;`
	`Warning: ORA-16827: Flashback Database is disabled`
	`Enabled in Zero Data Loss Mode.`
	`DGMGRL>`
	`DGMGRL> show configuration`
	`Configuration - rds_dg`
	`Protection Mode: MaxAvailability`
	`Members:`
	`orcl_a - Primary database`
	`Warning: ORA-16819: fast-start failover observer not started`
	`orcl_d - (*) Physical standby database`
		DBA

Tâche	Description	Compétences requises
	Warning: ORA-16819: fast-start failover observer not started Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 29 seconds ago) DGMGRL> CDB DGMGRL> enable fast_star t failover; Warning: ORA-16827: Flashback Database is disabled Enabled in Zero Data Loss Mode. DGMGRL> show configura tion; Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database Warning: ORA-16819 : fast-start failover observer not started rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: WARNING (status updated 11 seconds ago)	

Tâche	Description	Compétences requises
	`DGMGRL>`	

Tâche	Description	Compétences requises

Démarrez l'observateur pour la surveillance du FSFO et vérifiez l'état.	Vous pouvez démarrer l'observateur avant ou après avoir activé FSFO. Si FSFO est déjà activé, l'observateur commence immédiatement à surveiller l'état et les connexions aux bases de données de secours principales et cibles. Si le FSFO n'est pas activé, l'observateur ne commence à surveiller qu'une fois le FSFO activé.
	
	Lorsque vous démarrez l'observateur, la configuration de base de données principale s'affiche sans aucun message d'erreur, comme en témoigne la `show configuration` commande précédente.
	
	Non CDB
	
	`DGMGRL> start observer;`
	`[W000 2022-12-0`
	`1T06:16:51.271+00:00]`
	`FSFO target standby is`
	`orcl_d`
	`Observer 'ip-10-0-`
	`1-89' started`
	`[W000 2022-12-0`
	`1T06:16:51.352+00:00]`
	`Observer trace level is`
	`set to USER`
	
	`DGMGRL> show configura`
	`tion`
	`Configuration - rds_dg`
		DBA

Tâche	Description	Compétences requises
	Protection Mode: MaxAvailability Members: orcl_a - Primary database orcl_d - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 56 seconds ago) DGMGRL> DGMGRL> show observer Configuration - rds_dg Primary: orcl_a Active Target: orcl_d Observer "ip-10-0- 1-89" - Master Host Name: ip-10-0-1 -89 Last Ping to Primary: 1 second ago Last Ping to Target: 1 second ago DGMGRL> CDB DGMGRL> start observer; Succeeded in opening the observer file "/home/oracle/fsfo _ip-10-0-1-56.dat". [W000 2023-01-1 8T07:31:32.589+00:00] FSFO target standby is rdscdb_b	

Tâche	Description	Compétences requises
	Observer 'ip-10-0-1-56' started The observer log file is '/home/oracle/observer_ip-10-0-1-56.log'. DGMGRL> show configuration Configuration - rds_dg Protection Mode: MaxAvailability Members: rdscdb_a - Primary database rdscdb_b - (*) Physical standby database Fast-Start Failover: Enabled in Zero Data Loss Mode Configuration Status: SUCCESS (status updated 12 seconds ago) DGMGRL> DGMGRL> show observer; Configuration - rds_dg Primary: rdscdb_a Active Target: rdscdb_b Observer "ip-10-0-1-56" - Master Host Name: ip-10-0-1-56 Last Ping to Primary: 1 second ago Last Ping to Target: 2 seconds ago DGMGRL>	

Tâche	Description	Compétences requises
Vérifiez le basculement.	Dans ce scénario, un test de basculement peut être effectué en arrêtant manuellement l' EC2 instance principale. Avant d'arrêter l' EC2 instance, utilisez la `tail` commande pour surveiller le fichier journal de l'observateur en fonction de votre configura tion. `DGMGRL`À utiliser pour se connecter à la base de données de secours `orcl_d` avec l'utilisateur `RDS_DATAG UARD` et vérifier l'état d'Oracle Data Guard. Cela devrait indiquer qu'il s'`orcl_d`agit de la nouvelle base de données principale. **Note** Dans ce scénario de test de basculement, `orcl_d` se trouve la base de données non CDB. Avant le basculement, la base de données Flashback a été activée. `orcl_a` Une fois que l'ancienne base de données principale est remise en ligne et redémarre en `MOUNT` état, l'observateur la rétablit dans	DBA

Tâche	Description	Compétences requises

	une nouvelle base de données de secours. La base de données rétablie fait office de cible FSFO pour la nouvelle base de données principal e. Vous pouvez vérifier les détails dans les journaux des observateurs.
	
	`DGMGRL> show configura tion`
	`Configuration - rds_dg`
	`Protection Mode:  MaxAvailability`
	`Members:`
	`orcl_d - Primary  database`
	`Warning: ORA-16824 : multiple warnings,  including fast-star t failover-related  warnings, detected for  the database`
	`orcl_a - (*) Physical  standby database  (disabled)`
	`ORA-16661: the standby  database needs to be  reinstated`
	`Fast-Start Failover:  Enabled in Zero Data  Loss Mode`
	`Configuration Status:`
	`WARNING (status updated  25 seconds ago)`
	`DGMGRL>`	

Tâche	Description	Compétences requises

	L'exemple suivant montre un exemple de sortie `enobserver.log` .
	
	`$ tail -f /tmp/obse rver.log`
	`Unable to connect to database using rds_custom_orcl_a`
	`[W000 2023-01-1 8T07:50:32.589+00:00] Primary database cannot be reached.`
	`[W000 2023-01-1 8T07:50:32.589+00:00] Fast-Start Failover threshold has expired.`
	`[W000 2023-01-1 8T07:50:32.590+00:00] Try to connect to the standby.`
	`[W000 2023-01-1 8T07:50:32.590+00: 00] Making a last connection attempt to primary database before proceeding with Fast-Start Failover.`
	`[W000 2023-01-1 8T07:50:32.591+00:00] Check if the standby is ready for failover.`
	`[S002 2023-01-1 8T07:50:32.591+00:00] Fast-Start Failover started...`
	`2023-01-18T07:50 :32.591+00:00`
	`Initiating Fast-Star t Failover to database "orcl_d"...`	

Tâche	Description	Compétences requises
	[S002 2023-01-18T07:50:32.592+00:00] Initiating Fast-start Failover. Performing failover NOW, please wait... Failover succeeded, new primary is "orcl_d" 2023-01-18T07:55:32.101+00:00 [S002 2023-01-18T07:55:32.591+00:00] Fast-Start Failover finished... [W000 2023-01-18T07:55:32.591+00:00] Failover succeeded. Restart pinging. [W000 2023-01-18T07:55:32.603+00:00] Primary database has changed to orcl_d. [W000 2023-01-18T07:55:33.618+00:00] Try to connect to the primary. [W000 2023-01-18T07:55:33.622+00:00] Try to connect to the primary rds_custom_orcl_d. [W000 2023-01-18T07:55:33.634+00:00] The standby orcl_a needs to be reinstated [W000 2023-01-18T07:55:33.654+00:00] Try to connect to the new standby orcl_a. [W000 2023-01-18T07:55:33.654+00:	

Tâche	Description	Compétences requises
	00] Connection to the primary restored! [W000 2023-01-18T07:55:35.654+00:00] Disconnecting from database rds_custom_orcl_d. [W000 2023-01-18T07:55:57.701+00:00] Try to connect to the new standby orcl_a. ORA-12170: TNS:Connect timeout occurred	

Configuration de la connectivité entre l'application Oracle Peoplesoft et la base de données

Tâche	Description	Compétences requises
Créez et démarrez le service dans la base de données principale.	Vous pouvez éviter de modifier la configuration de l'application lors d'une transition de rôle en utilisant une entrée TNS qui contient à la fois les points de terminaison de base de données principaux et de secours dans la configuration. Vous pouvez définir deux services de base de données basés sur des rôles pour prendre en charge les charges de travail en lecture/écriture et en lecture seule. Dans l'exemple suivant, `orcl_rw` il s'agit du service de lecture/écriture actif sur la base de données principal	DBA

Tâche	Description	Compétences requises
	e. `orcl_ro`est le service en lecture seule et est actif sur la base de données de secours qui a été ouverte en mode lecture seule. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- --------- ----------- ORCL READ WRITE SQL> exec dbms_serv ice.create_service ('orcl_rw','orcl_r w'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.create_service ('orcl_ro','orcl_r o'); PL/SQL procedure successfully completed . SQL> exec dbms_serv ice.start_service('orcl_rw'); PL/SQL procedure successfully completed . SQL>`	

Tâche	Description	Compétences requises
Démarrez le service dans la base de données de secours.	Pour démarrer le service dans la base de données de secours en lecture seule, utilisez le code suivant. `SQL> select name,open _mode from v$database; NAME OPEN_MODE --------- ---------- ----------- ORCL READ ONLY WITH APPLY SQL> exec dbms_serv ice.start_service( 'orcl_ro'); PL/SQL procedure successfully completed . SQL>`	DBA

Tâche	Description	Compétences requises
Automatisez le démarrage du service lorsque la base de données principale est redémarrée.	Pour démarrer automatiq uement le service dans la base de données principale au redémarrage, utilisez le code suivant. `SQL> CREATE OR REPLACE TRIGGER TrgDgServices after startup on database DECLARE db_role VARCHAR(30); db_open_mode VARCHAR(30); BEGIN SELECT DATABASE_ROLE, OPEN_MODE INTO db_role, db_open_mode FROM V$DATABASE; IF db_role = 'PRIMARY' THEN DBMS_SERV 2 ICE.START_SERVICE('orcl_rw'); END IF; IF db_role = 'PHYSICAL STANDBY' AND db_open_mode LIKE 'READ ONLY%' THEN DBMS_SERVICE.START_SERVICE('orcl_ro'); END IF; END; / Trigger created. SQL>`	DBA

Tâche	Description	Compétences requises
Configurez une connexion entre les bases de données en lecture/écriture et en lecture seule.	Vous pouvez utiliser l'exemple de configuration d'application suivant pour les connexion s en lecture/écriture et en lecture seule. `ORCL_RW = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread.******.us-west-2.rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVICE_NAME = orcl_rw)))` `ORCL_RO = (DESCRIPTION = (CONNECT_TIMEOUT= 120)(RETRY_COUNT=20)(RETRY_DELAY=3)(TRANSPORT_CONNECT_TIMEOUT=3) (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST=devpsftdb.******.us-west-2`	DBA

Tâche	Description	Compétences requises
	.rds.amazonaws.com) (PORT=1521)) (ADDRESS = (PROTOCOL = TCP)(HOST=psftread .******.us-west-2. rds.amazonaws.com) (PORT=1521))) (CONNECT_DATA=(SERVIC E_NAME = orcl_ro)))	

Ressources connexes

- Activer la haute disponibilité avec Data Guard sur Amazon RDS Custom pour Oracle (Guide technique AWS)
- Configuration d'Amazon RDS en tant que PeopleSoft base de données Oracle (livre blanc AWS)
- Guide Oracle Data Guard Broker (documentation de référence Oracle)
- Concepts et administration de Data Guard (documentation de référence Oracle)
- Exigences de configuration FAN et FCF spécifiques à Oracle Data Guard (documentation de référence Oracle)

Déchargez les données d'un cluster Amazon Redshift entre différents comptes vers Amazon S3

Créée par Andrew Kamel (AWS)

Récapitulatif

Lorsque vous testez des applications, il est utile de disposer de données de production dans votre environnement de test. L'utilisation des données de production peut vous donner une évaluation plus précise de l'application que vous développez.

Ce modèle extrait les données d'un cluster Amazon Redshift dans un environnement de production vers un bucket Amazon Simple Storage Service (Amazon S3) dans un environnement de développement sur Amazon Web Services ().AWS

Le modèle décrit les étapes de configuration des comptes DEV et PROD, notamment les suivantes :

- Ressources requises
- AWS Identity and Access Management Rôles (IAM)
- Ajustements réseau apportés aux sous-réseaux, aux groupes de sécurité et au cloud privé virtuel (VPC) pour prendre en charge la connexion Amazon Redshift
- Exemple de AWS Lambda fonction avec un environnement d'exécution Python pour tester l'architecture

Pour accorder l'accès au cluster Amazon Redshift, le modèle permet de stocker les AWS Secrets Manager informations d'identification pertinentes. L'avantage est de disposer de toutes les informations nécessaires pour se connecter directement au cluster Amazon Redshift sans avoir besoin de savoir où se trouve le cluster Amazon Redshift. De plus, vous pouvez contrôler l'utilisation du secret.

Le secret enregistré dans Secrets Manager inclut l'hôte du cluster Amazon Redshift, le nom de la base de données, le port et les informations d'identification pertinentes.

Pour plus d'informations sur les considérations de sécurité liées à l'utilisation de ce modèle, consultez la section Bonnes pratiques.

Conditions préalables et limitations

Prérequis

- Un cluster Amazon Redshift exécuté dans le compte PROD
- Un bucket S3 créé dans le compte DEV
- Peering VPC entre les comptes DEV et PROD, avec tables de routage ajustées en conséquence
- Noms d'hôte DNS et résolution DNS activés pour les deux versions peered VPCs

Limites

- En fonction de la quantité de données que vous souhaitez interroger, le délai d'expiration de la fonction Lambda peut être dépassé.

  Si votre exécution prend plus de temps que le délai maximum Lambda (15 minutes), utilisez une approche asynchrone pour votre code Lambda. L'exemple de code de ce modèle utilise la bibliothèque psycopg2 pour Python, qui ne prend actuellement pas en charge le traitement asynchrone.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Le schéma suivant montre l'architecture cible, avec les comptes DEV et PROD.

Le schéma suivant illustre le flux de travail suivant :

1. La fonction Lambda du compte DEV assume le rôle IAM requis pour accéder aux informations d'identification Amazon Redshift dans Secrets Manager dans le compte PROD.

   La fonction Lambda récupère ensuite le secret du cluster Amazon Redshift.
2. La fonction Lambda du compte DEV utilise les informations pour se connecter au cluster Amazon Redshift dans le compte PROD via le peered. VPCs

   La fonction Lambda envoie ensuite une commande de déchargement pour interroger le cluster Amazon Redshift dans le compte PROD.
3. Le cluster Amazon Redshift du compte PROD assume le rôle IAM approprié pour accéder au compartiment S3 du compte DEV.

Le cluster Amazon Redshift décharge les données demandées dans le compartiment S3 du compte DEV.

Interrogation de données depuis Amazon Redshift

Le schéma suivant montre les rôles utilisés pour récupérer les informations d'identification Amazon Redshift et se connecter au cluster Amazon Redshift. Le flux de travail est lancé par la fonction Lambda.

Le schéma suivant illustre le flux de travail suivant :

1. Le compte `CrossAccount-SM-Read-Role` in the DEV suppose le compte `SM-Read-Role` in the PROD.
2. Le `SM-Read-Role` rôle utilise la politique ci-jointe pour récupérer le secret auprès de Secrets Manager.
3. Les informations d'identification sont utilisées pour accéder au cluster Amazon Redshift.

Chargement de données vers Amazon S3

Le schéma suivant montre le processus de lecture-écriture entre comptes permettant d'extraire des données et de les télécharger sur Amazon S3. Le flux de travail est lancé par la fonction Lambda. Le modèle enchaîne les rôles IAM dans Amazon Redshift. La commande de déchargement qui provient du cluster Amazon Redshift suppose `CrossAccount-S3-Write-Role` le, puis suppose le. `S3-Write-Role` Ce chaînage de rôles permet à Amazon Redshift d'accéder à Amazon S3.

Le flux de travail comprend les étapes suivantes :

1. Le compte `CrossAccount-SM-Read-Role` in the DEV suppose le compte `SM-Read-Role` in the PROD.
2. `SM-Read-Role`récupère les informations d'identification Amazon Redshift auprès de Secrets Manager.
3. La fonction Lambda se connecte au cluster Amazon Redshift et envoie une requête.
4. Le cluster Amazon Redshift suppose que. `CrossAccount-S3-Write-Role`

5. Cela `CrossAccount-S3-Write-Role` suppose que c'est `S3-Write-Role` dans le compte DEV.
6. Les résultats de la requête sont déchargés dans le compartiment S3 du compte DEV.

Outils

Services AWS

- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Redshift est un service d'entrepôt de données géré à l'échelle du pétaoctet dans le cloud AWS.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub unload-redshift-to-s3-python.

Bonnes pratiques

Avertissement de sécurité

Avant de mettre en œuvre cette solution, tenez compte des recommandations de sécurité importantes suivantes :

- N'oubliez pas que la connexion des comptes de développement et de production peut augmenter la portée et réduire le niveau de sécurité global. Nous recommandons de ne déployer cette solution que temporairement, en extrayant la portion de données requise, puis en détruisant immédiatement les ressources déployées. Pour détruire les ressources, vous devez supprimer la fonction Lambda,

supprimer tous les rôles et politiques IAM créés pour cette solution et révoquer tout accès réseau accordé entre les comptes.

- Consultez vos équipes de sécurité et de conformité avant de copier des données depuis des environnements de production vers des environnements de développement. Les informations personnelles identifiables (PII), les informations de santé protégées (PHI) et les autres données confidentielles ou réglementées ne doivent généralement pas être copiées de cette manière. Copiez uniquement les informations non confidentielles accessibles au public (par exemple, les données boursières publiques provenant d'une interface de boutique). Envisagez de tokeniser ou d'anonymiser les données, ou de générer des données de test synthétiques, au lieu d'utiliser des données de production dans la mesure du possible. L'un des principes de AWS sécurité consiste à tenir les gens à l'écart des données. En d'autres termes, les développeurs ne doivent pas effectuer d'opérations dans le compte de production.
- Limitez l'accès à la fonction Lambda dans le compte de développement, car elle peut lire les données du cluster Amazon Redshift dans l'environnement de production.
- Pour éviter de perturber l'environnement de production, appliquez les recommandations suivantes :
  - Utilisez un compte de développement dédié distinct pour les activités de test et de développement.
  - Mettez en œuvre des contrôles d'accès réseau stricts et limitez le trafic entre les comptes au strict nécessaire.
  - Surveillez et auditez l'accès à l'environnement de production et aux sources de données.
  - Mettez en œuvre des contrôles d'accès basés sur le principe du moindre privilège pour toutes les ressources et tous les services concernés.
  - Passez régulièrement en revue et alternez les informations d'identification, telles que AWS Secrets Manager les secrets et les clés d'accès aux rôles IAM.
- Reportez-vous à la documentation de sécurité suivante pour les services utilisés dans cet article :
  - AWS Lambda sécurité
  - Sécurité d'Amazon Redshift
  - Sécurité d'Amazon S3
  - AWS Secrets Manager sécurité
  - Bonnes pratiques de sécurité IAM

La sécurité est une priorité absolue lors de l'accès aux données et aux ressources de production. Suivez toujours les meilleures pratiques, mettez en œuvre des contrôles d'accès fondés sur le moindre privilège et révisez et mettez à jour régulièrement vos mesures de sécurité.

Épopées

Interrogez des données depuis Amazon Redshift

Tâche	Description	Compétences requises
Créez un secret pour le cluster Amazon Redshift.	Pour créer le secret du cluster Amazon Redshift, procédez comme suit : 1. Dans le compte PROD, connectez-vous à la AWS Management Console console Secrets Manager et ouvrez-la à https://console.aws.amazon.com/secretsmanager/ l'adresse. 2. Choisissez Enregistrer un nouveau secret. 3. Sélectionnez les informations d'identification pour l'entrepôt de données Amazon Redshift. 4. Pour Nom d'utilisateur et Mot de passe, entrez des valeurs pour votre instance, puis confirmez ou choisissez une valeur pour la clé de chiffrement. 5. Choisissez l'entrepôt de données Amazon Redshift auquel votre secret aura accès.	DevOps ingénieur

Tâche	Description	Compétences requises
	6. Entrez `Redshift-Creds-Secret` le nom du secret. 7. Effectuez les étapes de création restantes avec les choix par défaut, puis choisissez Store. 8. Consultez votre secret et notez la valeur de l'ARN secret qui a été générée pour identifier le secret.	

Tâche	Description	Compétences requises
Créez un rôle pour accéder à Secrets Manager.	Pour créer le rôle, procédez comme suit : 1. Dans le compte PROD, ouvrez la console IAM à l'adresse. https://console.aws.amazon.com/iam/ 2. Choisissez Policies (Politiques). 3. Choisissez Create Policy (Créer une politique). 4. Choisissez l'onglet JSON, puis entrez une politique IAM telle que la suivante : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "secretsmanager:GetResourcePolicy", "secretsmanager:GetSecretValue", "secretsmanager:DescribeSecret", "secretsmanager:ListSecretVersionIds" ],`	DevOps ingénieur

Tâche	Description	Compétences requises
	"Resource": ["<Redshift-Creds-Secret-ARN>"] }, { "Effect": "Allow", "Action": "secretsmanager:ListSecrets", "Resource": "*" }] } `Redshift-Creds-Secret-ARN` Remplacez-le par le nom de ressource Amazon (ARN) du secret Secrets Manager qui contient les informations et les informations d'identification du cluster Amazon Redshift.	

Chargement de données vers Amazon S3

Tâche	Description	Compétences requises
Créez un rôle pour accéder au compartiment S3.	Pour créer le rôle permettant d'accéder au compartiment S3, procédez comme suit :	DevOps ingénieur

Tâche	Description	Compétences requises
	1. Dans le compte DEV, ouvrez la console IAM. 2. Choisissez Policies (Politiques). 3. Choisissez Create Policy (Créer une politique). 4. Choisissez l'onglet JSON, puis entrez une politique IAM telle que la suivante : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "kmsstmt", "Effect": "Allow", "Action": [ "kms:Decrypt", "kms:Encrypt", "kms:GenerateDataKey" ], "Resource": [ "<kms-key-arn>" ] }, { "Sid": "s3stmt", "Effect": "Allow", "Action": [`	

Tâche	Description	Compétences requises

	<pre>"s3:PutObject",
	"s3:Get*",
	"s3:List*"
	],
	"Resource": [
	"arn:aws:s3:::mybucket",
	"arn:aws:s3:::mybucket/*"
	]
	}
	]
	}</pre> `mybucket`Remplacez-le par le nom du compartiment S3 auquel vous souhaitez accéder. En outre, si le compartiment S3 est chiffré, remplacez-le par `kms-key-arn` l'ARN de la clé AWS Key Management Service (AWS KMS) utilisée pour chiffrer le compartiment S3. Dans le cas contraire, vous n'avez pas besoin de AWS KMS cette section dans la politique.
	5. Choisissez Réviser la politique, entrez le `S3-Write-Policy` nom de la politique, puis choisissez Créer une politique.	

Tâche	Description	Compétences requises
	6. Dans le panneau de navigation, choisissez Roles (Rôles). 7. Sélectionnez Create role (Créer un rôle). 8. Pour le rôle d'entité de confiance, choisissez Politique de confiance personnalisée. 9. Choisissez Next : Permissions, puis sélectionnez la politique S3-Write-Policy que vous avez créée. 10. Entrez le `S3-Write-Role` nom du rôle, puis choisissez Créer un rôle.	

Tâche	Description	Compétences requises
Créez le rôle Amazon Redshift.	Pour créer le rôle Amazon Redshift, procédez comme suit : 1. Dans le compte PROD, ouvrez la console IAM. 2. Choisissez Policies (Politiques). 3. Choisissez Create Policy (Créer une politique). 4. Choisissez l'onglet JSON, puis entrez une politique IAM telle que la suivante : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "CrossAccountPolicy", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "S3-Write-Role-ARN" } ] }` `S3-Write-Role-ARN`Remplacez-le par l'ARN `S3-Write-Role` du compte DEV.	DevOps ingénieur

Tâche	Description	Compétences requises
	5. Choisissez Réviser la politique, entrez le `S3-Write-Role-Assume-Policy` nom de la politique, puis choisissez Créer une politique. 6. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle. 7. Choisissez le service AWS comme type d'entité de confiance, puis choisissez Redshift, Redshift - Customizable. 8. Choisissez Next : Permissions, puis sélectionnez la politique S3-Write-Role-Assume-Policy que vous avez créée. 9. Entrez le `CrossAccount-S3-Write-Role` nom du rôle, puis choisissez Créer un rôle. 10 Associez le rôle IAM à votre cluster Amazon Redshift.	

Déployez la fonction Lambda.

Tâche	Description	Compétences requises
Déployez la fonction Lambda.	Pour déployer une fonction Lambda dans le VPC	DevOps ingénieur

Tâche	Description	Compétences requises
	homologue, procédez comme suit : 1. Ouvrez la console Lambda à l'adresse. https://console.aws.amazon.com/lambda/ 2. Choisissez Functions. 3. Choisissez Créer une fonction. 4. Sous Informations de base, dans Nom de fonction, entrez un nom pour votre fonction. 5. Pour Runtime, choisissez Python 3.8. 6. Développez Modifier le rôle d'exécution par défaut, puis effectuez les opérations suivantes : a. Choisissez Utiliser un rôle existant. b. Pour Rôle existant, sélectionnez le rôle Lambda CrossAccount-RM-Read-Role que vous avez créé précédemment. 7. Développez les paramètres avancés, puis procédez comme suit : a. Cochez la case Activer le VPC.	

Tâche	Description	Compétences requises
	b. Pour le VPC, sélectionnez le VPC apparenté dans le compte DEV. c. Pour les sous-réseaux, sélectionnez le sous-réseau privé. d. Pour Groupes de sécurité, sélectionnez le groupe de sécurité par défaut. 8. Choisissez Créer une fonction. 9. Ajoutez la bibliothèque psycopg2 en tant que couche à la fonction Lambda. **Note** Vous pouvez utiliser une couche déjà déployée depuis le référentiel psycopg2-lambda-layer. Assurez-vous d'utiliser l'URL en fonction de votre environnement d'exécution Région AWS et de celui de Python.	

Testez l'architecture

Tâche	Description	Compétences requises

Importez les ressources requises.	Pour importer les ressource s requises, exécutez les commandes suivantes :
	`import ast`
	`import boto3`
	`import psycopg2`
	`import base64`
	`from botocore.`
	`exceptions import`
	` ClientError`
		Développeur d’applications

Exécutez la fonction de gestion Lambda.	La fonction Lambda utilise AWS Security Token Service (AWS STS) pour l'accès entre comptes et la gestion des informations d'identification temporaires. La fonction utilise l'opération d' AssumeRole API pour assumer temporair ement les autorisations du rôle `sm_read_role` IAM.
	Pour exécuter la fonction Lambda, utilisez l'exemple de code suivant :
	`def lambda_handler(eve`
	`nt, context):`
	`  sts_client =`
	` boto3.client('sts')`
	`  # Secrets Manager`
	` Configurations`
		Développeur d’applications

Tâche	Description	Compétences requises

	`secret_name = "redshift_creds"`
	`sm_region = "eu-west-1"`
	`sm_read_role = "arn:aws:iam::PROD_ACCOUNT_NUMBER:role/SM-Read-Role"`
	
	`# S3 Bucket Configurations`
	`s3_bucket_path = "s3://mybucket/"`
	`s3_bucket_region = "eu-west-1"`
	`s3_write_role = "arn:aws:iam::DEV_ACCOUNT_NUMBER:role/S3-Write-Role"`
	
	`# Redshift Configurations`
	`sql_query = "select * from category"`
	`redshift_db = "dev"`
	`redshift_s3_write_role = "arn:aws:iam::PROD_ACCOUNT_NUMBER:role/CrossAccount-S3-Write-Role"`
	
	`chained_s3_write_role = "%s,%s" % (redshift_s3_write_role, s3_write_role)`
	
	`assumed_role_object = sts_client.assume_role(`
	`RoleArn=sm_read_role,`	

Tâche	Description	Compétences requises

	RoleSessionName="CrossAccountRoleAssumption",
	ExternalId="YOUR_EXTERNAL_ID",
	)
	credentials = assumed_role_object['Credentials']
	
	secret_dict = ast.literal_eval(get_secret(credentials, secret_name, sm_region))
	execute_query(secret_dict, sql_query, s3_bucket_path, chained_s3_write_role, s3_bucket_region, redshift_db)
	
	return {
	'statusCode': 200
	}	

Tâche	Description	Compétences requises

Découvrez le secret.	Pour obtenir le secret Amazon Redshift, utilisez l'exemple de code suivant :
	
	`def get_secret(credentials, secret_name, sm_region):`
	`  # Create a Secrets Manager client`
	`  session = boto3.session.Session()`
	`  sm_client = session.client(`
	`  service_name='secretsmanager',`
	`  aws_access_key_id=credentials['AccessKeyId'],`
	`  aws_secret_access_key=credentials['SecretAccessKey'],`
	`  aws_session_token=credentials['SessionToken'],`
	`  region_name=sm_region`
	`  )`
	
	`  try:`
	`  get_secret_value_response = sm_client.get_secret_value(`
	`  SecretId=secret_name`
	`  )`
	`  except ClientError as e:`
	`  print(e)`
	`  raise e`
		Développeur d’applications

Tâche	Description	Compétences requises

	`else:`
	`  if 'SecretString' in get_secret_value_response:`
	`  return get_secret_value_response['SecretString']`
	`  else:`
	`  return base64.b64decode(get_secret_value_response['SecretBinary'])`	

Tâche	Description	Compétences requises

Exécutez la commande de déchargement.	Pour décharger les données dans le compartiment S3, utilisez l'exemple de code suivant.
	
	`def execute_query(secret_dict, sql_query, s3_bucket_path, chained_s3_write_role, s3_bucket_region, redshift_db):`
	`  conn_string = "dbname='%s' port='%s' user='%s' password='%s' host='%s'" \`
	`  %(redshift_db, secret_dict["port"], secret_dict["username"], secret_dict["password"], secret_dict["host"])`
	
	`  con = psycopg2.connect(conn_string)`
	
	`  unload_command = "UNLOAD ('{}') TO '{}' IAM_ROLE '{}' DELIMITER '|' REGION '{}';" \`
	`  .format(sql_query, s3_bucket_path +`
		Développeur d’applications

Tâche	Description	Compétences requises

	<pre>str(datetime.datetime.now()) + ".csv",
	
	chained_s3_write_role,
	
	s3_bucket_region)
	
	# Opening a cursor and run query
	cur = con.cursor()
	cur.execute(unload_command)
	
	print(cur.fetchone())
	cur.close()
	con.close()</pre>	

Nettoyage

Tâche	Description	Compétences requises
Supprimez la fonction Lambda.	Pour éviter d'encourir des coûts imprévus, supprimez les ressources et la connexion entre les comptes DEV et PROD. Pour supprimer la fonction Lambda, procédez comme suit : 1. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.	DevOps ingénieur

Tâche	Description	Compétences requises
	2. Localisez et sélectionnez la fonction Lambda que vous avez créée. 3. Choisissez Actions, puis Supprimer. 4. Confirmez la suppression.	

Tâche	Description	Compétences requises
Supprimez les rôles et les politiques IAM.	Supprimez les rôles et politiques IAM des comptes DEV et PROD. Dans le compte DEV, procédez comme suit : 1. Ouvrez la console IAM. 2. Supprimez les rôles suivants : • `S3-Write-Role` • `CrossAccount-RM-Read-Role` (Rôle Lambda) 3. Supprimez les politiques associées : • `S3-Write-Policy` • La CrossAccount politique à suivre pour assumer les rôles liés aux comptes PROD Dans le compte PROD, procédez comme suit : 1. Ouvrez la console IAM. 2. Supprimez les rôles suivants : • `SM-Read-Role` • `CrossAccount-S3-Write-Role` 3. Supprimez les politiques associées :	DevOps ingénieur

Tâche	Description	Compétences requises
	• CrossAccount Politique d'accès à Secrets Manager • `S3-Write-Role-Assume-Policy`	
Supprimez le secret dans Secrets Manager.	Pour supprimer le secret, procédez comme suit : 1. Dans le compte PROD, ouvrez la console Secrets Manager. 2. Localisez et sélectionnez le secret nommé`Redshift-Creds-Secret` . 3. Choisissez Actions, puis Delete secret (Supprimer le secret). 4. Confirmez la suppression.	DevOps ingénieur

Tâche	Description	Compétences requises
Supprimez les règles de peering et de groupe de sécurité des VPC.	Pour supprimer les règles de peering et de groupe de sécurité VPC, procédez comme suit : 1. Dans le compte PROD, ouvrez la EC2 console Amazon à https://console.aws.amazon.com/ec2/ l'adresse. 2. Accédez aux groupes de sécurité. 3. Trouvez le groupe de sécurité utilisé par le cluster Amazon Redshift. 4. Modifiez les règles entrantes et supprimez la règle qui autorise les connexions depuis le VPC Lambda du compte DEV. 5. Accédez à Connexions d'appairage VPC et supprimez la connexion d'appairage.	DevOps ingénieur

Tâche	Description	Compétences requises
Supprimez les données du compartiment S3.	Pour supprimer les données d'Amazon S3, procédez comme suit : 1. Dans le compte DEV, ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/. 2. Localisez le compartiment que vous avez utilisé pour le stockage des données. 3. Supprimez les objets contenus dans le compartiment ou supprimez le compartiment dans son intégralité s'il n'est plus nécessaire.	DevOps ingénieur
Nettoyez AWS KMS les clés.	Si vous avez créé des AWS KMS clés personnalisées pour le chiffrement, procédez comme suit : 1. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms/. 2. Localisez toutes les clés créées pour ce modèle. 3. Planifiez la suppression des clés. (Il existe une période d'attente obligatoire pour la suppression des clés).	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez et supprimez les CloudWatch journaux Amazon.	Pour supprimer les CloudWatch journaux, procédez comme suit : 1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/. 2. Vérifiez les groupes de journaux créés par votre fonction Lambda ou votre cluster Amazon Redshift. 3. Supprimez ces groupes de journaux s'ils ne sont plus nécessaires.	DevOps ingénieur

Ressources connexes

- CloudWatch Documentation Amazon
- Documentation IAM
- Documentation Lambda
- Documentation Amazon Redshift
- Documentation Amazon S3
- AWS Secrets Manager documentation
- AWS principes de sécurité

Informations supplémentaires

Après avoir déchargé les données d'Amazon Redshift vers Amazon S3, vous pouvez les analyser à l'aide d'Amazon Athena.

Amazon Athena est un service de requêtes de données volumineuses qui s'avère utile lorsque vous devez accéder à de gros volumes de données. Vous pouvez utiliser Athena sans avoir à

approvisionner des serveurs ou des bases de données. Athena prend en charge les requêtes complexes et vous pouvez l'exécuter sur différents objets.

Comme c'est le cas pour la plupart des autres Services AWS, le principal avantage d'Athena est qu'elle offre une grande flexibilité dans la façon dont vous exécutez les requêtes sans complexité supplémentaire. Lorsque vous utilisez Athena, vous pouvez interroger différents types de données, tels que CSV et JSON, dans Amazon S3 sans modifier le type de données. Vous pouvez interroger des données provenant de différentes sources, y compris extérieures AWS. Athena réduit la complexité car vous n'avez pas à gérer de serveurs. Athena lit les données directement depuis Amazon S3 sans les charger ni les modifier avant que vous n'exécutiez la requête.

Modèles de migration de base de données par charge de travail

Rubriques

- IBM
- Microsoft
- N/A
- Open source
- Oracle
- SAP

IBM

- Migrer une base de données DB2 d'Amazon EC2 vers Aurora compatible avec MySQL à l'aide d'AWS DMS
- Migrez Db2 for LUW vers Amazon EC2 en utilisant l'expédition des journaux pour réduire les temps d'arrêt
- Migrez Db2 for LUW vers Amazon EC2 avec une reprise après sinistre à haute disponibilité
- Migrez d'IBM Db2 sur Amazon vers une version compatible avec Aurora PostgreSQL EC2 à l'aide d'AWS DMS et d'AWS SCT
- Migrer d'un serveur WebSphere d'applications IBM vers Apache Tomcat sur Amazon EC2
- Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS

Microsoft

- Accélérez la découverte et la migration des charges de travail Microsoft vers AWS
- Accédez aux tables Microsoft SQL Server locales depuis Microsoft SQL Server sur Amazon à EC2 l'aide de serveurs liés
- Évaluez les performances des requêtes pour la migration des bases de données SQL Server vers MongoDB Atlas sur AWS
- Automatisez les tâches de base de données dans l'édition SQL Server Express exécutée sur Amazon à EC2 l'aide AWS Lambda d'un planificateur de tâches
- Modifier les applications Python et Perl pour prendre en charge la migration de bases de données de Microsoft SQL Server vers Amazon Aurora PostgreSQL Compatible Edition
- Configurer le routage en lecture seule dans un groupe de disponibilité Always On dans SQL Server sur AWS
- Création de CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel et Python
- Déployez des instances de cluster de basculement SQL Server sur Amazon EC2 et Amazon à l'aide FSx de Terraform
- Exporter une base de données Microsoft SQL Server vers Amazon S3 à l'aide d'AWS DMS
- Exportez les tables Amazon RDS for SQL Server vers un compartiment S3 à l'aide d'AWS DMS
- SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL
- Ingérez et migrez des instances EC2 Windows vers un compte AWS Managed Services
- Migrer une file d'attente de messagerie de Microsoft Azure Service Bus vers Amazon SQS
- Migrer une base de données Microsoft SQL Server d'Amazon EC2 vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server vers Aurora MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une application .NET de Microsoft Azure App Service vers AWS Elastic Beanstalk
- Migrer une base de données Microsoft SQL Server sur site vers Amazon EC2
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de serveurs liés

- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de méthodes de sauvegarde et de restauration natives
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer une base de données Microsoft SQL Server sur site vers Microsoft SQL Server sur Amazon EC2 exécutant Linux
- Migrez les données de Microsoft Azure Blob vers Amazon S3 à l'aide de Rclone
- Migrer une base de données Microsoft SQL Server sur site vers Amazon à EC2 l'aide du service de migration d'applications
- Migrer une base de données relationnelle vers MongoDB Atlas sur AWS
- Migrer SQL Server vers AWS à l'aide de groupes de disponibilité distribués
- Migrer les certificats SSL Windows vers un Application Load Balancer à l'aide d'ACM
- Réhébergez les charges de travail sur site dans le cloud AWS : liste de contrôle pour la migration
- Résoudre les erreurs de connexion après la migration de Microsoft SQL Server vers le cloud AWS
- Envoyer des notifications pour une instance de base de données Amazon RDS for SQL Server à l'aide d'un serveur SMTP sur site et de Database Mail
- Configurer un pipeline CI/CD pour la migration de base de données à l'aide de Terraform
- Configurez une infrastructure multi-AZ pour un SQL Server Always On FCI à l'aide d'Amazon FSx

N/A

- Créez un processus d'approbation pour les demandes de pare-feu lors d'une migration de réhébergement vers AWS
- Chiffrer une instance de base de données Amazon RDS pour PostgreSQL existante
- Estimation des coûts de stockage pour une table Amazon DynamoDB
- Mettre en œuvre la reprise après sinistre entre régions avec AWS DMS et Amazon Aurora

Open source

- Générez automatiquement un modèle PynamoDB et des fonctions CRUD pour Amazon DynamoDB à l'aide d'une application Python
- Connectez-vous en utilisant un tunnel SSH dans pgAdmin
- Création d'utilisateurs et de rôles d'application dans Aurora PostgreSQL compatible
- Activer les connexions chiffrées pour les instances de base de données PostgreSQL dans Amazon RDS
- Migrer Amazon RDS for Oracle vers Amazon RDS for PostgreSQL avec et en utilisant et AWS SCTAWS DMSAWS CLIAWS CloudFormation
- Migrer une base de données MariaDB sur site vers Amazon RDS for MariaDB à l'aide d'outils natifs
- Migrer une base de données MySQL sur site vers Amazon EC2
- Migrer une base de données MySQL sur site vers Amazon RDS for MySQL
- Migrer une base de données MySQL sur site vers Aurora MySQL
- Migrer une base de données PostgreSQL locale vers Aurora PostgreSQL
- Migrer une base de données Couchbase Server vers Amazon EC2
- Migrez d'IBM WebSphere Application Server vers Apache Tomcat sur Amazon EC2 avec Auto Scaling
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for Oracle à l'aide d'AWS DMS SharePlex
- Migrer d'Oracle GlassFish vers AWS Elastic Beanstalk
- Migrez de PostgreSQL sur EC2 Amazon vers Amazon RDS pour PostgreSQL à l'aide de pglogical
- Migrez les charges de travail de création, de formation et de déploiement de ML vers Amazon à SageMaker l'aide des outils de développement AWS
- Migrez des applications Java sur site vers AWS à l'aide d'AWS App2Container
- Migrez des bases de données MySQL sur site vers Aurora MySQL à l'aide de Percona, XtraBackup Amazon EFS et Amazon S3
- Migrer des tables externes Oracle vers des tables compatibles avec Amazon Aurora PostgreSQL
- Migrer les fonctions et procédures Oracle comportant plus de 100 arguments vers PostgreSQL
- Migrer les charges de travail Redis vers Redis Enterprise Cloud sur AWS
- Surveillez Amazon Aurora pour détecter les instances sans chiffrement
- Redémarrez automatiquement l'agent de réplication AWS sans le désactiver SELinux après le redémarrage d'un serveur source RHEL

- Planifiez des tâches pour Amazon RDS for PostgreSQL et Aurora PostgreSQL à l'aide de Lambda et Secrets Manager
- Configurer la réplication des données entre Amazon RDS for MySQL et MySQL sur EC2 Amazon à l'aide de GTID
- Transportez des bases de données PostgreSQL entre deux instances de base de données Amazon RDS à l'aide de pg_transport
- Déchargez les données d'un cluster Amazon Redshift entre différents comptes vers Amazon S3

Oracle

- Ajoutez HA à Oracle PeopleSoft sur Amazon RDS Custom à l'aide d'une réplique en lecture
- Convertir les requêtes Oracle JSON en SQL de base de données PostgreSQL
- Convertir VARCHAR2 (1) le type de données pour Oracle en type de données booléen pour Amazon Aurora PostgreSQL
- Émulez Oracle DR à l'aide d'une base de données globale Aurora compatible avec PostgreSQL
- Émuler des charges de travail Oracle RAC à l'aide de points de terminaison personnalisés dans Aurora PostgreSQL
- Estimez la taille du moteur Amazon RDS pour une base de données Oracle à l'aide des rapports AWR
- Gérer les blocs anonymes dans les instructions Dynamic SQL dans Aurora PostgreSQL
- Gérez les fonctions Oracle surchargées dans la compatibilité avec Aurora PostgreSQL
- Migrez progressivement d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle SQL Developer et d'AWS SCT
- Chargez des fichiers BLOB dans TEXT en utilisant le codage de fichiers compatible avec Aurora PostgreSQL
- Migrer les instances de base de données Amazon RDS for Oracle vers d'autres comptes utilisant AMS
- Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS
- Migrer une base de données Amazon RDS for Oracle vers Compte AWS une autre Région AWS et AWS DMS l'utiliser pour une réplication continue
- Migrer une instance de base de données Amazon RDS pour Oracle vers un autre VPC
- Migrer une base de données Oracle sur site vers Amazon à l'aide EC2 d'Oracle Data Pump
- Migrer une base de données Oracle sur site vers Amazon OpenSearch Service à l'aide de Logstash
- Migrer une base de données Oracle sur site vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle
- Migrez une base de données Oracle sur site vers Amazon RDS for Oracle en utilisant directement Oracle Data Pump Import via un lien de base de données

- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'Oracle Data Pump
- Migrer une base de données Oracle sur site vers Amazon RDS for PostgreSQL à l'aide d'un assistant Oracle et d'AWS DMS
- Migrer une base de données Oracle sur site vers Oracle sur Amazon EC2
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for MariaDB à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for Oracle à l'aide d'AWS DMS
- Migrer une base de données Oracle vers Amazon DynamoDB à l'aide d'AWS DMS
- Migrer une base de données Oracle vers Amazon RDS for Oracle à l'aide d'adaptateurs de GoldenGate fichiers plats Oracle
- Migrer une base de données Oracle vers Amazon Redshift à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle vers Aurora PostgreSQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une EnterpriseOne base de données Oracle JD Edwards vers AWS à l'aide d'Oracle Data Pump et d'AWS DMS
- Migrer une table partitionnée Oracle vers PostgreSQL à l'aide d'AWS DMS
- Migrer une PeopleSoft base de données Oracle vers AWS à l'aide d'AWS DMS
- Migrer les données d'une base de données Oracle sur site vers Aurora PostgreSQL
- Migrer d'Amazon RDS for Oracle vers Amazon RDS for MySQL
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide de vues matérialisées et d'AWS DMS
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide d'AWS DMS SharePlex
- Migrer d'une base de données Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle GoldenGate
- Migrez d'Oracle sur Amazon EC2 vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer d'Oracle vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer d'Oracle WebLogic vers Apache Tomcat (ToMee) sur Amazon ECS
- Migrer les index basés sur les fonctions d'Oracle vers PostgreSQL
- Migrer les applications existantes d'Oracle Pro*C vers ECPG
- Migrer les valeurs Oracle CLOB vers des lignes individuelles dans PostgreSQL sur AWS

- Migrer les codes d'erreur de la base de données Oracle vers une base de données compatible avec Amazon Aurora PostgreSQL
- Migrer Oracle E-Business Suite vers Amazon RDS Custom
- Migrer les fonctions natives d'Oracle vers PostgreSQL à l'aide d'extensions
- Migrer les variables de liaison Oracle OUT vers une base de données PostgreSQL
- Migrer Oracle PeopleSoft vers Amazon RDS Custom
- Migrer la fonctionnalité Oracle ROWID vers PostgreSQL sur AWS
- Migrer les packages pragma Oracle SERIALLY_REUSERABLE vers PostgreSQL
- Migrer les colonnes générées virtuellement d'Oracle vers PostgreSQL
- Surveillez GoldenGate les journaux Oracle à l'aide d'Amazon CloudWatch
- Replateformage d'Oracle Database Enterprise Edition vers l'édition Standard 2 sur Amazon RDS for Oracle
- Configuration d'une architecture HA/DR pour Oracle E-Business Suite sur Amazon RDS Custom avec une base de données de secours active
- Configuration de la fonctionnalité Oracle UTL_FILE sur Aurora compatible avec PostgreSQL
- Rôles de transition pour une PeopleSoft application Oracle sur Amazon RDS Custom for Oracle
- Valider les objets de base de données après la migration d'Oracle vers Amazon Aurora PostgreSQL

SAP

- Sauvegardez automatiquement les bases de données SAP HANA à l'aide de Systems Manager et EventBridge
- Migrer une base de données SAP ASE sur site vers Amazon EC2
- Migrez de SAP ASE vers Amazon RDS for SQL Server à l'aide d'AWS DMS
- Migrez SAP ASE sur Amazon EC2 vers Amazon Aurora PostgreSQL compatible avec AWS SCT et AWS DMS
- Migrez SAP HANA vers AWS à l'aide de SAP HSR avec le même nom d'hôte
- Réduisez le temps de migration homogène vers SAP en utilisant le service de migration d'applications
- Configuration de la reprise après sinistre pour SAP sur IBM Db2 on AWS

Plus de modèles

- Accédez à une base de données Amazon Neptune depuis un conteneur Amazon EKS
- Accédez aux tables Amazon DynamoDB, interrogez-les et joignez-les à l'aide d'Athena
- Données agrégées dans Amazon DynamoDB pour les prévisions de machine learning dans Athena
- Autoriser EC2 les instances à accéder en écriture aux compartiments S3 dans les comptes AMS
- Analysez et visualisez des données JSON imbriquées avec Amazon Athena et Amazon QuickSight
- Authentifier Microsoft SQL Server sur Amazon à EC2 l'aide d'AWS Directory Service
- Automatisez les sauvegardes pour les instances de base de données Amazon RDS for PostgreSQL à l'aide d'AWS Batch
- Archivez automatiquement les éléments sur Amazon S3 à l'aide de DynamoDB TTL
- Corriger automatiquement les instances et clusters de base de données Amazon RDS non chiffrés
- Arrêtez et démarrez automatiquement une instance de base de données Amazon RDS à l'aide de AWS Systems Manager Maintenance Windows
- Créez une architecture faiblement couplée avec des microservices en utilisant DevOps Practices et AWS Cloud9
- Créez des programmes COBOL DB2 en utilisant et AWS Mainframe ModernizationAWS CodeBuild
- Créez un maillage de données d'entreprise avec Amazon DataZone AWS CDK, et AWS CloudFormation
- Modifier les applications Python et Perl pour prendre en charge la migration de bases de données de Microsoft SQL Server vers Amazon Aurora PostgreSQL Compatible Edition
- Convertissez et décompressez les données EBCDIC en ASCII sur AWS à l'aide de Python
- Convertir la fonctionnalité temporelle Teradata NORMALIZE en Amazon Redshift SQL
- Convertir la fonctionnalité Teradata RESET WHEN en Amazon Redshift SQL
- Convertir VARCHAR2 (1) le type de données pour Oracle en type de données booléen pour Amazon Aurora PostgreSQL
- Création d'utilisateurs et de rôles d'application dans Aurora PostgreSQL compatible
- Création de CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel et Python
- Fournissez des enregistrements DynamoDB à Amazon S3 à l'aide de Kinesis Data Streams et Firehose avec AWS CDK

- Déployez un cluster Cassandra sur Amazon EC2 avec une statique privée IPs pour éviter le rééquilibrage
- Développez des assistants avancés basés sur l'IA générative basés sur le chat en utilisant RAG et des instructions ReAct
- Émulez Oracle DR à l'aide d'une base de données globale Aurora compatible avec PostgreSQL
- Activez le chiffrement transparent des données dans Amazon RDS for SQL Server
- Exporter une base de données Microsoft SQL Server vers Amazon S3 à l'aide d'AWS DMS
- SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL
- Migrez progressivement d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle SQL Developer et d'AWS SCT
- Chargez des fichiers BLOB dans TEXT en utilisant le codage de fichiers compatible avec Aurora PostgreSQL
- Gérez les informations d'identification à l'aide d'AWS Secrets Manager
- Migrer une base de données DB2 d'Amazon EC2 vers Aurora compatible avec MySQL à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server d'Amazon EC2 vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server vers Aurora MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer un environnement MongoDB auto-hébergé vers MongoDB Atlas sur AWS
- Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS
- Migrer Amazon RDS for Oracle vers Amazon RDS for PostgreSQL avec et en utilisant et AWS SCTAWS DMSAWS CLIAWS CloudFormation
- Migrer une instance de base de données Amazon RDS vers un autre VPC ou un autre compte
- Migrer une base de données Amazon RDS for Oracle vers Compte AWS une autre Région AWS et AWS DMS l'utiliser pour une réplication continue
- Migrer une instance de base de données Amazon RDS pour Oracle vers un autre VPC
- Migrer un cluster Amazon Redshift vers une région AWS en Chine

- Migrer une base de données MariaDB sur site vers Amazon RDS for MariaDB à l'aide d'outils natifs
- Migrer une base de données Microsoft SQL Server sur site vers Amazon EC2
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de serveurs liés
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de méthodes de sauvegarde et de restauration natives
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer une base de données Microsoft SQL Server sur site vers Microsoft SQL Server sur Amazon EC2 exécutant Linux
- Migrer une base de données MySQL sur site vers Amazon EC2
- Migrer une base de données MySQL sur site vers Amazon RDS for MySQL
- Migrer une base de données MySQL sur site vers Aurora MySQL
- Migrer une base de données Oracle sur site vers Amazon à l'aide EC2 d'Oracle Data Pump
- Migrer une base de données Oracle sur site vers Amazon OpenSearch Service à l'aide de Logstash
- Migrer une base de données Oracle sur site vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle
- Migrez une base de données Oracle sur site vers Amazon RDS for Oracle en utilisant directement Oracle Data Pump Import via un lien de base de données
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'Oracle Data Pump
- Migrer une base de données Oracle sur site vers Amazon RDS for PostgreSQL à l'aide d'un assistant Oracle et d'AWS DMS
- Migrer une base de données Oracle sur site vers Oracle sur Amazon EC2
- Migrer une base de données PostgreSQL locale vers Aurora PostgreSQL
- Migrer une base de données SAP ASE sur site vers Amazon EC2
- Migrer une base de données ThoughtSpot Falçon sur site vers Amazon Redshift

- Migrer une base de données Vertica sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for MariaDB à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for Oracle à l'aide d'AWS DMS
- Migrer une base de données Oracle vers Amazon DynamoDB à l'aide d'AWS DMS
- Migrer une base de données Oracle vers Amazon RDS for Oracle à l'aide d'adaptateurs de GoldenGate fichiers plats Oracle
- Migrer une base de données Oracle vers Amazon Redshift à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle vers Aurora PostgreSQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une EnterpriseOne base de données Oracle JD Edwards vers AWS à l'aide d'Oracle Data Pump et d'AWS DMS
- Migrer une table partitionnée Oracle vers PostgreSQL à l'aide d'AWS DMS
- Migrer une PeopleSoft base de données Oracle vers AWS à l'aide d'AWS DMS
- Migrer une base de données Couchbase Server vers Amazon EC2
- Migrer les données d'une base de données Oracle sur site vers Aurora PostgreSQL
- Migrez les données vers le à AWS Cloud l'aide de Starburst
- Migrez Db2 for LUW vers Amazon EC2 en utilisant l'expédition des journaux pour réduire les temps d'arrêt
- Migrez Db2 for LUW vers Amazon EC2 avec une reprise après sinistre à haute disponibilité
- Migrer d'Amazon RDS for Oracle vers Amazon RDS for MySQL
- Migrer du serveur Couchbase vers Couchbase Capella sur AWS
- Migrez d'IBM Db2 sur Amazon vers une version compatible avec Aurora PostgreSQL EC2 à l'aide d'AWS DMS et d'AWS SCT
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide de vues matérialisées et d'AWS DMS
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide d'AWS DMS SharePlex
- Migrer d'une base de données Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle GoldenGate
- Migrez d'Oracle sur Amazon EC2 vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT

- Migrer d'Oracle vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrez de PostgreSQL sur EC2 Amazon vers Amazon RDS pour PostgreSQL à l'aide de pglogical
- Migrez de SAP ASE vers Amazon RDS for SQL Server à l'aide d'AWS DMS
- Migrer les index basés sur les fonctions d'Oracle vers PostgreSQL
- Migrer les applications existantes d'Oracle Pro*C vers ECPG
- Migrer une base de données Microsoft SQL Server sur site vers Amazon à EC2 l'aide du service de migration d'applications
- Migrez les charges de travail Cloudera sur site vers Cloudera Data Platform sur AWS
- Migrez des bases de données MySQL sur site vers Aurora MySQL à l'aide de Percona, XtraBackup Amazon EFS et Amazon S3
- Migrer Oracle Business Intelligence 12c vers le cloud AWS à partir de serveurs sur site
- Migrer les valeurs Oracle CLOB vers des lignes individuelles dans PostgreSQL sur AWS
- Migrer les codes d'erreur de la base de données Oracle vers une base de données compatible avec Amazon Aurora PostgreSQL
- Migrer Oracle E-Business Suite vers Amazon RDS Custom
- Migrer des tables externes Oracle vers des tables compatibles avec Amazon Aurora PostgreSQL
- Migrer les fonctions natives d'Oracle vers PostgreSQL à l'aide d'extensions
- Migrer Oracle PeopleSoft vers Amazon RDS Custom
- Migrer la fonctionnalité Oracle ROWID vers PostgreSQL sur AWS
- Migrer les packages pragma Oracle SERIALLY_REUSERABLE vers PostgreSQL
- Migrer les charges de travail Redis vers Redis Enterprise Cloud sur AWS
- Migrer une base de données relationnelle vers MongoDB Atlas sur AWS
- Migrez SAP ASE sur Amazon EC2 vers Amazon Aurora PostgreSQL compatible avec AWS SCT et AWS DMS
- Migrer les colonnes générées virtuellement d'Oracle vers PostgreSQL
- Configurez un espace de données minimum viable pour partager les données entre les organisations
- Surveillez les ElastiCache clusters Amazon pour le chiffrement au repos
- Surveiller les ElastiCache clusters pour les groupes de sécurité
- Interrogez les tables Amazon DynamoDB avec SQL à l'aide d'Amazon Athena

- Réduisez le temps de migration homogène vers SAP en utilisant le service de migration d'applications
- Rotation des informations d'identification de base de données sans redémarrer les conteneurs
- Exécutez des charges de travail basées sur les messages à grande échelle à l'aide d'AWS Fargate
- Sécurisez et rationalisez l'accès des utilisateurs dans une base de données de fédération DB2 sur AWS en utilisant des contextes fiables
- Configuration d'une PeopleSoft architecture à haute disponibilité sur AWS
- Configuration de la fonctionnalité Oracle UTL_FILE sur Aurora compatible avec PostgreSQL
- Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS
- Simplifiez les déploiements de PostgreSQL sur Amazon EKS à l'aide de PGO
- Transférez des données Db2 z/OS à grande échelle vers Amazon S3 dans des fichiers CSV
- Transportez des bases de données PostgreSQL entre deux instances de base de données Amazon RDS à l'aide de pg_transport
- Valider les objets de base de données après la migration d'Oracle vers Amazon Aurora PostgreSQL
- Vérifiez que les nouveaux clusters Amazon Redshift sont lancés dans un VPC

Stockage et sauvegarde

Rubriques

- Autoriser EC2 les instances à accéder en écriture aux compartiments S3 dans les comptes AMS
- Automatisez l'ingestion de flux de données dans une base de données Snowflake à l'aide de Snowflake Snowpipe, Amazon S3, Amazon SNS et Amazon Data Firehose
- Chiffrez automatiquement les volumes Amazon EBS existants et nouveaux
- Sauvegardez les serveurs Sun SPARC dans l'émulateur Stromasys Charon-SSP sur le cloud AWS
- Sauvegardez et archivez les données sur Amazon S3 avec Veeam Backup & Replication
- Configuration de Veritas NetBackup pour le VMware cloud sur AWS
- Copiez les données d'un compartiment S3 vers un autre compte ou une autre région à l'aide de l'AWS CLI
- Copiez les données d'un compartiment S3 vers un autre compte et une autre région à l'aide de S3 Batch Replication
- Migrez les données d'un environnement Hadoop sur site vers Amazon S3 à l'aide d' DistCp AWS PrivateLink pour Amazon S3
- Plus de modèles

Autoriser EC2 les instances à accéder en écriture aux compartiments S3 dans les comptes AMS

Créée par Mansi Suratwala (AWS)

Récapitulatif

AWS Managed Services (AMS) vous aide à exploiter votre AWS infrastructure de manière plus efficace et plus sûre. Les comptes AMS sont dotés de dispositifs de sécurité pour une administration standardisée de vos AWS ressources. L'un des obstacles est que les profils d'instance Amazon Elastic Compute Cloud EC2 (Amazon) par défaut n'autorisent pas l'accès en écriture aux compartiments Amazon Simple Storage Service (Amazon S3). Toutefois, votre organisation peut disposer de plusieurs compartiments S3 et avoir besoin d'un contrôle accru de l'accès par EC2 les instances. Par exemple, vous souhaiterez peut-être stocker des sauvegardes de base de données à partir d' EC2 instances dans un compartiment S3.

Ce modèle explique comment utiliser requests for change (RFCs) pour permettre à vos EC2 instances d'accéder en écriture aux compartiments S3 de votre compte AMS. Une RFC est une demande créée par vous ou AMS pour apporter une modification à votre environnement géré et qui inclut un ID de type de modification (CT) pour une opération particulière.

Conditions préalables et limitations

Prérequis

- Un compte AMS Advanced. Pour plus d'informations à ce sujet, consultez les plans d'opérations AMS dans la documentation AMS.
- Accès au `customer-mc-user-role` rôle AWS Identity and Access Management (IAM) à soumettre RFCs.
- AWS Command Line Interface (AWS CLI), installé et configuré avec les EC2 instances de votre compte AMS.
- Compréhension de la manière de créer et de soumettre RFCs dans AMS. Pour plus d'informations à ce sujet, voir Quels sont les types de modifications AMS ? dans la documentation AMS.
- Compréhension des types de modifications manuels et automatisés (CTs). Pour plus d'informations à ce sujet, consultez Automatisé et manuel CTs dans la documentation AMS.

Architecture

Pile technologique

- AMS
- AWS CLI
- Amazon EC2
- Amazon S3
- IAM

Outils

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Managed Services (AMS) vous aide à exploiter votre infrastructure AWS de manière plus efficace et plus sécurisée.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.

Épopées

Création d'un compartiment S3 avec une RFC

Tâche	Description	Compétences requises
Créez un compartiment S3 à l'aide d'une RFC automatisée.	1. Connectez-vous à votre compte AMS, choisissez la page Choisir le type de modification RFCs, puis choisissez Create RFC.	Administrateur système AWS, développeur AWS

Tâche	Description	Compétences requises
	2. Soumettez la RFC automatisée Create S3 Bucket. **Note** Assurez-vous d'enregistrer le nom du compartiment S3.	

Créez un profil d'instance IAM et associez-le aux EC2 instances

Tâche	Description	Compétences requises
Soumettez une RFC manuelle pour créer un rôle IAM.	Lorsqu'un compte AMS est intégré, un profil d'instanc e IAM par défaut nommé `customer-mc-ec2-in stance-profile` est créé et associé à chaque EC2 instance de votre compte AMS. Toutefois, le profil d'instance ne dispose pas d'autorisations d'écriture sur vos compartiments S3. Pour ajouter les autorisat ions d'écriture, soumettez la RFC du manuel Create IAM Resource pour créer un rôle IAM doté des trois politique s suivantes :`customer_ ec2_instance_` , `customer_deny_policy`	Administrateur système AWS, développeur AWS

Tâche	Description	Compétences requises
	et. `customer_ec2_s3_integration_policy`	

> **Important**
>
> Les `customer_deny_policy` politiques `customer_ec2_instance_` et existent déjà dans votre compte AMS. Toutefois, vous devez créer à l'aide `customer_ec2_s3_integration_policy` de l'exemple de politique suivant :

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Sid": "",
       "Effect": "Allow",
       "Principal": {
         "Service": "ec2.amazonaws.com"
       },
       "Action": "sts:AssumeRole"
    }
  ]
```

Tâche	Description	Compétences requises

	}
	
	Role Permissions:
	{
	"Version":
	"2012-10-17",
	"Statement": [
	{
	"Action": [
	
	"s3:ListBucket",
	
	"s3:GetBucketLocat
	ion"
	],
	"Resource
	": "arn:aws:s3:::",
	"Effect":
	"Allow"
	},
	{
	"Action": [
	
	"s3:GetObject",
	
	"s3:PutObject",
	
	"s3:ListMultipartU
	ploadParts",
	
	"s3:AbortMultipart
	Upload"
	],
	"Resource
	": "arn:aws:s3:::/*",
	"Effect":
	"Allow"
	}
	]
	}	

Tâche	Description	Compétences requises
Soumettez une RFC manuelle pour remplacer le profil d'instance IAM.	Soumettez une RFC manuelle pour associer les EC2 instances cibles au nouveau profil d'instance IAM.	Administrateur système AWS, développeur AWS
Testez une opération de copie vers le compartiment S3.	Testez une opération de copie vers le compartiment S3 en exécutant la commande suivante dans AWS CLI : `aws s3 cp test.txt s3://<S3 bucket>/test2.txt`	Administrateur système AWS, développeur AWS

Ressources connexes

- Créez un profil d'instance IAM pour vos instances Amazon EC2
- Création d'un compartiment S3 (à l'aide de la console Amazon S3 AWS SDKs, ou AWS CLI)

Automatisez l'ingestion de flux de données dans une base de données Snowflake à l'aide de Snowflake Snowpipe, Amazon S3, Amazon SNS et Amazon Data Firehose

Créée par Bikash Chandra Rout (AWS)

Récapitulatif

Ce modèle décrit comment utiliser les services du cloud Amazon Web Services (AWS) pour traiter un flux continu de données et le charger dans une base de données Snowflake. Le modèle utilise Amazon Data Firehose pour transmettre les données à Amazon Simple Storage Service (Amazon S3), Amazon Simple Notification Service (Amazon SNS) pour envoyer des notifications lorsque de nouvelles données sont reçues, et Snowflake Snowpipe pour charger les données dans une base de données Snowflake.

En suivant ce modèle, vous pouvez disposer de données générées en continu et disponibles pour analyse en quelques secondes, éviter de multiples `COPY` commandes manuelles et bénéficier d'une prise en charge complète des données semi-structurées lors du chargement.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Source de données qui envoie en permanence des données à un flux de diffusion Firehose.
- Un compartiment S3 existant qui reçoit les données du flux de diffusion Firehose.
- Un compte Snowflake actif.

Limites

- Snowflake Snowpipe ne se connecte pas directement à Firehose.

Architecture

Pile technologique

- Amazon Data Firehose

- Amazon SNS
- Amazon S3
- Flocon de neige Snowpipe
- Base de données Snowflake

Outils

- Amazon Data Firehose est un service entièrement géré permettant de diffuser des données de streaming en temps réel vers des destinations telles qu'Amazon S3, Amazon Redshift, OpenSearch Amazon Service, Splunk et tout point de terminaison HTTP personnalisé ou appartenant à des fournisseurs de services tiers pris en charge.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.
- Amazon Simple Notification Service (Amazon SNS) coordonne et gère la mise à disposition ou l'envoi de messages à des clients ou à des points de terminaison abonnés.
- Snowflake — Snowflake est un entrepôt de données analytiques fourni en tant que (SaaS). Software-as-a-Service
- Snowflake Snowpipe — Snowpipe charge les données des fichiers dès qu'ils sont disponibles dans un stage Snowflake.

Épopées

Installez un Snowflake Snowpipe

Tâche	Description	Compétences requises
Créez un fichier CSV dans Snowflake.	Connectez-vous à Snowflake et exécutez la `CREATE FILE FORMAT` commande pour créer un fichier CSV avec un délimiteur de champs spécifié. Pour plus d'informations à ce sujet et sur d'autres commandes Snowflake, consultez la section Informations supplémentaires.	Developer

Tâche	Description	Compétences requises
Créez une scène Snowflake externe.	Exécutez la `CREATE STAGE` commande pour créer un stage Snowflake externe qui fait référence au fichier CSV que vous avez créé précédemment. Important : vous aurez besoin de l'URL du compartiment S3, de votre clé AWS d'accès et de votre clé d'accès AWS secrète. Exécutez la `SHOW STAGES` commande pour vérifier que le stage Snowflake est créé.	Developer
Créez la table cible Snowflake.	Exécutez la `CREATE TABLE` commande pour créer la table Snowflake.	Developer
Créez un tuyau.	Exécutez la `CREATE PIPE` commande ; assurez-vous qu'elle `auto_ingest=true` figure dans la commande. Exécutez la `SHOW PIPES` commande pour vérifier que le canal est créé. Copiez et enregistrez la valeur de la `notification_channel` colonne. Cette valeur sera utilisée pour configurer les notifications d'événements Amazon S3.	Developer

Configuration du compartiment S3

Tâche	Description	Compétences requises
Créez une politique de cycle de vie de 30 jours pour le compartiment S3.	Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la. Choisissez le compartiment S3 qui contient les données de Firehose. Choisissez ensuite l'onglet Gestion dans le compartiment S3 et choisissez Ajouter une règle de cycle de vie. Entrez un nom pour votre règle dans la boîte de dialogue Règle du cycle de vie et configurez une règle de cycle de vie de 30 jours pour votre compartiment. Pour obtenir de l'aide sur ce sujet et sur d'autres articles, consultez la section Ressources connexes.	Administrateur système, développeur
Créez une politique IAM pour le compartiment S3.	Ouvrez la console AWS Identity and Access Management (IAM) et choisissez Policies. Sélectionnez Créer une politique, puis l'onglet JSON. Copiez et collez la politique de la section Informations supplémentaires dans le champ JSON. Cette politique accordera `PutObject` des `DeleteObject` autorisations `GetObject` `GetObjectVersion`, ainsi que des	Administrateur système, développeur

Tâche	Description	Compétences requises
	`ListBucket` autorisations. Choisissez Réviser la politique , entrez un nom de stratégie , puis choisissez Créer une politique.	
Attribuez la politique à un rôle IAM.	Ouvrez la console IAM, sélectionnez Rôles, puis sélectionnez Créer un rôle. Choisissez un autre compte AWS comme entité de confiance. Entrez votre Compte AWS identifiant, puis choisissez Exiger un identifiant externe. Entrez un identifiant d'espace réservé que vous modifierez ultérieurement. Choisissez Next et attribuez la politique IAM que vous avez créée précédemment. Créez ensuite le rôle IAM.	Administrateur système, développeur
Copiez le nom de ressource Amazon (ARN) pour le rôle IAM.	Ouvrez la console IAM, puis sélectionnez Rôles. Choisissez le rôle IAM que vous avez créé précédemment, puis copiez et stockez l'ARN du rôle.	Administrateur système, développeur

Configurer une intégration de stockage dans Snowflake

Tâche	Description	Compétences requises
Créez une intégration de stockage dans Snowflake.	Connectez-vous à Snowflake et exécutez la `CREATE`	Administrateur système, développeur

Tâche	Description	Compétences requises
	`STORAGE INTEGRATION` commande. Cela modifiera la relation de confiance, accordera l'accès à Snowflake et fournira l'identifiant externe pour votre stage Snowflake.	
Récupérez le rôle IAM pour votre compte Snowflake.	Exécutez la `DESC INTEGRATION` commande pour récupérer l'ARN du rôle IAM. **Important** `<integration_name>`est le nom de l'intégration de stockage Snowflake que vous avez créée précédemment.	Administrateur système, développeur
Enregistrez les valeurs de deux colonnes.	Copiez et enregistrez les valeurs des `storage_aws_external_id` colonnes `storage_aws_iam_user_arn` et.	Administrateur système, développeur

Autoriser Snowflake Snowpipe à accéder au compartiment S3

Tâche	Description	Compétences requises
Modifiez la politique de rôle IAM.	Ouvrez la console IAM et choisissez Rôles. Choisissez le rôle IAM que vous avez	Administrateur système, développeur

Tâche	Description	Compétences requises
	créé précédemment et cliquez sur l'onglet Relations de confiance. Choisissez Modifier la relation d'approbation. Remplacez `snowflake_external_id` par la `storage_aws_external_id` valeur que vous avez copiée précédemment. Remplacez `snowflake_user_arn` par la `storage_aws_iam_user_arn` valeur que vous avez copiée précédemment. Choisissez ensuite Mettre à jour la politique de confiance.	

Activer et configurer les notifications SNS pour le compartiment S3

Tâche	Description	Compétences requises
Activez les notifications d'événements pour le compartiment S3.	Ouvrez la console Amazon S3 et choisissez votre compartiment. Choisissez Propriétés, puis sous Paramètres avancés, sélectionnez Événements. Choisissez Ajouter une notification, puis entrez le nom de cet événement. Si vous n'entrez pas de nom, un identifiant global unique (GUID) sera utilisé.	Administrateur système, développeur

Tâche	Description	Compétences requises
Configurez les notifications Amazon SNS pour le compartiment S3.	Sous Événements, choisissez ObjectCreate (Tous), puis choisissez SQS Queue dans la liste déroulante Envoyer vers. Dans la liste SNS, choisissez Ajouter un ARN de file d'attente SQS et collez la `notification_channel` valeur que vous avez copiée précédemment. Ensuite, choisissez Save (Enregistrer).	Administrateur système, développeur
Abonnez la file d'attente Snowflake SQS à la rubrique SNS.	Abonnez la file d'attente Snowflake SQS à la rubrique SNS que vous avez créée. Pour obtenir de l'aide concernant cette étape, consultez la section Ressources connexes.	Administrateur système, développeur

Vérifiez l'intégration de la scène Snowflake

Tâche	Description	Compétences requises
Vérifiez et testez Snowpipe.	Connectez-vous à Snowflake et ouvrez la scène Snowflake. Déposez les fichiers dans votre compartiment S3 et vérifiez si la table Snowflake les charge. Amazon S3 envoie des notifications SNS à Snowpipe lorsque de nouveaux objets apparaissent dans le compartiment S3.	Administrateur système, développeur

Ressources connexes

- Gestion du cycle de vie de votre stockage
- Abonnez la file d'attente Snowflake SQS à la rubrique Amazon SNS

Informations supplémentaires

Créez un format de fichier :

```
CREATE FILE FORMAT <name>
TYPE = 'CSV'
FIELD_DELIMITER = '|'
SKIP_HEADER = 1;
```

Créez une scène externe :

```
externalStageParams (for Amazon S3) ::=
  URL = 's3://[//]'

  [ { STORAGE_INTEGRATION =  } | { CREDENTIALS = ( {  { AWS_KEY_ID = `` AWS_SECRET_KEY
 = `` [ AWS_TOKEN = `` ] } | AWS_ROLE = ``  } ) ) }` ]
  [ ENCRYPTION = ( [ TYPE = 'AWS_CSE' ] [ MASTER_KEY = '' ] |
                   [ TYPE = 'AWS_SSE_S3' ] |
                   [ TYPE = 'AWS_SSE_KMS' [ KMS_KEY_ID = '' ] |
                   [ TYPE = NONE ] )
```

Créez une table :

```
CREATE [ OR REPLACE ] [ { [ LOCAL | GLOBAL ] TEMP[ORARY] | VOLATILE } | TRANSIENT ]
 TABLE [ IF NOT EXISTS ]
  <table_name>
    ( <col_name> <col_type> [ { DEFAULT <expr>
                              | { AUTOINCREMENT | IDENTITY } [ ( <start_num> ,
 <step_num> ) | START <num> INCREMENT <num> ] } ]
                               /* AUTOINCREMENT / IDENTITY supported only for numeric
 data types (NUMBER, INT, etc.) */
                           [ inlineConstraint ]
      [ , <col_name> <col_type> ... ]
      [ , outoflineConstraint ]
      [ , ... ] )
  [ CLUSTER BY ( <expr> [ , <expr> , ... ] ) ]
```

```
  [ STAGE_FILE_FORMAT = ( { FORMAT_NAME = '<file_format_name>'
                          | TYPE = { CSV | JSON | AVRO | ORC | PARQUET | XML }
 [ formatTypeOptions ] } ) ]
  [ STAGE_COPY_OPTIONS = ( copyOptions ) ]
  [ DATA_RETENTION_TIME_IN_DAYS = <num> ]
  [ COPY GRANTS ]
  [ COMMENT = '<string_literal>' ]
```

Afficher les étapes :

```
SHOW STAGES;
```

Créez un tube :

```
CREATE [ OR REPLACE ] PIPE [ IF NOT EXISTS ]
  [ AUTO_INGEST = [ TRUE | FALSE ] ]
  [ AWS_SNS_TOPIC =  ]
  [ INTEGRATION = '' ]
  [ COMMENT = '' ]
  AS
```

Afficher les pipes :

```
SHOW PIPES [ LIKE '<pattern>' ]
           [ IN { ACCOUNT | [ DATABASE ] <db_name> | [ SCHEMA ] <schema_name> } ]
```

Créez une intégration de stockage :

```
CREATE STORAGE INTEGRATION <integration_name>
  TYPE = EXTERNAL_STAGE
  STORAGE_PROVIDER = S3
  ENABLED = TRUE
  STORAGE_AWS_ROLE_ARN = '<iam_role>'
  STORAGE_ALLOWED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/')
  [ STORAGE_BLOCKED_LOCATIONS = ('s3://<bucket>/<path>/', 's3://<bucket>/<path>/') ]
```

Exemple :

```
create storage integration s3_int
  type = external_stage
  storage_provider = s3
```

```
  enabled = true
  storage_aws_role_arn = 'arn:aws:iam::001234567890:role/myrole'
  storage_allowed_locations = ('s3://amzn-s3-demo-bucket1/mypath1/', 's3://amzn-s3-
demo-bucket2/mypath2/')
  storage_blocked_locations = ('s3://amzn-s3-demo-bucket1/mypath1/sensitivedata/',
 's3://amzn-s3-demo-bucket2/mypath2/sensitivedata/');
```

Pour plus d'informations sur cette étape, consultez Configuration d'une intégration de stockage Snowflake pour accéder à Amazon S3 à partir de la documentation Snowflake.

Décrivez une intégration :

```
DESC INTEGRATION <integration_name>;
```

Politique relative aux compartiments S3 :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:PutObject",
              "s3:GetObject",
              "s3:GetObjectVersion",
              "s3:DeleteObject",
              "s3:DeleteObjectVersion"
            ],
            "Resource": "arn:aws:s3:::/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::",
            "Condition": {
                "StringLike": {
                    "s3:prefix": [
                        "/*"
                    ]
                }
            }
        }
    ]
```

```
}
```

Chiffrez automatiquement les volumes Amazon EBS existants et nouveaux

Créée par Tony DeMarco (AWS) et Josh Joy (AWS)

Récapitulatif

Le chiffrement des volumes Amazon Elastic Block Store (Amazon EBS) est important pour la stratégie de protection des données d'une entreprise. Il s'agit d'une étape importante dans la mise en place d'un environnement bien conçu. Bien qu'il n'existe aucun moyen direct de chiffrer des volumes ou des instantanés EBS non chiffrés existants, vous pouvez les chiffrer en créant un nouveau volume ou un nouvel instantané. Pour plus d'informations, consultez Encrypt EBS resources dans la documentation Amazon EC2 . Ce modèle fournit des contrôles préventifs et de détection pour chiffrer vos volumes EBS, qu'ils soient nouveaux ou existants. Dans ce modèle, vous configurez les paramètres du compte, créez des processus de correction automatisés et implémentez des contrôles d'accès.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- Interface de ligne de commande AWS (AWS CLI), installée et configurée sous macOS, Linux ou Windows
- jq, installé et configuré sur macOS, Linux ou Windows
- Les autorisations AWS Identity and Access Management (IAM) sont accordées pour avoir un accès en lecture et en écriture à AWS, CloudFormation Amazon Elastic Compute Cloud EC2 (Amazon), AWS Systems Manager, AWS Config et AWS Key Management Service (AWS KMS)
- AWS Organizations est configuré avec toutes les fonctionnalités activées, une exigence des politiques de contrôle des services
- AWS Config est activé dans les comptes cibles

Limites

- Dans votre compte AWS cible, il ne doit pas y avoir de règles AWS Config nommées encrypted-volumes. Cette solution déploie une règle portant ce nom. Les règles préexistantes portant ce nom peuvent entraîner l'échec du déploiement et entraîner des frais inutiles liés au traitement de la même règle plusieurs fois.

- Cette solution chiffre tous les volumes EBS avec la même clé AWS KMS.
- Si vous activez le chiffrement des volumes EBS pour le compte, ce paramètre est spécifique à la région. Si vous l'activez pour une région AWS, vous ne pouvez pas le désactiver pour des volumes ou des instantanés individuels dans cette région. Pour plus d'informations, consultez la section Chiffrement par défaut dans la EC2 documentation Amazon.
- Lorsque vous corrigez des volumes EBS non chiffrés existants, assurez-vous que l' EC2 instance n'est pas utilisée. Cette automatisation arrête l'instance afin de détacher le volume non chiffré et d'attacher le volume chiffré. Il y a des temps d'arrêt pendant que la correction est en cours. S'il s'agit d'un élément d'infrastructure essentiel pour votre entreprise, assurez-vous que des configurations de haute disponibilité manuelles ou automatiques sont en place afin de ne pas affecter la disponibilité des applications exécutées sur l'instance. Nous vous recommandons de corriger les ressources critiques uniquement pendant les fenêtres de maintenance standard.

Architecture

Flux de travail d'automatisation

1. AWS Config détecte un volume EBS non chiffré.
2. Un administrateur utilise AWS Config pour envoyer une commande de correction à Systems Manager.
3. L'automatisation de Systems Manager prend un instantané du volume EBS non chiffré.
4. L'automatisation de Systems Manager utilise AWS KMS pour créer une copie chiffrée de l'instantané.
5. L'automatisation de Systems Manager effectue les opérations suivantes :
   a. Arrête l' EC2 instance affectée si elle est en cours d'exécution
   b. Attache la nouvelle copie cryptée du volume à l' EC2 instance
   c. Rétablit l'état d'origine de l' EC2 instance

Outils

Services AWS

- CLI AWS — L'interface de ligne de commande AWS (AWS CLI) fournit un accès direct aux interfaces de programmation d'applications publiques APIs () des services AWS. Vous pouvez

explorer les fonctionnalités d'un service avec l'interface de ligne de commande AWS et développer des scripts shell pour gérer vos ressources. Outre les commandes équivalentes aux API de bas niveau, plusieurs services AWS proposent des personnalisations pour l'AWS CLI. Ces personnalisations peuvent inclure des commandes de plus haut niveau qui facilitent l'utilisation d'un service à l'aide d'une API complexe.

- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos ressources AWS. Vous créez un modèle qui décrit toutes les ressources AWS que vous souhaitez (telles que les EC2 instances Amazon), puis vous CloudFormation approvisionnez et configurez ces ressources pour vous.
- AWS Config — AWS Config fournit une vue détaillée de la configuration des ressources AWS dans votre compte AWS. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, pour que vous puissiez observer comment les configurations et les relations changent au fil du temps.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul redimensionnable que vous utilisez pour créer et héberger vos systèmes logiciels.
- AWS KMS — AWS Key Management Service (AWS KMS) est un service de chiffrement et de gestion des clés adapté au cloud. Les clés et fonctionnalités AWS KMS sont utilisées par d'autres services AWS, et vous pouvez les utiliser pour protéger les données dans votre environnement AWS.
- AWS Organizations — AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Systems Manager Automation — Systems Manager Automation simplifie les tâches courantes de maintenance et de déploiement pour les EC2 instances Amazon et les autres ressources AWS.

Autres services

- jq — jq est un processeur JSON en ligne de commande léger et flexible. Vous utilisez cet outil pour extraire des informations clés de la sortie de l'AWS CLI.

Code

- Le code de ce modèle est disponible dans le référentiel Corriger GitHub automatiquement les volumes EBS non chiffrés à l'aide des clés KMS du client.

Épopées

Automatisez la correction des volumes non chiffrés

Tâche	Description	Compétences requises
Téléchargez des scripts et CloudFormation des modèles.	Téléchargez le script shell, le fichier JSON et les CloudFormation modèles depuis le référentiel Corriger GitHub automatiquement les volumes EBS non chiffrés à l'aide des clés KMS du client.	Administrateur AWS, AWS général
Identifiez l'administrateur de la clé AWS KMS.	1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/. 2. Identifiez un utilisateur ou un rôle qui sera l'administrateur des clés AWS KMS. Si un nouvel utilisateur ou un nouveau rôle doit être créé à cette fin, créez-le maintenant. Pour plus d'informations, consultez la section Identités IAM dans la documentation IAM. Cette automatisation crée une nouvelle clé AWS KMS. 3. Une fois identifié, copiez le nom de ressource	Administrateur AWS, AWS général

Tâche	Description	Compétences requises
	Amazon (ARN) de l'utilisateur ou du rôle. Pour plus d'informations, consultez la section IAM ARNs dans la documentation IAM. Vous utiliserez cet ARN à l'étape suivante.	

Tâche	Description	Compétences requises
Déployez le modèle Stack1 CloudFormation .	1. Ouvrez la CloudFormation console AWS à l'adresse https://console.aws.amazon.com/cloudformation/. 2. Dans CloudFormation, déployez le `Stack1.yaml` modèle. Notez les détails de déploiement suivants : • Donnez à la pile un nom clair et descriptif. Notez le nom de la pile car vous aurez besoin de cette valeur à l'étape suivante. • Collez l'ARN de l'administrateur clé dans le seul champ de paramètre de Stack1. Cet utilisateur ou ce rôle devient l'administrateur de la clé AWS KMS créée par la pile. Pour plus d'informations sur le déploiement d'un CloudFormation modèle, consultez la section Utilisation des CloudFormation modèles AWS dans la CloudFormation documentation.	Administrateur AWS, AWS général

Tâche	Description	Compétences requises
Déployez le modèle Stack2. CloudFormation	Dans CloudFormation, déployez le `Stack2.yaml` modèle. Notez les détails de déploiement suivants : • Donnez à la pile un nom clair et descriptif. • Pour le seul paramètre de Stack2, entrez le nom de la pile que vous avez créée à l'étape précédent e. Cela permet à Stack2 de référencer la nouvelle clé et le nouveau rôle AWS KMS déployés par la pile à l'étape précédente.	Administrateur AWS, AWS général
Créez un volume non chiffré à des fins de test.	Créez une EC2 instance avec un volume EBS non chiffré. Pour obtenir des instructions, consultez la section Créer un volume Amazon EBS dans la EC2 documentation Amazon. Le type d'instance n'a pas d'importance et l'accès à l'instance n'est pas nécessair e. Vous pouvez créer une instance t2.micro pour rester dans le niveau gratuit, sans avoir besoin de créer une paire de clés.	Administrateur AWS, AWS général

Tâche	Description	Compétences requises
Testez la règle AWS Config.	1. Ouvrez la console AWS Config à l'adresse https://console.aws.amazon.com/config/. Sur la page Règles, choisissez la règle des volumes chiffrés. 2. Vérifiez que votre nouvelle instance de test non chiffrée apparaît dans la liste des ressources non conformes. Si le volume n'apparaît pas immédiatement, attendez quelques minutes et actualisez les résultats. La règle AWS Config détecte les modifications des ressources peu après la création de l'instance et du volume. 3. Sélectionnez la ressource, puis choisissez Corriger. Vous pouvez consulter la progression et le statut de la correction dans Systems Manager comme suit : 1. Ouvrez la console AWS Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager/. 2. Dans le panneau de navigation de gauche,	Administrateur AWS, AWS général

Tâche	Description	Compétences requises
	sélectionnez Automation (Automatisation). 3. Cliquez sur le lien Execution ID pour afficher les étapes et le statut.	
Configurez des comptes ou des régions AWS supplémen taires.	Si nécessaire pour votre cas d'utilisation, répétez cette épopée pour tous les comptes ou régions AWS supplémen taires.	Administrateur AWS, AWS général

Activer le chiffrement des volumes EBS au niveau du compte

Tâche	Description	Compétences requises
Exécutez le script d'activation.	1. Dans un shell bash, utilisez la `cd` commande pour accéder au référentiel cloné. 2. Saisissez la commande suivante pour exécuter le script `enable-ebs-encryption-for-account` . `./Bash/enable-ebs-encryption-for-account.sh`	Administrateur AWS, AWS général, bash
Vérifiez que les paramètres sont mis à jour.	1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.	Administrateur AWS, AWS général

Tâche	Description	Compétences requises
	2. Sur le côté droit de l'écran, sous Paramètres, choisissez Protection et sécurité des données. 3. Dans la section Chiffrement EBS, vérifiez que l'option Toujours chiffrer les nouveaux volumes EBS est activée et que la clé de chiffrement par défaut est définie sur l'ARN que vous avez spécifié précédemment. **Note** Si le paramètre Toujours chiffrer les nouveaux volumes EBS est désactivé ou si la clé est toujours définie sur alias/aws/ebs, vérifiez que vous êtes connecté au même compte et à la même région AWS où vous avez exécuté le script shell, et vérifiez que votre shell ne contient pas de messages d'erreur.	

Tâche	Description	Compétences requises
Configurez des comptes ou des régions AWS supplémentaires.	Si nécessaire pour votre cas d'utilisation, répétez cette épopée pour tous les comptes ou régions AWS supplémentaires.	Administrateur AWS, AWS général

Empêcher la création d'instances non chiffrées

Tâche	Description	Compétences requises
Créez une politique de contrôle des services.	1. Ouvrez la console AWS Organizations à l'adresse https://console.aws.amazon.com/organizations/v2/. 2. Créez une nouvelle politique de contrôle des services. Pour plus d'informations, consultez la section Création d'une politique de contrôle des services dans la documentation AWS Organizations. 3. Ajoutez le contenu de `DenyUnencryptedEC2.json` à la politique et enregistrez-le. Vous avez téléchargé ce fichier JSON depuis le GitHub dépôt de la première épopée. 4. Attachez cette politique à la racine de l'organisation ou à toute unité organisat	Administrateur AWS, AWS général

Tâche	Description	Compétences requises
	ionnelle nécessaire (OUs). Pour plus d'informations, consultez la section Attacher et détacher des politiques de contrôle des services dans la documenta tion AWS Organizations.	

Ressources connexes

Documentation des services AWS

- AWS CLI
- AWS Config
- AWS CloudFormation
- Amazon EC2
- AWS KMS
- AWS Organizations
- AWS Systems Manager Automation

Autres ressources

- manuel jq (site Web jq)
- télécharger jq () GitHub

Sauvegardez les serveurs Sun SPARC dans l'émulateur Stromasys Charon-SSP sur le cloud AWS

Créée par Kevin Yung (AWS), Luis Ramos (Stromasys) et Rohit Darji (AWS)

Récapitulatif

Ce modèle propose quatre options pour sauvegarder vos serveurs Sun Microsystems SPARC après une migration d'un environnement sur site vers le cloud Amazon Web Services (AWS). Ces options de sauvegarde vous aident à mettre en œuvre un plan de sauvegarde qui répond à l'objectif de point de restauration (RPO) et à l'objectif de temps de restauration (RTO) de votre entreprise, utilise des approches automatisées et réduit vos coûts opérationnels globaux. Le modèle fournit une vue d'ensemble des quatre options de sauvegarde et des étapes à suivre pour les mettre en œuvre.

Si vous utilisez un serveur Sun SPARC hébergé en tant qu'invité sur un émulateur Stromasys Charon-SSP, vous pouvez utiliser l'une des trois options de sauvegarde suivantes :

- Option de sauvegarde 1 : bande virtuelle Stromasys : utilisez la fonction de bande virtuelle Charon-SSP pour configurer une installation de sauvegarde sur le serveur Sun SPARC et archiver vos fichiers de sauvegarde sur Amazon Simple Storage Service (Amazon S3) et Amazon Simple Storage ServiceGlacier à l'aide d'AWS Systems Manager Automation.
- Option de sauvegarde 2 : instantané Stromasys — Utilisez la fonction de capture instantanée Charon-SSP pour configurer une installation de sauvegarde pour les serveurs invités Sun SPARC à Charon-SSP.
- Option de sauvegarde 3 : instantané du volume Amazon Elastic Block Store (Amazon EBS) — Si vous hébergez l'émulateur Charon-SSP sur Amazon Elastic Compute Cloud (Amazon), vous pouvez utiliser un instantané de volume EC2 Amazon EBS pour créer des sauvegardes pour un système de fichiers Sun SPARC.

Si vous utilisez un serveur Sun SPARC hébergé en tant qu'invité sur le matériel et Charon-SSP sur EC2 Amazon, vous pouvez utiliser l'option de sauvegarde suivante :

- Option de sauvegarde 4 : bibliothèque de bandes virtuelles (VTL) AWS Storage Gateway — Utilisez une application de sauvegarde avec une passerelle de bande Storage Gateway VTL pour sauvegarder les serveurs Sun SPARC.

Si vous utilisez un serveur Sun SPARC hébergé en tant que zone personnalisée sur un serveur Sun SPARC, vous pouvez utiliser les options de sauvegarde 1, 2 et 4.

Stromasys fournit des logiciels et des services permettant d'émuler les anciens systèmes critiques SPARC, Alpha, VAX et PA-RISC. Pour plus d'informations sur la migration vers le cloud AWS à l'aide de l'émulation Stromasys, consultez Réhéberger SPARC, Alpha ou d'autres systèmes existants sur AWS avec Stromasys sur le blog AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Serveurs Sun SPARC existants.
- Licences existantes pour Charon-SSP. Les licences pour Charon-SSP sont disponibles sur AWS Marketplace et les licences pour Stromasys Virtual Environment (VE) sont disponibles auprès de Stromasys. Pour plus d'informations, contactez le service commercial de Stromasys.
- Connaissance des serveurs Sun SPARC et des sauvegardes Linux.
- Connaissance de la technologie d'émulation Charon-SSP. Pour plus d'informations à ce sujet, consultez la section Émulation de serveurs existants de Stromasys dans la documentation de Stromasys.
- Si vous souhaitez utiliser la fonction de bande virtuelle ou des applications de sauvegarde pour les systèmes de fichiers de vos serveurs Sun SPARC, vous devez créer et configurer les installations de sauvegarde pour le système de fichiers du serveur Sun SPARC.
- Compréhension du RPO et du RTO. Pour plus d'informations à ce sujet, consultez les objectifs de reprise après sinistre du livre blanc sur le pilier de fiabilité dans la documentation AWS Well-Architected Framework.
- Pour utiliser l'option 4 de sauvegarde, vous devez disposer des éléments suivants :
  - Application de sauvegarde logicielle qui prend en charge une passerelle Storage Gateway VTL Tape Gateway. Pour plus d'informations à ce sujet, consultez Working with VTL devices dans la documentation AWS Storage Gateway.
  - Bacula Director ou une application de sauvegarde similaire, installée et configurée. Pour plus d'informations à ce sujet, consultez la documentation de Bacula Director.

Le tableau suivant fournit des informations sur les quatre options de sauvegarde de ce modèle.

Options de sauvegarde	Assure la cohérence des crashs ?	Assure la cohérence des applications ?	Solution d'appliance de sauvegarde virtuelle ?	Cas d'utilisation typiques
Option 1 : bande virtuelle Stromasys	Oui Vous pouvez automatiser les instantanés du système de fichiers Sun SPARC pour sauvegarder les données sur une bande virtuelle. Par exemple, vous pouvez utiliser des instantanés UFS ou ZFS.	Oui Cette option de sauvegarde nécessite un script automatique pour effacer les transactions en cours, configurer un mode en lecture seule ou hors ligne temporaire pendant la capture instantanée du système de fichiers ou effectuer un vidage des données d'une application. Vous pouvez également avoir besoin d'une interruption de l'application ou d'un mode lecture seule.	Oui	Sauvegarde des systèmes de fichiers du serveur Sun SPARC avec des fichiers .tar ou .zip Sauvegarde des données d'application
Option 2 — Instantané Stromasys	Oui	Oui	Non	Instantané du serveur Sun SPARC

Vous devez configurer le gestionnaire Charon-SSP ou utiliser un argument de démarrage en ligne de commande pour activer cette fonctionnalité. Vous devez également exécuter une commande Linux pour demander à l'émulateur Charon-SSP d'enregistrer l'état du serveur invité Sun SPARC dans un fichier instantané. **Important** Vous devez arrêter le serveur invité Sun SPARC.	Cette option de sauvegarde crée un instantané du serveur invité émulé, y compris ses disques virtuels et son vidage de mémoire. **Important** Vous devez arrêter le serveur invité Sun SPARC pendant le snapshot.	Sauvegarde des données d'application

Option 3 — Instantané du volume Amazon EBS	Oui Vous pouvez utiliser AWS Backup pour automatiser le snapshot Amazon EBS.	Oui Cette option de sauvegarde nécessite un script automatique pour effacer les transactions en cours et configurer un arrêt temporaire ou en lecture seule de l'instance EC2 pendant la capture instantanée du volume Amazon EBS. **Important** Cette option de sauvegarde peut nécessiter une interruption de l'application ou le mode lecture seule pour garantir la cohérence	Non	Instantané des systèmes de fichiers du serveur Sun SPARC Sauvegarde des données d'application

des applications.

Option 4 — AWS Storage Gateway VTL	Oui Vous pouvez sauvegarder automatiquement les données de sauvegarde du système de fichiers Sun SPARC sur la VTL à l'aide d'un agent de sauvegarde.	Oui Cette option de sauvegarde nécessite un script automatique pour effacer les transactions en cours et configurer un mode en lecture seule ou hors ligne temporaire pendant le snapshot du système de fichiers ou le vidage des données de l'application. **Important** Cette option de sauvegarde peut nécessiter une interruption de l'application ou le mode lecture seule.	Oui	Un vaste parc de sauvegardes du système de fichiers du serveur Sun SPARC Sauvegarde des données d'application

Limites

- Vous pouvez utiliser les approches de ce modèle pour sauvegarder des serveurs Sun SPARC individuels, mais vous pouvez également utiliser ces options de sauvegarde pour les données partagées si vos applications s'exécutent dans un cluster.

Outils

Option de sauvegarde 1 : bande virtuelle Stromasys

- Émulateur Stromasys Charon-SSP — L'émulateur Charon-SSP crée la réplique virtuelle du matériel SPARC d'origine dans un système informatique standard compatible x86 64 bits. Il exécute le code binaire SPARC d'origine, y compris les systèmes d'exploitation (OSs) tels que SunOS ou Solaris, leurs produits en couches et leurs applications.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul redimensionnable que vous utilisez pour créer et héberger vos systèmes logiciels.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) fournit un système de fichiers set-and-forget élastique simple, sans serveur, à utiliser avec les services cloud AWS et les ressources sur site.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.
- Amazon S3 Glacier — Amazon Simple Storage Service Glacier est une classe de stockage Amazon S3 sécurisée, durable et extrêmement économique pour l'archivage des données et la sauvegarde à long terme.
- AWS Systems Manager Automation — L'automatisation, une fonctionnalité d'AWS Systems Manager, simplifie les tâches courantes de maintenance et de déploiement des EC2 instances et des autres ressources AWS.

Option de sauvegarde 2 : instantané Stromasys

- Émulateur Stromasys Charon-SSP — L'émulateur Charon-SSP crée la réplique virtuelle du matériel SPARC d'origine dans un système informatique standard compatible x86 64 bits. Il exécute le code binaire SPARC d'origine, OSs notamment SunOS ou Solaris, leurs produits en couches et leurs applications.

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul redimensionnable que vous utilisez pour créer et héberger vos systèmes logiciels.
- Amazon EFS — Amazon Elastic File System (Amazon EFS) fournit un système de fichiers set-and-forget élastique simple, sans serveur, à utiliser avec les services cloud AWS et les ressources sur site.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.
- Amazon S3 Glacier — Amazon Simple Storage Service Glacier est une classe de stockage Amazon S3 sécurisée, durable et extrêmement économique pour l'archivage des données et la sauvegarde à long terme.
- AWS Systems Manager Automation — L'automatisation, une fonctionnalité d'AWS Systems Manager, simplifie les tâches courantes de maintenance et de déploiement des EC2 instances et des autres ressources AWS.

Option de sauvegarde 3 : instantané du volume Amazon EBS

- Émulateur Stromasys Charon-SSP — L'émulateur Charon-SSP crée la réplique virtuelle du matériel SPARC d'origine dans un système informatique standard compatible x86 64 bits. Il exécute le code binaire SPARC d'origine, OSs notamment SunOS ou Solaris, leurs produits en couches et leurs applications.
- AWS Backup — AWS Backup est un service de protection des données entièrement géré qui facilite la centralisation et l'automatisation des services AWS, dans le cloud et sur site.
- Amazon EBS — Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances. EC2
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul redimensionnable que vous utilisez pour créer et héberger vos systèmes logiciels.

Option de sauvegarde 4 : AWS Storage Gateway VTL

- Émulateur Stromasys Charon-SSP — L'émulateur Charon-SSP crée la réplique virtuelle du matériel SPARC d'origine dans un système informatique standard compatible x86 64 bits. Il exécute le code binaire SPARC d'origine, OSs notamment SunOS ou Solaris, leurs produits en couches et leurs applications.
- Bacula — Bacula est un système de sauvegarde informatique open source destiné aux entreprises. Pour savoir si votre application de sauvegarde existante prend en charge Tape Gateway, consultez la section Applications de sauvegarde tierces prises en charge pour une Tape Gateway dans la documentation AWS Storage Gateway.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul redimensionnable que vous utilisez pour créer et héberger vos systèmes logiciels.
- Amazon RDS for MySQL — Amazon Relational Database Service (Amazon RDS) prend en charge les instances de base de données exécutant plusieurs versions de MySQL.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.
- Amazon S3 Glacier — Amazon Simple Storage Service Glacier est une classe de stockage Amazon S3 sécurisée, durable et extrêmement économique pour l'archivage des données et la sauvegarde à long terme.
- AWS Storage Gateway — Storage Gateway connecte une appliance logicielle sur site au stockage dans le cloud afin de permettre une intégration parfaite des fonctionnalités de sécurité des données entre votre environnement informatique sur site et l'infrastructure de stockage AWS.

Épopées

Option de sauvegarde 1 — Création d'une sauvegarde sur bande virtuelle Stromasys

Tâche	Description	Compétences requises
Créez un système de fichiers partagé Amazon EFS pour le stockage de fichiers sur bande virtuelle.	Connectez-vous à la console de gestion AWS ou utilisez l'interface de ligne de commande AWS pour créer un système de fichiers Amazon EFS.	Architecte du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations à ce sujet, consultez la section Création d'un système de fichiers Amazon EFS dans la documentation Amazon EFS.	
Configurez l'hôte Linux pour monter le système de fichiers partagé.	Installez le pilote Amazon EFS sur l'instance Amazon EC2 Linux et configurez le système d'exploitation Linux pour monter le système de fichiers partagé Amazon EFS au démarrage. Pour plus d'informations à ce sujet, consultez la section Montage de systèmes de fichiers à l'aide de l'assistant de montage EFS dans la documentation Amazon EFS.	DevOps ingénieur
Installez l'émulateur Charon-SSP.	Installez l'émulateur Charon-SSP sur l'instance Amazon Linux. EC2 Pour plus d'informations à ce sujet, consultez la section Configuration d'une instance cloud AWS pour Charon-SSP dans la documentation de Stromasys.	DevOps ingénieur

Tâche	Description	Compétences requises
Créez un conteneur de fichiers sur bande virtuelle dans le système de fichiers partagé pour chaque serveur invité Sun SPARC.	Exécutez la `touch <vtape-container-name>` commande pour créer un conteneur de fichiers sur bande virtuelle dans le système de fichiers partagé pour chaque serveur invité Sun SPARC déployé dans l'émulateur Charon-SSP.	DevOps ingénieur
Configurez Charon-SSP Manager pour créer des unités de bande virtuelle pour les serveurs invités Sun SPARC.	Connectez-vous à Charon-SSP Manager, créez des unités de bande virtuelle et configurez-les pour utiliser les fichiers de conteneur de bandes virtuelles pour chaque serveur invité Sun SPARC. Pour plus d'informations à ce sujet, consultez le guide de l'utilisateur de Charon-SSP 5.2 pour Linux dans la documentation de Stromasys.	DevOps ingénieur
Vérifiez que le périphérique de bande virtuelle est disponible sur les serveurs invités Sun SPARC.	Connectez-vous à chaque serveur invité Sun SPARC et exécutez la `mt -f /dev/rmt/1` commande pour vérifier que le périphérique de bande virtuelle est configuré dans le système d'exploitation.	DevOps ingénieur

Tâche	Description	Compétences requises
Développez le manuel d'automatisation et d'automatisation de Systems Manager.	Développez le manuel d'automatisation de Systems Manager et configurez les fenêtres de maintenance et les associations dans Systems Manager pour planifier le processus de sauvegarde. Pour plus d'informations à ce sujet, consultez les procédures d'automatisation et la configuration des fenêtres de maintenance dans la documentation d'AWS Systems Manager.	Architecte du cloud
Configurez Systems Manager Automation pour archiver les fichiers conteneurs de bandes virtuelles pivotés.	Utilisez l'exemple de code de l'option Back 1 dans la section Informations supplémentaires pour développer un runbook Systems Manager Automation afin d'archiver les fichiers conteneurs de bandes virtuelles pivotés sur Amazon S3 et Amazon S3 Glacier.	Architecte du cloud

Tâche	Description	Compétences requises
Déployez le runbook Systems Manager Automation pour l'archivage et la planification.	Déployez le runbook Systems Manager Automation et planifiez-le pour qu'il s'exécute automatiquement dans Systems Manager. Pour plus d'informations à ce sujet, consultez les procédures d'automatisation dans la documentation de Systems Manager.	Architecte du cloud

Option de sauvegarde 2 — Création d'un instantané Stromasys

Tâche	Description	Compétences requises
Créez un système de fichiers partagé Amazon EFS pour le stockage de fichiers sur bande virtuelle.	Connectez-vous à la console de gestion AWS ou utilisez l'interface de ligne de commande AWS pour créer un système de fichiers Amazon EFS. Pour plus d'informations à ce sujet, consultez la section Création de votre système de fichiers Amazon EFS dans la documentation Amazon EFS.	Architecte du cloud
Configurez l'hôte Linux pour monter le système de fichiers partagé.	Installez le pilote Amazon EFS dans l'instance Amazon EC2 Linux et configurez le système d'exploitation Linux pour monter le système de	DevOps ingénieur

Tâche	Description	Compétences requises
	fichiers partagé Amazon EFS au démarrage. Pour plus d'informations à ce sujet, consultez la section Montage de systèmes de fichiers à l'aide de l'assistant de montage EFS dans la documentation Amazon EFS.	
Installez l'émulateur Charon-SSP.	Installez l'émulateur Charon-SSP sur l'instance Amazon Linux. EC2 Pour plus d'informations à ce sujet, consultez la section Configuration d'une instance cloud AWS pour Charon-SSP dans la documentation de Stromasys.	DevOps ingénieur
Configurez les serveurs invités Sun SPARC pour qu'ils démarrent avec l'option de capture instantanée.	Utilisez le gestionnaire Charon-SSP pour configurer l'option de capture instantanée pour chaque serveur invité Sun SPARC. Pour plus d'informations à ce sujet, consultez le guide de l'utilisateur de Charon-SSP 5.2 pour Linux dans la documentation de Stromasys.	DevOps ingénieur

Tâche	Description	Compétences requises
Développez le manuel d'automatisation de Systems Manager.	Utilisez l'exemple de code de l'option Backup 2 dans la section Informations supplémentaires pour développer un runbook Systems Manager Automatio n afin d'exécuter à distance la commande de capture instantanée sur un serveur invité Sun SPARC pendant une fenêtre de maintenance.	Architecte du cloud
Déployez le runbook Systems Manager Automation et configurez l'association avec les hôtes Amazon EC2 Linux.	Déployez le runbook Systems Manager Automation et configurez les fenêtres de maintenance et les associati ons dans Systems Manager pour planifier le processus de sauvegarde. Pour plus d'informations à ce sujet, consultez les procédures d'automatisation et la configuration des fenêtres de maintenance dans la documentation d'AWS Systems Manager.	Architecte du cloud

Tâche	Description	Compétences requises
Archivez les instantanés dans un espace de stockage à long terme.	Utilisez le code d'exemple de runbook de la section Informations supplémentaires pour développer un runbook Systems Manager Automatio n afin d'archiver les fichiers de snapshots sur Amazon S3 et Amazon S3 Glacier.	Architecte du cloud

Option de sauvegarde 3 — Création d'un instantané de volume Amazon EBS

Tâche	Description	Compétences requises
Installez l'émulateur Charon-SSP.	Installez l'émulateur Charon-SSP sur l'instance Amazon Linux. EC2 Pour plus d'informations à ce sujet, consultez la section Configuration d'une instance cloud AWS pour Charon-SS P dans la documentation de Stromasys.	DevOps ingénieur
Créez des volumes EBS pour les serveurs invités Sun SPRAC.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon EBS, puis créez des volumes EBS pour les serveurs invités Sun SPRAC. Pour plus d'informations à ce sujet, consultez la section Configuration d'une instance cloud AWS pour Charon-SS	Architecte du cloud

Tâche	Description	Compétences requises
	P dans la documentation de Stromasys.	
Attachez les volumes EBS à l'instance Amazon EC2 Linux.	Sur la EC2 console Amazon, attachez les volumes EBS à l'instance Amazon EC2 Linux. Pour plus d'informations à ce sujet, consultez Attacher un volume Amazon EBS à une instance dans la EC2 documentation Amazon.	AWS DevOps
Mappez les volumes EBS en tant que lecteurs SCSI dans l'émulateur Charon-SSP.	Configurez Charon-SSP Manager pour mapper les volumes EBS en tant que disques SCSI sur les serveurs invités Sun SPARC. Pour plus d'informations à ce sujet, consultez la section de configuration du stockage SCSI du guide Charon-SSP V5.2 pour Linux dans la documentation de Stromasys.	AWS DevOps

Tâche	Description	Compétences requises
Configurez le calendrier AWS Backup pour la capture instantanée des volumes EBS.	Configurez la politique et les plannings d'AWS Backup pour créer des instantanés des volumes EBS. Pour plus d'informations à ce sujet, consultez le didacticiel de sauvegarde et de restauration Amazon EBS à l'aide d'AWS Backup dans la documentation du AWS Developer Center.	AWS DevOps

Option de sauvegarde 4 — Création d'une VTL AWS Storage Gateway

Tâche	Description	Compétences requises
Créez un périphérique Tape Gateway.	Connectez-vous à l'AWS Management Console, ouvrez la console AWS Storage Gateway, puis créez un périphérique Tape Gateway dans un VPC. Pour plus d'informations à ce sujet, consultez la section Création d'une passerelle dans la documentation AWS Storage Gateway.	Architecte du cloud
Créez une instance de base de données Amazon RDS pour le catalogue Bacula.	Ouvrez la console Amazon RDS et créez une instance de base de données Amazon RDS for MySQL.	Architecte du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations à ce sujet, consultez Création d'une instance de base de données MySQL et connexion à une base de données sur une instance de base de données MySQL dans la documentation Amazon RDS.	
Déployez le contrôleur d'application de sauvegarde dans le VPC.	Installez Bacula sur l'EC2 instance, déployez le contrôleur d'application de sauvegarde, puis configurez le stockage de sauvegarde pour qu'il se connecte au périphérique Tape Gateway. Vous pouvez utiliser l'exemple de configuration du démon de stockage Bacula Director dans le `Bacula-storage-daemon-config.txt` fichier (joint). Pour plus d'informations à ce sujet, consultez la documentation de Bacula.	AWS DevOps

Tâche	Description	Compétences requises
Configurez l'application de sauvegarde sur les serveurs invités Sun SPARC.	Configurez un deuxième client pour installer et configurer l'application de sauvegarde sur les serveurs invités Sun SPARC en utilisant l'exemple de configuration de Bacula figurant dans le `SUN-SPARC-Guest-Bacula-Config.txt` fichier (joint).	DevOps ingénieur
Configurez la configuration et planifiez la sauvegarde.	Configurez la configuration et les plannings de sauvegarde dans le contrôleur d'application de sauvegarde à l'aide de l'exemple de configuration de Bacula Director figurant dans le `Bacula-Directory-Config.txt` fichier (joint). Pour plus d'informations à ce sujet, consultez la documentation de Bacula.	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez que la configuration et les plannings de sauvegarde sont corrects.	Suivez les instructions de la documentation de Bacula pour effectuer les tests de validation et de sauvegarde de votre configuration sur les serveurs invités Sun SPARC. Par exemple, vous pouvez utiliser les commandes suivantes pour valider les fichiers de configuration : • `bacula-dir -t -c bacula-dir.conf` • `bacula-fd -t -c bacula-fd.conf` • `bacula-sd -t -c bacula-sd.conf`	DevOps ingénieur

Ressources connexes

- SPARC virtuel Charon avec licence VE
- SPARC virtuel Charon
- Utilisation des services cloud et du stockage d'objets avec Bacula Enterprise Edition
- Objectifs de reprise après sinistre (DR)
- Solutions d'émulation de systèmes Charon Legacy

Informations supplémentaires

Option de sauvegarde 1 — Création d'une bande virtuelle Stromasys

Vous pouvez utiliser l'exemple de code d'exécution de Systems Manager Automation suivant pour démarrer automatiquement la sauvegarde, puis échanger les bandes :

```
...
# example backup script saved in SUN SPARC Server
 #!/usr/bin/bash
 mt -f  rewind
 tar -cvf
 mt -f  offline
...
         mainSteps:
         - action: aws:runShellScript
           name:
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               # Validate tape backup container file exists
               if [ ! -f {{TapeBackupContainerFile}} ]; then
                 logger -s -p local3.warning "Tape backup container file is not exists
 - {{TapeBackupContainerFile}}, create a new one"
                 touch {{TapeBackupContainerFile}}
               fi
         - action: aws:runShellScript
           name: startBackup
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               user={{BACKUP_USER}}
               keypair={{KEYPAIR_PATH}}
               server={{SUN_SPARC_IP}}
               backup_script={{BACKUP_SCRIPT}}
               ssh -i $keypair $user@$server -c "/usr/bin/bash $backup_script"
         - action: aws:runShellScript
           name: swapVirtualDiskContainer
           inputs:
             onFailure: Abort
             timeoutSeconds: "1200"
             runCommand:
             - |
               mv {{TapeBackupContainerFile}} {{TapeBackupContainerFile}}.$(date +%s)
               touch {{TapeBackupContainerFile}}
         - action: aws:runShellScript
```

```
          name: uploadBackupArchiveToS3
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              aws s3 cp {{TapeBackupContainerFile}} s3://{{BACKUP_BUCKET}}/
{{SUN_SPARC_IP}}/$(date '+%Y-%m-%d')/
 ...
```

Option de sauvegarde 2 — Instantané Stromasys

Vous pouvez utiliser l'exemple de code d'exécution de Systems Manager Automation suivant pour automatiser le processus de sauvegarde :

```
     ...

        mainSteps:
        - action: aws:runShellScript
          name: startSnapshot
          inputs:
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              # You may consider some graceful stop of the application before taking a
 snapshot
              # Query SSP PID by configuration file
              # Example: ps ax | grep ssp-4 | grep Solaris10.cfg | awk '{print $1"
"$5}' | grep ssp4 | cut -f1 -d" "
              pid=`ps ax | grep ssp-4 | grep {{SSP_GUEST_CONFIG_FILE}} | awk '{print
$1" "$5}' | grep ssp4 | cut -f1 -d" "`
              if [ -n "${pid}" ]; then
                kill -SIGTSTP ${pid}
              else
                echo "No PID found for SPARC guest with config
 {{SSP_GUEST_CONFIG_FILE}}"
                exit 1
              fi
        - action: aws:runShellScript
          name: startBackup
          inputs:
            onFailure: Abort
```

```
              timeoutSeconds: "1200"
              runCommand:
              - |
                # upload snapshot and virtual disk files into S3
                aws s3 sync {{SNAPSHOT_FOLDER}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
                aws s3 cp {{VIRTUAL_DISK_FILE}} s3://{{BACKUP_BUCKET}}/$(date '+%Y-%m-
%d')/
          - action: aws:runShellScript
            name: restratSPARCGuest
            inputs:
              onFailure: Abort
              timeoutSeconds: "1200"
              runCommand:
              - |
                /opt/charon-ssp/ssp-4u/ssp4u -f {{SSP_GUEST_CONFIG_FILE}} -d -a
 {{SPARC_GUEST_NAME}} --snapshot {{SNAPSHOT_FOLDER}}
 ...
```

Option de sauvegarde 4 — AWS Storage Gateway VTL

Si vous utilisez des zones non globales Solaris pour exécuter des serveurs Sun SPARC existants virtualisés, l'approche des applications de sauvegarde peut être appliquée aux zones non globales exécutées sur les serveurs Sun SPARC (par exemple, le client de sauvegarde peut s'exécuter à l'intérieur des zones non globales). Toutefois, le client de sauvegarde peut également s'exécuter sur l'hôte Solaris et prendre des instantanés des zones non globales. Les instantanés peuvent ensuite être sauvegardés sur une bande.

L'exemple de configuration suivant ajoute le système de fichiers qui héberge les zones non globales de Solaris dans la configuration de sauvegarde de l'hôte Solaris :

```
FileSet {
   Name = "Branded Zones"
   Include {
     Options {
       signature = MD5
     }
     File = /zones
   }
 }
```

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Sauvegardez et archivez les données sur Amazon S3 avec Veeam Backup & Replication

Créée par Jeanna James (AWS), Anthony Fiore (AWS) (AWS) et William Quigley (AWS)

Récapitulatif

Ce modèle détaille le processus d'envoi des sauvegardes créées par Veeam Backup & Replication aux classes de stockage d'objets Amazon Simple Storage Service (Amazon S3) prises en charge en utilisant la fonctionnalité de référentiel de sauvegarde évolutif de Veeam.

Veeam prend en charge plusieurs classes de stockage Amazon S3 afin de répondre au mieux à vos besoins spécifiques. Vous pouvez choisir le type de stockage en fonction de l'accès aux données, de la résilience et des exigences de coût de vos données de sauvegarde ou d'archivage. Par exemple, vous pouvez stocker des données que vous n'avez pas l'intention d'utiliser pendant 30 jours ou plus dans un accès peu fréquent (IA) d'Amazon S3 à moindre coût. Si vous prévoyez d'archiver des données pendant 90 jours ou plus, vous pouvez utiliser Amazon Simple Storage Service Glacier (Amazon S3 Glacier) Flexible Retrieval ou S3 Glacier Deep Archive avec le niveau d'archivage de Veeam. Vous pouvez également utiliser S3 Object Lock pour créer des sauvegardes immuables dans Amazon S3.

Ce modèle n'explique pas comment configurer Veeam Backup & Replication avec une passerelle sur bande intégrée. AWS Storage Gateway Pour plus d'informations sur ce sujet, consultez Veeam Backup & Replication using AWS VTL Gateway - Deployment Guide sur le site Web de Veeam.

> **Warning**
>
> Ce scénario nécessite que les utilisateurs AWS Identity and Access Management (IAM) disposent d'un accès programmatique et d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires. Les clés d'accès peuvent être mises à jour si nécessaire. Pour plus d'informations, consultez la section Mise à jour des clés d'accès dans le guide de l'utilisateur IAM.

Conditions préalables et limitations

Prérequis

- Veeam Backup & Replication, y compris Veeam Availability Suite ou Veeam Backup Essentials, installé (vous pouvez vous inscrire pour bénéficier d'un essai gratuit)
- Licence Veeam Backup & Replication avec fonctionnalité Enterprise ou Enterprise Plus, qui inclut la licence universelle Veeam (VUL)
- Un utilisateur IAM actif ayant accès à un compartiment Amazon S3
- Un utilisateur IAM actif ayant accès à Amazon Elastic Compute Cloud (Amazon EC2) et Amazon Virtual Private Cloud (Amazon VPC), s'il utilise le niveau d'archivage
- Connectivité réseau sur site ou Services AWS avec bande passante disponible pour le trafic de sauvegarde et de restauration via une connexion Internet publique ou une interface virtuelle AWS Direct Connect publique (VIF)
- Les ports réseau et points de terminaison suivants ont été ouverts pour garantir une communication correcte avec les référentiels de stockage d'objets :
  - Stockage Amazon S3 — TCP — port 443 : utilisé pour communiquer avec le stockage Amazon S3.
  - Stockage Amazon S3 — points de terminaison cloud — `*.amazonaws.com` pour Régions AWS les AWS GovCloud (US) Regions régions ou `*.amazonaws.com.cn` pour la Chine : utilisé pour communiquer avec le stockage Amazon S3. Pour obtenir la liste complète des points de terminaison de connexion, consultez les points de terminaison Amazon S3 dans la AWS documentation.
  - Stockage Amazon S3 — TCP HTTP — port 80 : utilisé pour vérifier l'état du certificat. N'oubliez pas que les points de terminaison de vérification des certificats, à savoir les serveurs de liste de révocation de certificats (CRL) URLs et de protocole OCSP (Online Certificate Status Protocol), sont susceptibles d'être modifiés. La liste réelle des adresses se trouve dans le certificat lui-même.
  - Stockage Amazon S3 — points de terminaison de vérification des certificats — `*.amazontrust.com` : utilisé pour vérifier l'état du certificat. N'oubliez pas que les points de terminaison de vérification des certificats (serveurs CRL URLs et OCSP) sont susceptibles de changer. La liste réelle des adresses se trouve dans le certificat lui-même.

Limites

- Veeam ne prend pas en charge les politiques de cycle de vie S3 sur les buckets S3 utilisés comme référentiels de stockage d'objets Veeam. Il s'agit notamment des politiques relatives aux transitions de classes de stockage Amazon S3 et des règles d'expiration du cycle de vie S3. Veeam doit être la seule entité à gérer ces objets. L'activation des politiques S3 Lifecycle peut avoir des conséquences inattendues, notamment des pertes de données.

Versions du produit

- Veeam Backup & Replication v9.5 Update 4 ou version ultérieure (sauvegarde uniquement ou niveau de capacité)
- Veeam Backup & Replication v10 ou version ultérieure (niveau de sauvegarde ou de capacité et S3 Object Lock)
- Veeam Backup & Replication v11 ou version ultérieure (niveau de sauvegarde ou de capacité, niveau d'archivage ou d'archivage et S3 Object Lock)
- Veeam Backup & Replication v12 ou version ultérieure (niveau de performance, niveau de sauvegarde ou de capacité, niveau d'archivage ou d'archivage et S3 Object Lock)
- S3 Standard
- S3 standard – Accès peu fréquent
- S3 One Zone-IA
- S3 Glacier Flexible Retrieval (v11 et versions ultérieures uniquement)
- S3 Glacier Deep Archive (v11 et versions ultérieures uniquement)
- S3 Glacier Instant Retrieval (v12 et versions ultérieures uniquement)

Architecture

Pile technologique source

- Installation Veeam Backup & Replication sur site avec connectivité depuis un serveur de sauvegarde Veeam ou un serveur de passerelle Veeam vers Amazon S3

Pile technologique cible

- Amazon S3
- Amazon VPC et Amazon EC2 (si vous utilisez le niveau d'archivage)

Architecture cible : SOBR

Le schéma suivant montre l'architecture du référentiel de sauvegarde évolutif (SOBR).

Le logiciel Veeam Backup and Replication protège les données contre les erreurs logiques telles que les défaillances du système, les erreurs d'application ou les suppressions accidentelles. Dans ce schéma, les sauvegardes sont d'abord exécutées sur site, puis une copie secondaire est envoyée directement à Amazon S3. Une sauvegarde représente une point-in-time copie des données.

Le flux de travail comprend trois composants principaux requis pour hiérarchiser ou copier des sauvegardes vers Amazon S3, ainsi qu'un composant facultatif :

- Veeam Backup & Replication (1) : serveur de sauvegarde chargé de coordonner, de contrôler et de gérer l'infrastructure de sauvegarde, les paramètres, les tâches, les tâches de restauration et les autres processus.
- Serveur de passerelle Veeam (non illustré dans le schéma) : serveur de passerelle sur site en option requis si le serveur de sauvegarde Veeam ne dispose pas de connectivité sortante vers Amazon S3.
- Référentiel de sauvegarde évolutif (2) : système de référentiel avec support de mise à l'échelle horizontale pour le stockage de données à plusieurs niveaux. Le référentiel de sauvegarde évolutif comprend un ou plusieurs référentiels de sauvegarde qui fournissent un accès rapide aux données et peuvent être étendus avec des référentiels de stockage d'objets Amazon S3 pour le stockage à long terme (niveau de capacité) et l'archivage (niveau d'archivage). Veeam utilise le référentiel de sauvegarde évolutif pour hiérarchiser automatiquement les données entre le stockage local (niveau de performance) et le stockage d'objets Amazon S3 (niveaux de capacité et d'archivage).

> **Note**
>
> À partir de Veeam Backup & Replication v12.2, la fonctionnalité Direct to S3 Glacier rend le niveau de capacité S3 optionnel. Un SOBR peut être configuré avec un niveau de performance et un niveau d'archivage S3 Glacier. Cette configuration est utile pour les utilisateurs qui ont des investissements importants dans le stockage local (sur site) pour le niveau de capacité et qui ont uniquement besoin de conserver leurs archives à long terme dans le cloud. Pour plus d'informations, consultez la documentation de Veeam Backup & Replication.

- Amazon S3 (3) : service de stockage d' AWS objets offrant évolutivité, disponibilité des données, sécurité et performances.

Architecture cible : DTO

Le schéma suivant montre l'architecture direct-to-object (DTO).

Dans ce schéma, les données de sauvegarde sont directement transférées vers Amazon S3 sans être stockées sur site au préalable. Les copies secondaires peuvent être stockées dans S3 Glacier.

Automatisation et mise à l'échelle

Vous pouvez automatiser la création de ressources IAM et de compartiments S3 en utilisant les AWS CloudFormation modèles fournis dans le VeeamHub GitHub référentiel. Les modèles incluent à la fois des options standard et immuables.

Outils

Outils et Services AWS

- Veeam Backup & Replication est une solution de Veeam pour protéger, sauvegarder, répliquer et restaurer vos charges de travail virtuelles et physiques.
- AWS CloudFormationvous aide à modéliser et à configurer vos AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs Comptes AWS et Régions AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que vous le souhaitez, et vous pouvez les étendre ou les intégrer.
- AWS Identity and Access Management (IAM) est un service Web permettant de contrôler en toute sécurité l'accès à Services AWS. Avec IAM, vous pouvez gérer de manière centralisée les utilisateurs, les informations d'identification de sécurité telles que les clés d'accès et les autorisations qui contrôlent les AWS ressources auxquelles les utilisateurs et les applications peuvent accéder.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- Amazon S3 Glacier (S3 Glacier) est un service sécurisé et durable pour l'archivage des données à faible coût et la sauvegarde à long terme.
- Amazon Virtual Private Cloud (Amazon VPC) fournit une section isolée de manière logique dans AWS Cloud laquelle vous pouvez lancer des AWS ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Code

Utilisez les CloudFormation modèles fournis dans le VeeamHub GitHub référentiel pour créer automatiquement les ressources IAM et les compartiments S3 pour ce modèle. Si vous préférez créer ces ressources manuellement, suivez les étapes de la section Epics.

Bonnes pratiques

- Conformément aux meilleures pratiques IAM, nous vous recommandons vivement de changer régulièrement les informations d'identification utilisateur IAM à long terme, telles que l'utilisateur IAM que vous utilisez pour écrire des sauvegardes Veeam Backup & Replication sur Amazon S3. Pour plus d'informations, veuillez consulter Bonnes pratiques de sécurité dans la documentation IAM.

Épopées

Configurer le stockage Amazon S3 dans votre compte

Tâche	Description	Compétences requises
Créez un utilisateur IAM.	Suivez les instructions de la documentation IAM pour créer un utilisateur IAM. Cet utilisateur ne doit pas avoir accès à la AWS console et vous devrez créer une clé d'accès pour	Administrateur AWS

Tâche	Description	Compétences requises
	cet utilisateur. Veeam utilise cette entité pour s'authentifier afin de lire et AWS d'écrire dans vos compartiments S3. Vous devez accorder le moindre privilège (c'est-à-dire accorder uniquement les autorisations nécessaires à l'exécution d'une tâche) afin que l'utilisateur n'ait pas plus d'autorité qu'il n'en a besoin. Pour des exemples de politiques IAM à associer à votre utilisateur Veeam IAM, consultez la section Informations supplémentaires. **Note** Vous pouvez également utiliser les CloudFormation modèles fournis dans le VeeamHub GitHub référentiel pour créer un utilisateur IAM et un compartiment S3 pour ce modèle.	

Tâche	Description	Compétences requises
Créez un compartiment S3.	1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la. 2. Si vous n'avez pas encore de compartiment S3 existant à utiliser comme espace de stockage cible, choisissez Create bucket, puis spécifiez un nom de bucket et des paramètres de bucket. Région AWS • Nous vous recommandons d'activer l'option Bloquer l'accès public pour le compartiment S3 et de configurer les politiques d'accès et d'autorisation des utilisateurs afin de répondre aux exigences de votre organisation. Pour un exemple, consultez la documentation Amazon S3. • Nous vous recommandons d'activer S3 Object Lock, même si vous n'avez pas l'intention de l'utiliser immédiatement. Ce paramètre ne peut être activé qu'au moment de la création du compartiment S3.	Administrateur AWS

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Création d'un compartiment dans la documentation Amazon S3.	

Ajoutez Amazon S3 et S3 Glacier Flexible Retrieval (ou S3 Glacier Deep Archive) à Veeam Backup & Replication

Tâche	Description	Compétences requises
Lancez l'assistant de dépôt de nouveaux objets.	Avant de configurer le stockage d'objets et les référentiels de sauvegarde évolutifs dans Veeam, vous devez ajouter les référentiels de stockage Amazon S3 et S3 Glacier que vous souhaitez utiliser pour les niveaux de capacité et d'archivage. Dans le prochain épisode, vous allez connecter ces référentiels de stockage à votre référentiel de sauvegarde évolutif. 1. Sur la console Veeam, ouvrez la vue Backup Infrastructure. 2. Dans le volet d'inventaire, choisissez le nœud Backup Repositories, puis choisissez Add Repository. 3. Dans la boîte de dialogue Add Backup Repositor	Administrateur AWS, propriétaire de l'application

Tâche	Description	Compétences requises
	y, sélectionnez Object Storage, Amazon S3.	

Tâche	Description	Compétences requises
Ajoutez le stockage Amazon S3 pour le niveau de capacité.	1. Dans la boîte de dialogue Amazon Cloud Storage Services, sélectionnez Amazon S3. 2. À l'étape Nom de l'assistant, spécifiez le nom du stockage d'objets et une brève description, telle que le créateur et la date de création. 3. À l'étape Compte de l'assistant, spécifiez le compte de stockage d'objets. • Pour les informations d'identification, choisissez l'utilisateur IAM que vous avez créé dans le premier épisode pour accéder à votre espace de stockage d'objets Amazon S3. • Pour la région AWS, choisissez l' Région AWS emplacement du compartiment S3. 4. À l'étape Bucket de l'assistant, spécifiez les paramètres de stockage d'objets. • Pour la région du centre de données, choisissez l' Région AWS emplacement du compartiment S3.	Administrateur AWS, propriétaire de l'application

Tâche	Description	Compétences requises
	• Pour Bucket, choisissez le compartiment S3 que vous avez créé dans le premier épisode épique. • Pour Dossier, créez ou sélectionnez un dossier cloud auquel mapper votre référentiel de stockage d'objets. • Si vous souhaitez activer l'immuabilité, choisisse z Rendre les sauvegard es récentes immuables pendant X jours et définissez la période pendant laquelle vos sauvegardes doivent être verrouillées. Notez que l'activation de l'immuabilité entraîne une augmentation des coûts en raison de l'augment ation du nombre d'appels d'API vers Amazon S3 depuis Veeam. 5. À l'étape Résumé de l'assistant, passez en revue les informations de configuration, puis choisisse z Terminer.	

Tâche	Description	Compétences requises
Ajoutez le stockage S3 Glacier au niveau d'archivage.	Si vous souhaitez créer un niveau d'archivage, utilisez les autorisations IAM détaillées dans la section Informations supplémentaires. 1. Lancez l'assistant de dépôt de nouveaux objets comme décrit précédemment. 2. Dans la boîte de dialogue Amazon Cloud Storage Services, sélectionnez Amazon S3 Glacier. 3. À l'étape Nom de l'assistant, spécifiez le nom du stockage d'objets et une brève description, telle que le créateur et la date de création. 4. À l'étape Compte de l'assistant, spécifiez le compte de stockage d'objets. • Pour les informations d'identification, choisissez l'utilisateur IAM que vous avez créé dans le premier épisode pour accéder à votre stockage d'objets S3 Glacier. • Pour la région AWS, choisissez l' Région AWS emplacement du compartiment S3.	Administrateur AWS, propriétaire de l'application

Tâche	Description	Compétences requises
	5. À l'étape Bucket de l'assistant, spécifiez les paramètres de stockage d'objets. • Pour la région du centre de données, choisissez le Région AWS. • Pour Bucket, choisissez un compartiment S3 pour stocker vos données de sauvegarde. Il peut s'agir du même compartiment que celui que vous avez utilisé pour le niveau de capacité. • Pour Dossier, créez ou sélectionnez un dossier cloud auquel mapper votre référentiel de stockage d'objets. • Si vous souhaitez activer l'immuabilité, choisissez Rendre les sauvegardes récentes immuables pendant toute la durée de leur politique de conservation. Notez que l'activation de l'immuabilité entraîne une augmentation des coûts en raison de l'augmentation du nombre d'appels d'API vers Amazon S3 depuis Veeam.	

Tâche	Description	Compétences requises
	• Si vous souhaitez utiliser S3 Glacier Deep Archive comme classe de stockage d'archiva ge, choisissez Utiliser la classe de stockage Deep Archive. 6. À l'étape Proxy Appliance de l'assistant, configurez l'instance auxiliaire utilisée pour transférer les données d'Amazon S3 vers S3 Glacier. Vous pouvez utiliser les paramètres par défaut ou configurer chaque paramètre manuellem ent. Pour configurer les paramètres manuellement, procédez comme suit : • Choisissez Personnaliser. • EC2 Par type d'instanc e, choisissez le type d'instance pour l'applian ce proxy, en fonction de vos exigences en termes de vitesse et de coût pour le transfert des fichiers de sauvegarde vers le niveau d'archiva ge de votre référentiel de sauvegarde évolutif. • Pour Amazon VPC, choisissez le VPC pour l'instance cible.	

Tâche	Description	Compétences requises
	• Pour Sous-réseau, choisissez le sous-réseau pour l'appliance proxy. • Pour Groupe de sécurité, choisissez le groupe de sécurité à associer à l'appliance proxy. • Pour le port du redirecteur, spécifiez le port TCP pour le routage des demandes entre l'appliance proxy et les composants de l'infrastructure de sauvegarde. • Cliquez sur OK pour confirmer vos paramètres. 7. À l'étape Résumé de l'assistant, passez en revue les informations de configuration, puis choisissez Terminer.	

Ajoutez des référentiels de sauvegarde évolutifs

Tâche	Description	Compétences requises
Lancez l'assistant New Scale-Out Backup Repository.	1. Sur la console Veeam, ouvrez la vue Backup Infrastructure. 2. Dans le volet d'inventaire, choisissez Scale-out	Propriétaire de l'application, administrateur des systèmes AWS

Tâche	Description	Compétences requises
	Repositories, puis choisissez Add Scale-out Repository.	

Tâche	Description	Compétences requises
Ajoutez un référentiel de sauvegarde évolutif et configurez les niveaux de capacité et d'archivage.	1. À l'étape Nom de l'assistant, spécifiez le nom et une brève description du référentiel de sauvegarde évolutif. 2. Si nécessaire, ajoutez des extensions de performances. Vous pouvez également utiliser votre référentiel de sauvegarde local Veeam existant comme niveau de performance. À partir de la version 12 de Veeam, vous pouvez ajouter un bucket S3 comme extension de performance pour les sauvegardes direct-to-object (DTO), en contournant un niveau de performance local. 3. Choisissez Avancé et spécifiez des options supplémentaires pour le référentiel de sauvegarde évolutif. • Choisissez Utiliser des fichiers de sauvegarde par machine pour créer un fichier de sauvegarde distinct pour chaque machine et écrire ces fichiers dans le référentiel de sauvegarde dans	Propriétaire de l'application, administrateur des systèmes AWS

Tâche	Description	Compétences requises
	plusieurs flux simultané ment. Cette option est recommandée pour une meilleure utilisation des ressources de stockage et de calcul. • Choisissez Effectuer une sauvegarde complète lorsque l'étendue requise est hors ligne pour créer un fichier de sauvegard e complet au cas où une étendue contenant des points de restaurat ion pour une sauvegard e incrémentielle serait déconnectée. Cette option nécessite de l'espace libre dans le référentiel de sauvegard e évolutif pour héberger un fichier de sauvegarde complet. 4. À l'étape Stratégie de l'assistant, spécifiez la politique de placement des sauvegardes pour le référentiel. • Choisissez Data locality pour stocker les fichiers de sauvegarde complets et incrémentiels appartenant à la même chaîne, avec le même	

Tâche	Description	Compétences requises
	niveau de performance. Vous pouvez stocker des fichiers appartena nt à une nouvelle chaîne de sauvegarde avec le même niveau de performance ou dans un autre (sauf si vous utilisez un dispositif de stockage dédupliquant comme extension de performan ce). • Choisissez Performan ce pour stocker des fichiers de sauvegarde complets et incrément iels à différents niveaux de performance. Cette option nécessite une connexion réseau rapide et fiable. Si vous choisissez Performan ce, vous pouvez limiter les types de fichiers de sauvegarde à stocker pour chaque niveau de performance. Par exemple, vous pouvez stocker des fichiers de sauvegarde complets sur une extension et des fichiers de sauvegarde incrémentiels sur d'autres extensions. Pour choisir les types de fichiers :	

Tâche	Description	Compétences requises
	• Choisissez Personnaliser. • Dans la boîte de dialogue Paramètres de placement des sauvegardes, choisissez une étendue de performance, puis sélectionnez Modifier. • Choisissez le type de fichiers de sauvegarde que vous souhaitez stocker dans l'étendue. 5. À l'étape Niveau de capacité de l'assistant, configurez le niveau de stockage à long terme que vous souhaitez associer au référentiel de sauvegarde évolutif. • Choisissez Étendre la capacité du référentiel de sauvegarde évolutif grâce au stockage en mode objet. Pour le référentiel de stockage d'objets, choisissez le stockage Amazon S3 pour le niveau de capacité que vous avez ajouté dans l'épopée précédente. • Choisissez Fenêtre pour sélectionner une fenêtre	

Tâche	Description	Compétences requises
	temporelle pour déplacer ou copier des données. • Choisissez Copier les sauvegardes vers le stockage d'objets dès leur création pour copier tous les fichiers de sauvegard e ou uniquement les fichiers de sauvegarde récemment créés dans la limite de leurs capacités. • Choisissez Déplacer les sauvegardes vers le stockage d'objets à mesure qu'elles vieilliss ent en dehors de la fenêtre de restaurat ion opérationnelle pour transférer les chaînes de sauvegarde inactives dans la limite de leur capacité. Dans le champ Déplacer les fichiers de sauvegarde datant de plus de X jours, spécifiez la durée après laquelle les fichiers de sauvegard e doivent être déchargés . (Pour décharger les chaînes de sauvegarde inactives le jour de leur création, spécifiez 0 jour.) Vous pouvez également	

Tâche	Description	Compétences requises
	choisir Override pour déplacer les fichiers de sauvegarde plus rapidement si le référenti el de sauvegarde évolutif a atteint le seuil que vous spécifiez. • Choisissez Chiffrer les données téléchargées vers le stockage d'objets et spécifiez un mot de passe pour chiffrer toutes les données et leurs métadonnées en vue du déchargement. Choisisse z Ajouter ou Gérer les mots de passe pour définir un nouveau mot de passe. 6. À l'étape Niveau d'archiva ge de l'assistant, configure z le niveau de stockage d'archives que vous souhaitez associer au référentiel de sauvegard e évolutif. (Cette étape n'apparaît pas si vous avez ignoré l'ajout du stockage Amazon S3 Glacier.) • Choisissez Archiver les sauvegardes complètes GFS vers le stockage d'objets. Pour le référenti el de stockage d'objets,	

Tâche	Description	Compétences requises
	choisissez le stockage Amazon S3 Glacier que vous avez ajouté dans l'épopée précédente. • Pour les sauvegardes Archive GFS datant de plus de N jours, choisissez une fenêtre temporelle pour déplacer les fichiers vers l'étendue de l'archive. (Pour archiver les chaînes de sauvegarde inactives le jour de leur création, spécifiez 0 jour.) 7. À l'étape Résumé de l'assistant, passez en revue la configuration du référentiel de sauvegarde évolutif, puis choisissez Terminer.	

Ressources connexes

- Création d'un utilisateur IAM dans votre Compte AWS (documentation IAM)
- Création d'un compartiment (documentation Amazon S3)
- Blocage de l'accès public à votre espace de stockage Amazon S3 (documentation Amazon S3)
- Utilisation du verrouillage d'objets S3 (documentation Amazon S3)
- Documentation technique de Veeam
- Comment créer une politique IAM sécurisée pour la connexion au stockage d'objets S3 (documentation Veeam)

Informations supplémentaires

Les sections suivantes fournissent des exemples de politiques IAM que vous pouvez utiliser lorsque vous créez un utilisateur IAM dans la section Epics de ce modèle.

Politique IAM pour le niveau de capacité

> **Note**
>
> Dans l'exemple de politique, remplacez le nom des compartiments S3 par le nom du `<yourbucketname>` compartiment S3 que vous souhaitez utiliser pour les sauvegardes au niveau de capacité de Veeam. Notez également que la politique doit être limitée aux ressources spécifiques utilisées par Veeam (indiquées dans les `Resource` spécifications de la politique suivante), et que la première partie de la politique désactive le chiffrement côté client, comme indiqué dans le billet de AWS blog Empêcher le chiffrement involontaire des objets Amazon S3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<your-bucket-name>/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        },
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObjectVersion",
                "s3:ListBucketVersions",
                "s3:ListBucket",
                "s3:PutObjectLegalHold",
                "s3:GetBucketVersioning",
```

```
                "s3:GetObjectLegalHold",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObject*",
                "s3:GetObject*",
                "s3:GetEncryptionConfiguration",
                "s3:PutObjectRetention",
                "s3:PutBucketObjectLockConfiguration",
                "s3:DeleteObject*",
                "s3:DeleteObjectVersion",
                "s3:GetBucketLocation"

            ],
            "Resource": [
                "arn:aws:s3:::<yourbucketname>",
                "arn:aws:s3:::<yourbucketname>/*"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Politique IAM pour le niveau d'archivage

> **Note**
>
> Dans l'exemple de politique, remplacez le nom des compartiments S3 par le nom du <yourbucketname> compartiment S3 que vous souhaitez utiliser pour les sauvegardes au niveau de l'archive Veeam.

Pour utiliser votre VPC, votre sous-réseau et vos groupes de sécurité existants :

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
```

```
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs"
            ],
            "Resource": "arn:aws:ec2:<region>:<account-id>:*"
        }
    ]
}
```

Pour créer de nouveaux VPC, sous-réseaux et groupes de sécurité, procédez comme suit :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:RestoreObject",
                "s3:ListBucket",
                "s3:AbortMultipartUpload",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:GetBucketLocation",
                "s3:GetBucketObjectLockConfiguration",
                "s3:PutObjectRetention",
                "s3:GetObjectVersion",
                "s3:PutObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:DeleteObjectVersion",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws:s3:::<bucket-name>",
                "arn:aws:s3:::<bucket-name>/*"
            ]
        }
    ]
```

```
}

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2Permissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:CreateKeyPair",
                "ec2:DescribeKeyPairs",
                "ec2:RunInstances",
                "ec2:DeleteKeyPair",
                "ec2:DescribeVpcAttribute",
                "ec2:CreateTags",
                "ec2:DescribeSubnets",
                "ec2:TerminateInstances",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeVpcs",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateRoute",
                "ec2:CreateInternetGateway",
                "ec2:AttachInternetGateway",
                "ec2:ModifyVpcAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstanceTypes"
            ],
            "Resource": "*"
        }
    ]
}
```

Configuration de Veritas NetBackup pour le VMware cloud sur AWS

Créée par Shubham Salani (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on AWS n'est plus revendu ni par AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre représentant AWS pour plus de détails.

De nombreuses entreprises utilisent Veritas NetBackup comme solution de sauvegarde et de restauration pour leurs charges de travail sur site basées sur VMware vSphere. Une fois que les entreprises ont migré leurs charges de travail vers des centres de données définis par logiciel (SDDCs) dans le VMware cloud sur l'infrastructure Amazon Web Services (AWS), il n'existe aucune lift-and-shift procédure d'intégration claire. NetBackup Ce modèle décrit comment configurer Veritas NetBackup dans votre compte AWS et le configurer pour sauvegarder les charges de travail de votre compte. VMware SDDCs

Ce modèle ne contient pas d'instructions pour la migration de vos charges de travail. Pour plus d'informations, consultez Migrer le VMware SDDC vers le VMware cloud sur AWS à l'aide VMware de HCX. Lorsque vous configurez vos charges de travail VMware dans le cloud sur AWS, utilisez un cluster étendu (VMware documentation). Dans cette configuration, votre cluster couvre deux zones de disponibilité AWS au sein d'une même région. Cela garantit une disponibilité et une résilience élevées dans le cas où l'une des zones de disponibilité deviendrait indisponible. Elastic DRS et un hôte témoin vSAN (VMware documentation) copient facilement les données vers une troisième zone de disponibilité, connue sous le nom de domaine de défaillance. Cette solution de parité peut vous aider à récupérer les données en cas de panne. Comme cette approche nécessite trois zones de disponibilité, lorsque vous sélectionnez une région AWS pour votre environnement VMware cloud, assurez-vous qu'elle comporte au moins trois zones de disponibilité. Pour plus d'informations, consultez Régions et zones de disponibilité.

Dans ce modèle, chaque SDDC possède un hôte de sauvegarde, qui est un serveur proxy. À l'aide des instances Amazon Elastic Compute Cloud (Amazon EC2), vous configurez le serveur NetBackup principal et le serveur multimédia dans un cloud privé virtuel (VPC) distinct, un pour chaque SDDC. Les interfaces réseau élastiques fournissant une bande passante élevée et une faible latence, vous les utilisez pour configurer la connectivité entre les hôtes de sauvegarde et leurs NetBackup serveurs principaux et multimédias correspondants. Les EC2 instances dirigent les sauvegardes

vers les volumes Amazon Elastic Block Store (Amazon EBS), qui constituent le premier point de sauvegarde. Vous pouvez utiliser AWS DataSync pour conserver vos volumes EBS à des fins de SDDCs synchronisation.

Vous pouvez également utiliser AWS Transit Gateway et un point de terminaison VPC d'interface pour connecter les volumes EBS à un autre service de stockage, tel qu'Amazon Simple Storage Service (Amazon S3). Conformément à votre politique de rétention, vous pouvez utiliser les classes de stockage S3 Glacier de S3 Intelligent-Tiering pour optimiser vos coûts de stockage. Pour plus d'informations, consultez Utilisation des classes de stockage Amazon S3 (documentation Amazon S3).

Conditions préalables et limitations

Prérequis

- Votre environnement VMware Cloud on AWS utilise un cluster étendu qui couvre deux zones de disponibilité.
- L'hôte de sauvegarde doit résider sur le SDDC VMware Cloud on AWS qui a accès à la banque de données où les fichiers VMDK (VMware Virtual Machine Disk File) sont déployés.
- HotAdd le mode transport doit être activé sur le NetBackup client pour sauvegarder et restaurer les machines virtuelles (VMs), et il doit autoriser les restaurations à partir de fichiers et de dossiers dirigés par l'utilisateur.

Limites

- Le serveur NetBackup principal doit utiliser la résolution DNS pour une adresse IP privée pour l'hôte de sauvegarde vCenter dans le SDDC.
- Les fichiers hôtes du serveur NetBackup principal et de l'hôte de sauvegarde doivent contenir les éléments suivants :
  - L'adresse IP privée et le nom DNS privé du serveur principal
  - Adresse IP privée et nom DNS privé de l'hôte de sauvegarde
- Si vous configurez des points de terminaison VPC d'interface sur un compartiment S3, le pare-feu SDDC Compute Gateway doit être configuré pour autoriser le protocole HTTPS à partir d'une source de bloc CIDR (Classless Inter-Domain Routing). Pour plus d'informations, consultez Accéder à un compartiment S3 à l'aide d'un point de terminaison S3 (VMware documentation).
- VMware Cloud on AWS ne prend pas en charge les fonctionnalités suivantes NetBackup :

- Sauvegarde ou restauration de modèles de machines virtuelles
- Utilisation de NetBackup vSphere Client (plug-in) HTML5
- Verrouillage et déverrouillage VMs pour les sauvegardes ou les restaurations
- Les sauvegardes ne peuvent pas être stockées dans une banque de données vSAN
- Modes de transport NBD (Network Block Device), NBDSSL et SAN

Versions du produit

- VMware Cloud sur AWS SDDC version 1.0 ou ultérieure
- Veritas NetBackup version 8.1.2 ou ultérieure
- Linux version 6.8 ou ultérieure
- VMware vSphere version 6.0 ou ultérieure

Architecture

Le schéma suivant montre la configuration de NetBackup for VMware Cloud on AWS. Les serveurs NetBackup principal et multimédia sont déployés dans un VPC distinct et sont connectés aux hôtes de sauvegarde dans les SDDCs interfaces réseau Elastic. Le serveur NetBackup principal et le serveur multimédia stockent les sauvegardes dans des volumes Amazon EBS. Vous pouvez éventuellement configurer du stockage supplémentaire dans des compartiments Amazon S3 à l'aide d'AWS Transit Gateway et d'un point de terminaison VPC d' PrivateLink interface AWS.

Outils

Services et outils AWS

- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2
- AWS vous PrivateLink aide à créer des connexions privées unidirectionnelles entre vos clouds privés virtuels (VPCs) et des services extérieurs au VPC.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que

vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Autres services

- VMware Cloud on AWS est une offre cloud intégrée développée conjointement par Amazon Web Services (AWS) et VMware.
- NetBackup pour VMware sauvegarder et restaurer les machines VMware virtuelles qui s'exécutent sur VMware ESXi des hôtes.

Épopées

Configuration des NetBackup serveurs

Tâche	Description	Compétences requises
Mettez à jour les règles du pare-feu.	Mettez à jour les règles de pare-feu pour établir la connectivité entre le SDDC VMware Cloud on AWS et le serveur NetBackup principal et le serveur multimédia. Procédez comme suit : 1. Connectez-vous au VMware cloud sur AWS à l'adresse https://vmc.vmware.com/ 2. Dans l'onglet Mise en réseau et sécurité, choisissez Gateway Firewall. 3. Sur la page Gateway Firewall, choisissez Compute Gateway.	Administrateur réseau, administrateur du cloud

Tâche	Description	Compétences requises
	4. Choisissez AJOUTER une règle, puis créez une nouvelle règle avec les paramètres de port de pare-feu nécessaires. Pour plus d'informations, consultez les exigences relatives aux ports du NetBackup pare-feu (documentation Veritas).	

Tâche	Description	Compétences requises
Lancez le serveur NetBackup principal et le serveur multimédia.	1. Connectez-vous à l'AWS Management Console et ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/ 2. Lancez une EC2 instance (EC2 documentation Amazon) et utilisez les informations de configuration suivantes : a. Pour le serveur NetBackup principal et le serveur multimédia, sélectionnez l'`NBU-Linux-GA-8-1-2-Setup-f032d23e-881b-4dee-ba70-b9ca3e915910-ami-072509a7ffc156938.4` Amazon Machine Image (AMI). Cette AMI préconfigurée est disponible via AWS Marketplace. b. Sélectionnez un type d'instance. NetBackup recommande `m5.2xlarge` pour le serveur principal et le serveur multimédia.	Administrateur cloud, administrateur de sauvegarde

Tâche	Description	Compétences requises
Configurez l'hôte de sauvegarde pour NetBackup.	1. Connectez-vous au VMware cloud sur AWS à l'adresse https://vmc.vmware.com/ 2. Sélectionnez le SDDC. 3. Choisissez l'onglet Open VCENTER. Cela ouvre le SDDC vCenter. 4. Notez le nom de domaine complet (FQDN) de l'hôte de sauvegarde. 5. Connectez-vous à la console NetBackup d'administration. Pour plus d'informations, consultez la section Connexion à la console d' NetBackup administration (documentation Veritas). 6. Sélectionnez le serveur principal et le serveur multimédia, puis choisissez VMware Access Hosts. 7. Ajoutez le nom de domaine complet de l'hôte de sauvegarde. 8. Choisissez Appliquer, puis OK.	Administrateur cloud, administrateur de sauvegarde

(Facultatif) Configurer le stockage Amazon S3

Tâche	Description	Compétences requises
Configurez le stockage dans Amazon S3.	1. Passez en revue les options de stockage dans le cloud d'Amazon S3 (documentation Veritas) et sélectionnez la classe de stockage adaptée à vos besoins. 2. Configurez NetBackup pour utiliser Amazon S3 pour le stockage dans le cloud conformément aux instructions de la section Configuration du stockage dans le cloud dans NetBackup (documentation Veritas).	Administrateur du cloud, AWS général

Ressources connexes

Documentation AWS

- Création d'un point de terminaison VPC d'interface (documentation AWS PrivateLink)

Documentation Veritas

- NetBackup exigences relatives aux ports de pare-feu

VMware documentation

- Déployer une machine virtuelle à partir d'un modèle OVF dans une bibliothèque de contenu
- VMware Frais de transfert de données dans le cloud sur AWS : comment ça marche ? (VMware billet de blogue)
- VMware Cloud sur AWS : clusters étendus

Copiez les données d'un compartiment S3 vers un autre compte ou une autre région à l'aide de l'AWS CLI

Créée par Appasaheb Bagali (AWS) et Purushotham G K (AWS)

Récapitulatif

Ce modèle décrit comment migrer les données d'un compartiment Amazon Simple Storage Service (Amazon S3) d'un compte source AWS vers un compartiment S3 de destination d'un autre compte AWS, dans la même région AWS ou dans une autre région.

Le compartiment S3 source autorise l'accès à AWS Identity and Access Management (IAM) à l'aide d'une politique de ressources attachée. Un utilisateur du compte de destination doit assumer un rôle doté `PutObject` d'`GetObject`autorisations pour le compartiment source. Enfin, vous exécutez `copy` des `sync` commandes pour transférer les données du compartiment S3 source vers le compartiment S3 de destination.

Les comptes sont propriétaires des objets qu'ils téléchargent dans des compartiments S3. Si vous copiez des objets entre comptes et régions, vous accordez au compte de destination la propriété des objets copiés. Vous pouvez modifier le propriétaire d'un objet en remplaçant sa liste de contrôle d'accès (ACL) par`bucket-owner-full-control`. Toutefois, nous vous recommandons d'accorder des autorisations programmatiques entre comptes au compte de destination, car cela ACLs peut être difficile à gérer pour plusieurs objets.

> **Warning**
>
> Ce scénario nécessite que les utilisateurs IAM disposent d'un accès programmatique et d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisat ions lorsqu'elles ne sont plus nécessaires. Les clés d'accès peuvent être mises à jour si nécessaire. Pour plus d'informations, consultez la section Mise à jour des clés d'accès dans le guide de l'utilisateur IAM.

Ce modèle couvre une migration unique. Pour les scénarios qui nécessitent une migration continue et automatique de nouveaux objets d'un compartiment source vers un compartiment de destination,

vous pouvez plutôt utiliser S3 Batch Replication, comme décrit dans le modèle Copier les données d'un compartiment S3 vers un autre compte et une autre région à l'aide de S3 Batch Replication.

Conditions préalables et limitations

- Deux comptes AWS actifs dans la même région AWS ou dans des régions différentes.
- Un compartiment S3 existant dans le compte source.
- Si le chiffrement par défaut de votre compartiment Amazon S3 source ou de destination est activé, vous devez modifier les autorisations clés d'AWS Key Management Service (AWS KMS). Pour plus d'informations, consultez l'article AWS re:Post à ce sujet.
- Connaissance des autorisations entre comptes.

Architecture

Outils

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

Bonnes pratiques

- Bonnes pratiques de sécurité dans l'IAM (documentation IAM)
- Appliquer les autorisations du moindre privilège (documentation IAM)

Épopées

Création d'un utilisateur et d'un rôle IAM dans le compte AWS de destination

Tâche	Description	Compétences requises
Créez un utilisateur IAM et obtenez la clé d'accès.	1. Connectez-vous à l'AWS Management Console et créez un utilisateur IAM disposant d'un accès programmatique. Pour connaître les étapes détaillées, consultez la section Création d'utilisateurs IAM dans la documentation IAM. Il n'est pas nécessaire de joindre des politiques pour cet utilisateur. 2. Générez une clé d'accès et une clé secrète pour cet utilisateur. Pour obtenir des instructions, consultez la section Compte AWS et clés d'accès dans la documentation AWS.	AWS DevOps
Créez une politique basée sur l'identité IAM.	Créez une politique basée sur l'identité IAM nommée à l'aide `S3MigrationPolicy` des autorisations suivantes . Pour connaître les étapes détaillées, consultez la section Création de politiques IAM dans la documentation IAM. `{`	AWS DevOps

Tâche	Description	Compétences requises
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetObject", "s3:GetObjectTagging", "s3:GetObjectVersion", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::amazon-s3-demo-source-bucket", "arn:aws:s3:::amazon-s3-demo-source-bucket/*"] }, { "Effect": "Allow", "Action": ["s3:ListBucket", "s3:PutObject",	

Tâche	Description	Compétences requises

	<pre>"s3:PutObjectAcl",
	
	"s3:PutObjectTaggi
	ng",
	
	"s3:GetObjectTaggi
	ng",
	
	"s3:GetObjectVersi
	on",
	
	"s3:GetObjectVersi
	onTagging"
	],
	"Resource":
	[
	
	"arn:aws:s3:::amazon-
	s3-demo-destination-
	bucket",
	
	"arn:aws:s3:::amazon-
	s3-demo-destination-
	bucket/*"
	]
	}
	]
	}</pre>
	Note
	Modifiez les noms des compartiments source et de destination en fonction de votre cas d'utilisation.	

Tâche	Description	Compétences requises
	Cette politique basée sur l'identité permet à l'utilisateur qui assume ce rôle d'accéder au compartiment source et au compartiment de destination.	

Tâche	Description	Compétences requises
Créez un rôle IAM.	Créez un rôle IAM nommé `S3MigrationRole` en utilisant la politique de confiance suivante, puis attachez le rôle créé `S3MigrationPolicy` précédemment. Pour connaître les étapes détaillées, consultez la section Création d'un rôle pour déléguer des autorisations à un utilisateur IAM dans la documentation IAM. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<destination_account>:user/<user_name>" }, "Action": "sts:AssumeRole", "Condition": {} } ] }`	AWS DevOps

Tâche	Description	Compétences requises
	Note Modifiez le nom de ressource Amazon (ARN) du rôle IAM ou du nom d'utilisateur de destination dans la politique de confiance en fonction de votre cas d'utilisation. Cette politique de confiance permet à l'utilisateur IAM nouvellement créé d'assumer `S3MigrationRole` .	

Créez et associez la politique de compartiment S3 au compte source

Tâche	Description	Compétences requises
Créez et attachez une politique de compartiment S3.	Connectez-vous à l'AWS Management Console pour votre compte source et ouvrez la console Amazon S3. Choisissez votre compartiment S3 source, puis choisissez Permissions. Sous Politique de compartiment, choisissez Modifier, puis collez la politique de compartiment suivante. Choisissez Save (Enregistrer).	Administrateur du cloud

Tâche	Description	Compétences requises

	{
	"Version":
	"2012-10-17",
	"Statement": [
	{
	"Sid":
	"DelegateS3Access",
	"Effect":
	"Allow",
	"Principa
	l": {"AWS": "arn:aws:
	iam::<destination_
	account>:role/<Rol
	eName>"},
	"Action":
	["s3:ListBucket",
	
	"s3:GetObject",
	
	"s3:GetObjectTaggi
	ng",
	
	"s3:GetObjectVersi
	on",
	
	"s3:GetObjectVersi
	onTagging"
	
	],
	"Resource":
	[
	
	"arn:aws:s3:::amazon-
	s3-demo-source-bucket/
	*",
	
	"arn:aws:s3:::amazon-
	s3-demo-source-bucket"
	]
	}
	]	

Tâche	Description	Compétences requises
	} **Note** Assurez-vous d'inclure l'ID de compte AWS pour le compte de destination et de configurer le modèle de politique de compartiment en fonction de vos besoins. Cette politique basée sur les ressources permet au rôle de destination `S3MigrationRole` d'accéder aux objets S3 du compte source.	

Configuration du compartiment S3 de destination

Tâche	Description	Compétences requises
Créez un compartiment S3 de destination.	Connectez-vous à l'AWS Management Console pour votre compte de destination, ouvrez la console Amazon S3, puis choisissez Create bucket. Créez un compartiment S3 selon vos besoins. Pour plus d'informations, consultez la section Création	Administrateur du cloud

Tâche	Description	Compétences requises
	d'un compartiment dans la documentation Amazon S3.	

Copier les données dans le compartiment S3 de destination

Tâche	Description	Compétences requises
Configurez l'AWS CLI avec les informations d'identif ication utilisateur nouvellement créées.	1. Installez la dernière version de l'AWS CLI. Pour obtenir des instructions, consultez la section Installation ou mise à jour de la dernière version de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS. 2. Exécutez `$ aws configure` et mettez à jour la CLI avec la clé d'accès AWS de l'utilisa teur que vous avez créé. Pour plus d'informations, consultez la section Configuration et paramètre s des fichiers d'identification dans la documentation de l'AWS CLI.	AWS DevOps
Assumez le rôle de migration S3.	1. Utilisez la CLI AWS pour supposer que `S3Migrati onRole` : `aws sts assume-role \`	Administrateur AWS

Tâche	Description	Compétences requises
	`--role-arn "arn:aws:iam::<destination_account>:role/S3MigrationRole" \ --role-session-name AWSCLI-Session` Cette commande génère plusieurs informations. Dans le bloc d'informations d'identification, vous avez besoin du `AccessKeyId` `SecretAccessKey` , et`SessionToken` . Cet exemple utilise les variables d'environnement `RoleAccessKeyID` `RoleSecretKey` , et`RoleSessionToken` . Notez que l'horodatage du champ d'expiration est indiqué dans le fuseau horaire UTC. L'horodatage indique la date d'expiration des informations d'identification temporaires du rôle IAM. Si les informations d'identification temporaires expirent, vous devez appeler à nouveau l'`sts:AssumeRole` API. 2. Créez trois variables d'environnement pour assumer le rôle IAM. Ces	

Tâche	Description	Compétences requises

	variables d'environnement sont renseignées avec le résultat suivant :
	
	`# Linux`
	`export AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`export AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`export AWS_SESSI ON_TOKEN=RoleSessi onToken`
	`# Windows`
	`set AWS_ACCES S_KEY_ID=RoleAcces sKeyID`
	`set AWS_SECRE T_ACCESS_KEY=RoleS ecretKey`
	`set AWS_SESSI ON_TOKEN=RoleSessi onToken`
	
	3. Vérifiez que vous avez assumé le rôle IAM en exécutant la commande suivante :
	
	`aws sts get-caller-identity`
	
	Pour plus d'informations, consultez le centre de connaissances AWS.	

Tâche	Description	Compétences requises

Copiez et synchronisez les données du compartiment S3 source vers le compartiment S3 de destination.	Lorsque vous avez assumé le rôle, `S3MigrationRole` vous pouvez copier les données à l'aide de la commande copy (cp) ou de synchronisation (sync).
	
	Copiez (consultez le manuel de référence des commandes de l'AWS CLI pour plus de détails) :
	
	`aws s3 cp s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --recursive --source-region SOURCE-REGION-NAME --region DESTINATION-REGION-NAME`
	
	Synchronisez (consultez le manuel de référence des commandes de l'AWS CLI pour plus de détails) :
	
	`aws s3 sync s3://amazon-s3-demo-source-bucket/ \ s3://amazon-s3-demo-destination-bucket/ \ --source-region SOURCE-REGION-NAME`
		Administrateur du cloud

Tâche	Description	Compétences requises
	`--region DESTINATION-REGION-NAME`	

Résolution des problèmes

Problème	Solution
Une erreur s'est produite (`AccessDenied`) lors de l'appel de l'`ListObjects` opération : Accès refusé	• Assurez-vous d'avoir assumé le rôle`S3MigrationRole`. • Exécutez `aws sts get-caller-identity` pour vérifier le rôle utilisé. Si la sortie n'affiche pas l'ARN pour`S3MigrationRole`, reprenez le rôle et réessayez.

Ressources connexes

- Création d'un compartiment S3 (documentation Amazon S3)
- Politiques relatives aux compartiments Amazon S3 et politiques utilisateur (documentation Amazon S3)
- Identités IAM (utilisateurs, groupes et rôles) (documentation IAM)
- commande cp (documentation de la CLI AWS)
- commande de synchronisation (documentation de la CLI AWS)

Copiez les données d'un compartiment S3 vers un autre compte et une autre région à l'aide de S3 Batch Replication

Créée par Appasaheb Bagali (AWS), Lakshmikanth BD (AWS), Purushotham GK (AWS), Shubham Harsora (AWS) et Suman Rajotia (AWS)

Récapitulatif

Ce modèle explique comment vous pouvez utiliser la réplication par lots Amazon Simple Storage Service (Amazon S3) pour copier automatiquement le contenu d'un compartiment S3 vers un autre compartiment S3, sans aucune intervention manuelle, après avoir configuré les compartiments. Les compartiments source et de destination peuvent se trouver dans le même compartiment ou dans des régions différentes Comptes AWS .

S3 Batch Replication vous permet de répliquer des objets Amazon S3 qui existaient avant la mise en place d'une configuration de réplication, des objets précédemment répliqués et des objets dont la réplication n'a pas échoué. Cette méthode utilise une tâche S3 Batch Operations. Lorsque le travail est terminé, vous recevez un rapport d'achèvement.

Vous pouvez utiliser S3 Batch Replication dans des scénarios qui nécessitent une migration continue et automatique de nouveaux objets d'un compartiment source vers un compartiment de destination. Pour une migration unique, vous pouvez utiliser le AWS Command Line Interface (AWS CLI) à la place, comme décrit dans le modèle Copier les données d'un compartiment S3 vers un autre compte et une autre région à l'aide du AWS CLI.

Conditions préalables et limitations

- Une source Compte AWS.
- Une destination Compte AWS.
- Un compartiment S3 dans le compte source contenant quelques objets (fichiers ou dossiers).
- Un ou plusieurs compartiments S3 dans le compte de destination.
- La gestion des versions S3 est activée sur les compartiments source et de destination.
- AWS Identity and Access Management Autorisations (IAM) permettant de créer une stratégie IAM, un rôle IAM et une politique de compartiment S3 sur les comptes source et de destination.
- Les règles du cycle de vie Amazon S3 sont désactivées lorsque la tâche S3 Batch Replication est active. Cela garantit la parité entre les compartiments source et de destination. Dans le

cas contraire, le compartiment de destination risque de ne pas être une réplique exacte du compartiment source.

Architecture

Outils

AWS services

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Bonnes pratiques

La vidéo suivante de AWS re:Invent 2022 présente les meilleures pratiques d'utilisation de la réplication Amazon S3 pour la conformité réglementaire, la protection des données et l'amélioration des performances des applications.

https://www.youtube-nocookie.com/embed/ou JEb ISBL04 ? contrôles = 0

Épopées

Création d'une politique et d'un rôle IAM pour la réplication entre comptes dans le compte source

Tâche	Description	Compétences requises
Créez une politique IAM pour la réplication entre comptes.	Dans le compte AWS source : 1. Ouvrez la console IAM. 2. Créez une nouvelle politique IAM. 3. Dans la section Éditeur de politiques, choisissez JSON et collez le code suivant.	Administrateur du cloud, administrateur AWS

Tâche	Description	Compétences requises
	{ "Version": "2012-10-17", "Statement": [{ "Sid": "GetSourceBucketConfiguration", "Effect": "Allow", "Action": ["s3:ListBucket", "s3:GetBucketLocation", "s3:GetBucketAcl", "s3:GetReplicationConfiguration", "s3:GetObjectVersionForReplication", "s3:GetObjectVersionAcl", "s3:GetObjectVersionTagging"], "Resource": ["arn:aws:s3:::source-bucket-name", "arn:aws:s3:::source-bucket-name/*"]	

Tâche	Description	Compétences requises
	`},{"Sid": "ReplicateToDestinationBuckets","Effect": "Allow","Action": ["s3:List*","s3:*Object","s3:ReplicateObject","s3:ReplicateDelete","s3:ReplicateTags"],"Resource": ["arn:aws:s3:::destination-bucket-name*","arn:aws:s3:::destination-bucket-name/*"]},{"Sid": "PermissionToOverrideBucketOwner","Effect": "Allow","Action": [`	

Tâche	Description	Compétences requises

	<pre>"s3:ObjectOwnerOverrideToBucketOwner"
	            ],
	            "Resource": [
	"arn:aws:s3:::destination-bucket-name*",
	"arn:aws:s3:::destination-bucket-name/*"
	            ]
	        }
	    ]
	}</pre> Cette politique comprend trois déclarations :
	• `GetSourceBucketConfiguration` fournit un accès à la configuration de réplication et à la version de l'objet pour la réplication sur le compartiment source.
	• `ReplicateToDestinationBuckets` permet d'accéder à la réplication vers le compartiment de destination. Vous pouvez spécifier plusieurs compartiments	

Tâche	Description	Compétences requises
	de destination dans le tableau. • `PermissionToOverrideBucketOwner` fournit un accès à `ObjectOwnerOverrideToBucketOwner` afin que le compartiment de destination puisse posséder les objets du compte de destination qui ont été répliqués à partir du compte source. 4. Choisissez Next, saisissez un nom de stratégie tel que `cross-account-bucket-replication-policy`, puis choisissez Create policy. Pour plus d'informations, consultez Création de politiques IAM dans la documentation IAM.	

Tâche	Description	Compétences requises
Créez un rôle IAM pour la réplication entre comptes.	Dans le compte AWS source : 1. Sur la console IAM, créez un rôle IAM avec les informations suivantes : a. Pour le type d'entité de confiance, choisissez le service AWS. b. Pour le service, choisissez S3. c. Pour le cas d'utilisation, choisissez S3 Batch Operations. d. Choisissez la politique que vous avez créée à l'étape précédente. 2. Entrez un nom de rôle tel que cross-account-bucket-replication -role, puis choisissez Create role. Pour plus d'informations, consultez la section Création de rôles IAM dans la documentation IAM.	Administrateur du cloud, administrateur AWS

Création d'une règle de réplication dans le compte source

Tâche	Description	Compétences requises
Créez une règle de réplication par rapport au compartiment source dans le compte source.	Dans le compte AWS source :	Administrateur AWS, administrateur du cloud

Tâche	Description	Compétences requises
	1. Ouvrez la console Amazon S3. 2. Accédez au compartiment source, puis sélectionnez l'onglet Gestion. 3. Créez une règle de réplication avec la configuration suivante : a. Entrez un nom de règle tel que `s3-replication-rule` . b. Pour Statut, sélectionnez Enabled. c. Pour le champ d'application de la règle, choisissez S'applique à tous les objets du compartiment. d. Pour Destination, choisissez Spécifier un compartiment dans un autre compte, puis entrez le Compte AWS numéro de destination et le nom du compartiment. e. Choisissez l'option permettant de remplacer la propriété de l'objet par le propriétaire du compartiment de destination. f. Pour le rôle IAM, choisissez le rôle que vous avez créé	

Tâche	Description	Compétences requises
	précédemment dans le compte source. g. Pour Options de réplication supplémentaires, sélectionnez toutes les options disponibles. Ils permettent de répliquer le contenu rapidement, de surveiller la progression de la réplication grâce aux CloudWatch métriques Amazon, de répliquer les marqueurs de suppression et de répliquer les modifications des métadonnées. h. Choisissez Enregistrer. 4. Si vous avez plusieurs compartiments de destination, créez des règles de réplication supplémentaires. Pour plus d'informations, consultez la section Configuration de la réplication lorsque les compartiments source et de destination appartiennent à des comptes différents dans la documentation Amazon S3.	

Appliquer une politique de compartiment au compartiment de destination

Tâche	Description	Compétences requises
Appliquez une politique de compartiment au compartiment de destination.	Cette étape doit être effectuée pour chaque compartiment de destination individuellement dans les comptes de AWS destination. Dans le compte AWS de destination : 1. Ouvrez la console Amazon S3, accédez au compartiment de destination et choisissez l'onglet Permissions. 2. Modifiez la politique de compartiment en fournissant le code JSON suivant, puis enregistrez la politique : `{ "Version": "2012-10-17", "Id": "PolicyForDestinationBucket", "Statement": [ { "Sid": "Permissions on objects and buckets", "Effect": "Allow", "Principal": {`	Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
	"AWS": "arn:aws:iam::SourceAWSAccountNumber:role/IAM-Role-created-in-step1-in-source-account" }, "Action": ["s3:List*", "s3:GetBucketVersioning", "s3:PutBucketVersioning", "s3:ReplicateDelete", "s3:ReplicateObject"], "Resource": ["arn:aws:s3:::destination-bucket", "arn:aws:s3:::destination-bucket/*"] }, { "Sid": "Permission to override bucket owner", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::SourceAWSAccountNumber	

Tâche	Description	Compétences requises

	<pre>:role/IAM-Role-cre
	ated-in-step1-in-s
	ource-account"
	},
	"Action":
	"s3:ObjectOwnerOve
	rrideToBucketOwner",
	"Resource
	": "arn:aws:s3:::dest
	ination-bucket/*"
	}
	]
	}</pre>
	Cette politique inclut deux déclarations :
	• `Permissions on objects and bucketsindique` que le compartiment de destination peut répliquer le contenu en fonction du rôle défini dans le compte source. Le rôle fournit des autorisations au compartiment source.
	• `Permission to override bucket ownerindique` que le compartiment de destination est autorisé à remplacer la propriété du compte source.	

Testez la réplication entre comptes Amazon S3

Tâche	Description	Compétences requises
Vérifiez que la réplication fonctionne correctement.	1. Ajoutez un objet au compartiment source. 2. Vérifiez que le nouvel objet apparaît dans les compartiments S3 des comptes de destination. 3. Afficher CloudWatch les statistiques : a. Dans le compartiment source, choisissez l'onglet Metrics. b. Dans la section Mesures de réplication, sélectionnez une règle de réplication. c. Choisissez Display charts (Afficher les graphiques). Les graphiques reflètent l'état de la réplication en affichant les opérations en attente de réplication, la latence de réplication et les octets en attente de réplication. Pour plus d'informations, consultez la section Surveillance des métriques avec Amazon CloudWatch dans la documentation Amazon S3.	Administrateur AWS, administrateur du cloud

Ressources connexes

- Quand dois-je utiliser IAM ? (documentation IAM)
- Fonctionnement de l'IAM (documentation IAM)
- Création de rôles IAM (documentation IAM)
- Création de politiques IAM (documentation IAM)
- Présentation de la gestion des accès : autorisations et politiques (documentation IAM)
- Création, configuration et utilisation de compartiments Amazon S3 (documentation Amazon S3)
- Chargement, téléchargement et utilisation d'objets dans Amazon S3 (documentation Amazon S3)
- Réplication d'objets (documentation Amazon S3)

Migrez les données d'un environnement Hadoop sur site vers Amazon S3 à l'aide d' DistCp AWS PrivateLink pour Amazon S3

Créée par Jason Owens (AWS), Andres Cantor (AWS), Jeff Klopfenstein (AWS), Bruno Rocha Oliveira (AWS) et Samuel Schmidt (AWS)

Récapitulatif

Ce modèle montre comment migrer presque n'importe quel volume de données d'un environnement Apache Hadoop sur site vers le cloud Amazon Web Services (AWS) en utilisant l'outil open source Apache avec DistCpAWS pour PrivateLink Amazon Simple Storage Service (Amazon S3). Au lieu d'utiliser l'Internet public ou une solution proxy pour migrer les données, vous pouvez utiliser AWS PrivateLink pour Amazon S3 pour migrer les données vers Amazon S3 via une connexion réseau privée entre votre centre de données sur site et un Amazon Virtual Private Cloud (Amazon VPC). Si vous utilisez des entrées DNS dans Amazon Route 53 ou si vous ajoutez des entrées dans le fichier /etc/hosts dans tous les nœuds de votre cluster Hadoop sur site, vous êtes automatiquement dirigé vers le point de terminaison d'interface approprié.

Ce guide fournit des instructions d'utilisation DistCp pour migrer des données vers le cloud AWS. DistCp est l'outil le plus couramment utilisé, mais d'autres outils de migration sont disponibles. Par exemple, vous pouvez utiliser des outils AWS hors ligne tels qu'AWS Snowball ou AWS Snowmobile, ou des outils AWS en ligne tels qu'AWS Storage Gateway ou AWS. DataSync De plus, vous pouvez utiliser d'autres outils open source tels qu'Apache NiFi.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec une connexion réseau privée entre votre centre de données sur site et le cloud AWS
- Hadoop, installé sur site avec DistCp
- Un utilisateur Hadoop ayant accès aux données de migration dans le système de fichiers distribué Hadoop (HDFS)
- Interface de ligne de commande AWS (AWS CLI), installée et configurée
- Autorisations pour placer des objets dans un compartiment S3

Limites

Les limites du cloud privé virtuel (VPC) s'appliquent à AWS PrivateLink pour Amazon S3. Pour plus d'informations, consultez Propriétés et limites des points de terminaison de l'interface et PrivateLink quotas AWS (PrivateLink documentation AWS).

AWS PrivateLink pour Amazon S3 ne prend pas en charge les éléments suivants :

- Points de terminaison FIPS (Federal Information Processing Standard)
- Points de terminaison du site Web
- Points de terminaison globaux hérités

Architecture

Pile technologique source

- Cluster Hadoop avec installation DistCp

Pile technologique cible

- Amazon S3
- Amazon VPC

Architecture cible

Le schéma montre comment l'administrateur Hadoop copie des DistCp données depuis un environnement sur site via une connexion réseau privée, telle qu'AWS Direct Connect, vers Amazon S3 via un point de terminaison d'interface Amazon S3.

Outils

Services AWS

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que

vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Autres outils

- Apache Hadoop DistCp (copie distribuée) est un outil utilisé pour copier de grands inter-clusters et intra-clusters. DistCp utilise Apache MapReduce pour la distribution, la gestion des erreurs, la restauration et les rapports.

Épopées

Migrer les données vers le cloud AWS

Tâche	Description	Compétences requises
Créez un point de terminaison PrivateLink pour AWS pour Amazon S3.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, choisissez Endpoints, puis Create Endpoint. 3. En regard de Catégorie de service, choisissez Services AWS. 4. Dans la zone de recherche, entrez s3, puis appuyez sur Entrée. 5. Dans les résultats de recherche, sélectionnez com.amazonaws. < your-aws-region >Nom du service .s3 où la valeur de la colonne Type est Interface.	Administrateur AWS

Tâche	Description	Compétences requises
	6. Pour VPC, choisissez votre VPC. Pour les sous-réseaux, choisissez vos sous-réseaux. 7. Pour Groupe de sécurité, choisissez ou créez un groupe de sécurité qui autorise le protocole TCP 443. 8. Ajoutez des balises en fonction de vos besoins, puis choisissez Create endpoint.	

Tâche	Description	Compétences requises
Vérifiez les points de terminaison et recherchez les entrées DNS.	1. Ouvrez la console Amazon VPC, choisissez Endpoints, puis sélectionnez le point de terminaison que vous avez créé précédemment. 2. Dans l'onglet Détails, recherchez la première entrée DNS pour les noms DNS. Il s'agit de l'entrée DNS régionale. Lorsque vous utilisez ce nom DNS, les demandes alternent entre des entrées DNS spécifiques aux zones de disponibilité. 3. Choisissez l'onglet Sous-réseaux. Vous pouvez trouver l'adresse de l'interface elastic network du point de terminaison dans chaque zone de disponibilité.	Administrateur AWS

Tâche	Description	Compétences requises

Vérifiez les règles de pare-feu et les configurations de routage.	Pour vérifier que les règles de votre pare-feu sont ouvertes et que votre configuration réseau est correctement configuré e, utilisez Telnet pour tester le point de terminaison sur le port 443. Par exemple :
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	`Trying 10.104.88.6...`
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	`...`
	`$ telnet vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com 443`
	`Trying 10.104.71.141...`
	`Connected to vpce-<your-VPC-endpoint-ID>.s3.us-east-2.vpce.amazonaws.com.`
	Note
	Si vous utilisez l'entrée Regional, un test
		Administrateur réseau, administrateur AWS

Tâche	Description	Compétences requises
	réussi montre que le DNS alterne entre les deux adresses IP que vous pouvez voir dans l'onglet Sous-réseaux du point de terminais on sélectionné dans la console Amazon VPC.	

Tâche	Description	Compétences requises
Configurez la résolution du nom.	Vous devez configurer la résolution des noms pour permettre à Hadoop d'accéder au point de terminaison de l'interface Amazon S3. Vous ne pouvez pas utiliser le nom du point de terminaison lui-même. Au lieu de cela, vous devez résoudre `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` ou `*.s3.<your-aws-region>.amazonaws.com`. Pour plus d'informations sur cette limitation de dénomination, consultez Présentation du client Hadoop S3A (site Web Hadoop). Choisissez l'une des options de configuration suivantes : • Utilisez le DNS local pour résoudre l'adresse IP privée du point de terminaison. Vous pouvez modifier le comportement de tous les compartiments ou de certains compartiments. Pour plus d'informations, consultez « Option 2 : accéder à Amazon S3 à l'aide des zones de politique de réponse du système de	Administrateur AWS

Tâche	Description	Compétences requises
	noms de domaine (DNS RPZ) » dans Accès hybride sécurisé à Amazon S3 via AWS PrivateLink (article de blog AWS). • Configurez le DNS local pour transférer le trafic de manière conditionnelle vers les points de terminaison entrants du résolveur dans le VPC. Le trafic est redirigé vers la Route 53. Pour plus d'informations, consultez « Option 3 : transfert de requêtes DNS depuis un site à l'aide des points de terminaison entrants Amazon Route 53 » dans Accès hybride sécurisé à Amazon S3 via AWS (article de blog PrivateLink AWS). • Modifiez le fichier /etc/hosts sur tous les nœuds de votre cluster Hadoop. Il s'agit d'une solution temporaire pour les tests et n'est pas recommandée pour la production. Pour modifier le fichier /etc/hosts, ajoutez une entrée pour ou. `<your-bucket-name>.s3.<your-aws-region>.amazonaws.com` `s3.<your-aws-regio`	

Tâche	Description	Compétences requises
	n>.amazonaws.com Le fichier /etc/hosts ne peut pas avoir plusieurs adresses IP pour une entrée. Vous devez choisir une adresse IP unique dans l'une des zones de disponibilité, qui devient alors un point de défaillance unique.	

Tâche	Description	Compétences requises
Configurez l'authentification pour Amazon S3.	Pour vous authentifier auprès d'Amazon S3 via Hadoop, nous vous recommand ons d'exporter les informati ons d'identification de rôle temporaires vers l'environ nement Hadoop. Pour plus d'informations, consultez Authentification avec S3 (site Web Hadoop). Pour les tâches de longue durée, vous pouvez créer un utilisate ur et attribuer une politique autorisant à placer des données uniquement dans un compartiment S3. La clé d'accès et la clé secrète peuvent être stockées sur Hadoop, accessibles uniquement au DistCp job lui-même et à l'administrateur Hadoop. Pour plus d'informa tions sur le stockage des secrets, consultez Stockage des secrets avec les fournisse urs d'informations d'identif ication Hadoop (site Web Hadoop). Pour plus d'informa tions sur les autres méthodes d'authentification, consultez Comment obtenir les informati ons d'identification d'un rôle IAM à utiliser avec l'accès CLI à un compte AWS dans la	Administrateur AWS

Tâche	Description	Compétences requises

	documentation d'AWS IAM Identity Center (successeur d'AWS Single Sign-On).
	
	Pour utiliser des informations d'identification temporaires, ajoutez-les à votre fichier d'informations d'identification ou exécutez les commandes suivantes pour exporter les informations d'identification vers votre environnement :
	
	`export AWS_SESSION_TOKEN=SECRET-SESSION-TOKEN`
	`export AWS_ACCESS_KEY_ID=SESSION-ACCESS-KEY`
	`export AWS_SECRET_ACCESS_KEY=SESSION-SECRET-KEY`
	
	Si vous utilisez une combinaison classique de clé d'accès et de clé secrète, exécutez les commandes suivantes :
	
	`export AWS_ACCESS_KEY_ID=my.aws.key`
	`export AWS_SECRET_ACCESS_KEY=my.secret.key`	

Tâche	Description	Compétences requises
	Note Si vous utilisez une combinaison de clé d'accès et de clé secrète, remplacez le fournisseur d'informations d'identification dans les DistCp commandes par `"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" "org.apache.hadoop.fs.s3a.SimpleAWSCredentialsProvider"` .	

Tâche	Description	Compétences requises
Transférez des données en utilisant DistCp.	Pour DistCp transférer des données, exécutez les commandes suivantes : `hadoop distcp -Dfs.s3a.aws.credentials.provider=\"org.apache.hadoop.fs.s3a.TemporaryAWSCredentialsProvider" \ -Dfs.s3a.access.key="${AWS_ACCESS_KEY_ID}" \ -Dfs.s3a.secret.key="${AWS_SECRET_ACCESS_KEY}" \ -Dfs.s3a.session.token="${AWS_SESSION_TOKEN}" \ -Dfs.s3a.path.style.access=true \ -Dfs.s3a.connection.ssl.enabled=true \ -Dfs.s3a.endpoint=s3.<your-aws-region>.amazonaws.com \ hdfs:///user/root/ s3a://<your-bucket-name>` **Note** La région AWS du point de terminaison n'est pas automatiquement découverte lorsque vous utilisez	Ingénieur de migration, administrateur AWS

Tâche	Description	Compétences requises
	la DistCp commande avec AWS PrivateLink pour Amazon S3. Hadoop 3.3.2 et les versions ultérieures résolvent ce problème en activant l'option permettant de définir explicitement la région AWS du compartiment S3. Pour plus d'informations, consultez S3A pour ajouter l'option fs.s3a.endpoint.region afin de définir la région AWS (site Web Hadoop). Pour plus d'informations sur les fournisseurs S3A supplémentaires, consultez la section Configuration générale du client S3A (site Web Hadoop). Par exemple, si vous utilisez le chiffrement, vous pouvez ajouter l'option suivante à la série de commandes ci-dessus en fonction de votre type de chiffrement : `-Dfs.s3a.server-side-encryption-algo`	

Tâche	Description	Compétences requises
	`rithm=AES-256 [or SSE-C or SSE-KMS]` **Note** Pour utiliser le point de terminaison d'interface avec S3A, vous devez créer une entrée d'alias DNS pour le nom régional S3 (par exemple,`s3.<your-aws-region>.amazonaws.com`) du point de terminaison d'interface. Consultez la section Configurer l'authentification pour Amazon S3 pour obtenir des instructions. Cette solution de contournement est requise pour Hadoop 3.3.2 et les versions antérieures. Les futures versions de S3A ne nécessiteront pas cette solution de contournement. Si vous rencontrez des problèmes de signature avec Amazon S3, ajoutez une	

Tâche	Description	Compétences requises
	option permettant d'utiliser la signature Signature Version 4 (Sigv4) : `-Dmapreduce.map.java.opts="-Dcom.amazonaws.services.s3.enableV4=true"`	

Plus de modèles

- Accès Services AWS depuis IBM z/OS en installant le AWS CLI
- Automatisez les sauvegardes basées sur les événements depuis Amazon S3 CodeCommit à l'aide CodeBuild de and Events CloudWatch
- Archivez automatiquement les éléments sur Amazon S3 à l'aide de DynamoDB TTL
- Sauvegardez automatiquement les bases de données SAP HANA à l'aide de Systems Manager et EventBridge
- Sauvegardez et archivez les données du mainframe sur Amazon S3 à l'aide de BMC AMI Cloud Data
- Créez un pipeline de services ETL pour charger les données de manière incrémentielle d'Amazon S3 vers Amazon Redshift à l'aide d'AWS Glue
- Configurez la journalisation des appels de modèles dans Amazon Bedrock en utilisant AWS CloudFormation
- Convertissez et décompressez les données EBCDIC en ASCII sur AWS à l'aide de Python
- Convertir VARCHAR2 (1) le type de données pour Oracle en type de données booléen pour Amazon Aurora PostgreSQL
- Créez une définition de tâche Amazon ECS et montez un système de fichiers sur des EC2 instances à l'aide d'Amazon EFS
- Fournissez des enregistrements DynamoDB à Amazon S3 à l'aide de Kinesis Data Streams et Firehose avec AWS CDK
- Déployez un système de fichiers Lustre pour un traitement des données performant à l'aide de Terraform et DRA
- Estimation des coûts de stockage pour une table Amazon DynamoDB
- Identifiez les compartiments Amazon S3 publics à l'aide AWS Organizations de Security Hub
- Migrer les instances de base de données Amazon RDS for Oracle vers d'autres comptes utilisant AMS
- Migrer un serveur SFTP sur site vers AWSAWS Transfer for SFTP
- Migrer une table partitionnée Oracle vers PostgreSQL à l'aide d'AWS DMS
- Migrez les données de Microsoft Azure Blob vers Amazon S3 à l'aide de Rclone
- Migrer les valeurs Oracle CLOB vers des lignes individuelles dans PostgreSQL sur AWS
- Migrer des systèmes de fichiers partagés dans le cadre d'une migration AWS de grande envergure

- Migrez de petits ensembles de données sur site vers Amazon S3 à l'aide d'AWS SFTP
- Surveillez Amazon Aurora pour détecter les instances sans chiffrement
- Déplacez les fichiers du mainframe directement vers Amazon S3 à l'aide de Transfer Family
- Supprimez EC2 les entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Exécutez des charges de travail dynamiques avec un stockage de données persistant en utilisant Amazon EFS sur Amazon EKS avec AWS Fargate
- Importation réussie d'un compartiment S3 en tant que CloudFormation stack AWS
- Synchronisez les données entre les systèmes de fichiers Amazon EFS dans différentes régions AWS à l'aide d'AWS DataSync
- Afficher les détails des instantanés EBS pour votre compte AWS ou votre organisation

Outils pour développeurs

Rubriques

- DevOps
- Infrastructure
- Applications Web et mobiles

DevOps

Rubriques

- Automatisez AWS les opérations d'infrastructure en utilisant Amazon Bedrock
- Automatisez les CloudFront mises à jour lorsque les points de terminaison de l'équilibreur de charge changent à l'aide de Terraform
- Automatisez les CodeGuru révisions Amazon pour les applications AWS CDK Python à l'aide d' GitHub Actions
- Automatisez l'évaluation des ressources AWS
- Installez automatiquement les systèmes SAP à l'aide d'outils open source
- Automatisez le déploiement du portefeuille et des produits AWS Service Catalog à l'aide d'AWS CDK
- Automatisez les sauvegardes basées sur les événements depuis Amazon S3 CodeCommit à l'aide CodeBuild de and Events CloudWatch
- Automatisez la suppression des AWS CloudFormation piles et des ressources associées
- Automatisez la gestion dynamique du pipeline pour le déploiement de solutions de correctifs dans les environnements Gitflow en utilisant et AWS Service CatalogAWS CodePipeline
- Automatisez l'ingestion et la visualisation des métriques personnalisées Amazon MWAA sur Amazon Managed Grafana à l'aide de Terraform
- Simplifiez le développement et le déploiement des robots Amazon Lex à l'aide d'un flux de travail automatisé
- Automatisez le déploiement d'ensembles de piles à l'aide d'AWS CodePipeline et d'AWS CodeBuild
- Associez automatiquement une politique gérée par AWS pour Systems Manager aux profils d' EC2 instance à l'aide de Cloud Custodian et d'AWS CDK
- Créez automatiquement des pipelines CI/CD et des clusters Amazon ECS pour les microservices à l'aide d'AWS CDK
- Créez une architecture faiblement couplée avec des microservices en utilisant DevOps Practices et AWS Cloud9
- Créez et envoyez des images Docker vers Amazon ECR à l'aide d' GitHub Actions et de Terraform
- Créez et testez des applications iOS avec AWS CodeCommit CodePipeline, AWS et AWS Device Farm

- Consultez les applications ou les CloudFormation modèles AWS CDK pour connaître les meilleures pratiques à l'aide des packs de règles cdk-nag
- Configurer l'authentification TLS mutuelle pour les applications exécutées sur Amazon EKS
- Automatisez la création de ressources AppStream 2.0 à l'aide d'AWS CloudFormation
- Créez un analyseur de journaux personnalisé pour Amazon ECS à l'aide d'un routeur de journaux Firelens
- Création d'un pipeline et d'une AMI à l'aide de CodePipeline and HashiCorp Packer
- Créez un pipeline et déployez des mises à jour d'artefacts sur des instances locales à l'aide de EC2 CodePipeline
- Créez automatiquement des pipelines CI dynamiques pour les projets Java et Python
- Déployez des CloudWatch canaris Synthetics à l'aide de Terraform
- Déployer un pipeline CI/CD pour les microservices Java sur Amazon ECS
- Déployez une ChatOps solution pour gérer les résultats du scan SAST en utilisant Amazon Q Developer dans les applications de chat, les actions personnalisées et AWS CloudFormation
- Déployez un pare-feu à l'aide d'AWS Network Firewall et d'AWS Transit Gateway
- Déployer une tâche AWS Glue avec un pipeline AWS CodePipeline CI/CD
- Déployez un cluster Amazon EKS depuis AWS Cloud9 à l'aide d'un profil d'instance EC2
- Déployez du code dans plusieurs régions AWS à l'aide d'AWS CodePipeline CodeCommit, AWS et AWS CodeBuild
- Exécutez des requêtes SQL Amazon Redshift à l'aide de Terraform
- Exportez les rapports AWS Backup de l'ensemble d'une organisation dans AWS Organizations sous forme de fichier CSV
- Exporter les balises d'une liste d' EC2 instances Amazon vers un fichier CSV
- Générez un CloudFormation modèle AWS contenant les règles gérées par AWS Config à l'aide de Troposphere
- Donnez aux instances de SageMaker bloc-notes un accès temporaire à un CodeCommit référentiel dans un autre compte AWS
- Mettre en œuvre une stratégie GitHub de branchement Flow pour les environnements multi-comptes DevOps
- Mettre en œuvre une stratégie de branchement Gitflow pour les environnements multi-comptes DevOps

- Mettre en œuvre une stratégie de branchement de type Trunk pour les environnements multi-comptes DevOps
- Mettez en œuvre une analyse Checkov personnalisée et centralisée pour appliquer la politique avant de déployer AWS l'infrastructure
- Détectez automatiquement les modifications et lancez différents CodePipeline pipelines pour un monorepo dans CodeCommit
- Intégrer un référentiel Bitbucket à AWS Amplify à l'aide d'AWS CloudFormation
- Lancez un CodeBuild projet sur des comptes AWS à l'aide de Step Functions et d'une fonction proxy Lambda
- Gérez le basculement multi-AZ pour les clusters EMR à l'aide d'Application Recovery Controller
- Gérez les déploiements bleu/vert de microservices vers plusieurs comptes et régions à l'aide des services de code AWS et des clés multirégionales AWS KMS
- Surveillez les référentiels Amazon ECR pour détecter les autorisations génériques à l'aide d'AWS et d'AWS Config CloudFormation
- Optimisez les déploiements multicomptes sans serveur en utilisant les flux de travail et AWS CDK Actions GitHub
- Effectuez des actions personnalisées à partir d' CodeCommit événements AWS
- Provisionner AWS Service Catalog des produits basés sur AWS CloudFormation des modèles à l'aide d' GitHub actions
- Fournissez des rôles IAM avec le moindre privilège en déployant une solution de distribution automatique de rôles
- Publier CloudWatch les statistiques Amazon dans un fichier CSV
- Supprimez EC2 les entrées Amazon Comptes AWSAWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Supprimez EC2 les entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Exécutez des tests unitaires pour les tâches ETL Python en AWS Glue utilisant le framework pytest
- Configuration d'un référentiel de graphiques Helm v3 dans Amazon S3
- Configuration d'un pipeline CI/CD à l'aide d'AWS et d' CodePipeline AWS CDK
- Configurez une journalisation centralisée à l'échelle de l'entreprise à l'aide de Terraform
- Configurer le end-to-end chiffrement des applications sur Amazon EKS à l'aide du gestionnaire de certificats et de Let's Encrypt

- Simplifiez le déploiement d'applications multi-locataires Amazon EKS à l'aide de Flux
- Abonnement de plusieurs points de terminaison de messagerie à une rubrique SNS à l'aide d'une ressource personnalisée
- Coordonnez la dépendance des ressources et l'exécution des tâches à l'aide de la structure AWS Fargate WaitCondition hook
- Utiliser des référentiels sources Git tiers dans AWS CodePipeline
- Créez un pipeline CI/CD pour valider les configurations Terraform à l'aide d'AWS CodePipeline
- Plus de modèles

Automatisez AWS les opérations d'infrastructure en utilisant Amazon Bedrock

Créée par Ishwar Chauthaiwale (AWS) et Anand Bukkapatnam Tirumala (AWS)

Récapitulatif

Dans les solutions cloud natives, l'automatisation des opérations d'infrastructure communes joue un rôle essentiel dans le maintien d'environnements efficaces, sécurisés et rentables. La gestion manuelle des opérations prend du temps et est sujette à des erreurs humaines. En outre, les membres de l'équipe ayant différents niveaux d' AWS expertise doivent effectuer ces tâches tout en garantissant le respect des protocoles de sécurité. Ce modèle montre comment utiliser Amazon Bedrock pour automatiser les opérations d' AWS infrastructure courantes par le biais du traitement du langage naturel (NLP).

Ce modèle peut aider les entreprises à développer un code réutilisable, modulaire et sécurisé pour déployer une infrastructure générative basée sur l'IA dans plusieurs environnements. En mettant l'accent sur l'infrastructure en tant que code (IaC) et l'automatisation, il offre des DevOps avantages clés, notamment le contrôle des versions, des déploiements cohérents, une réduction des erreurs, un provisionnement plus rapide et une collaboration améliorée.

Le modèle met en œuvre une architecture sécurisée qui permet aux équipes de gérer les opérations liées aux clés Services AWS , notamment :

- Gestion des versions des compartiments Amazon Simple Storage Service (Amazon S3)
- Création d'instantanés Amazon Relational Database Service (Amazon RDS)
- Gestion des instances Amazon Elastic Compute Cloud (Amazon EC2)

L'architecture utilise des points de terminaison Amazon Virtual Private Cloud (Amazon VPC) et un réseau privé pour une communication sécurisée, avec des AWS Lambda fonctions fonctionnant comme des exécuteurs de tâches au sein de sous-réseaux privés. Amazon S3 assure la gestion des données et met en œuvre des rôles et des autorisations complets AWS Identity and Access Management (IAM) pour garantir des contrôles d'accès appropriés. Cette solution n'inclut pas de fonctionnalité d'historique des discussions, et la discussion n'est pas stockée.

Conditions préalables et limitations

- Un actif Compte AWS.

- Des mesures de contrôle d'accès appropriées doivent être mises en place pour sécuriser et contrôler l'accès. Les exemples de contrôle d'accès incluent l'utilisation de l'accès aux modèles de base AWS Systems Manager, un rôle IAM pour le déploiement et des rôles basés sur les services, la désactivation de l'accès public aux compartiments Amazon S3 et la mise en place d'une file d'attente de lettres mortes.
- Une AWS Key Management Service (AWS KMS) clé gérée par le client.
- AWS Command Line Interface (AWS CLI) version 2 ou ultérieure, installée et configurée dans l'environnement de déploiement.
- Terraform AWS Provider version 4 ou ultérieure installée et configurée.
- Terraform version 1.5.7 ou ultérieure installée et configurée.
- Passez en revue et définissez des schémas OpenAPI pour les groupes d'action de vos agents dans Amazon Bedrock afin de vous protéger contre les accès non autorisés et de préserver l'intégrité des données.
- Accès activé dans votre compte Compte AWS pour les Amazon Titan Text Embeddings v2 requis et pour les modèles de base Claude 3.5 Sonnet ou Claude 3 Haiku. Pour éviter l'échec du déploiement, vérifiez que votre déploiement cible Région AWS prend en charge les modèles requis.
- Un cloud privé virtuel (VPC) configuré conformément aux meilleures pratiques du AWS Well Architected Framework.
- Révision de la politique Amazon Responsible AI terminée.

Versions du produit

- Amazon Titan Text Embeddings v2
- Sonnet Anthropic Claude 3.5 ou Haïku Claude 3
- Terraform AWS Provider version 4 ou ultérieure
- Terraform version 1.5.7 ou ultérieure

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

L'architecture de la solution se compose de plusieurs couches qui fonctionnent ensemble pour traiter les demandes en langage naturel et exécuter les AWS opérations correspondantes :

1. L'utilisateur fait des demandes d'opérations via la console de chat Amazon Bedrock.
2. Le chatbot utilise les bases de connaissances Amazon Bedrock pour le traitement des demandes. Il implémente le modèle Amazon Titan Text Embeddings v2 pour le traitement du langage naturel.
3. Si l'invite utilisateur inclut une demande d'action, le groupe d'actions Amazon Bedrock utilise le modèle Anthropic Claude 3 Haiku ou le modèle Claude 3.5 Sonnet (selon votre choix) pour la logique d'exécution et définit les opérations via un schéma OpenAPI.
4. Le groupe d'actions atteint les points de terminaison Amazon VPC à l'aide d'une communication AWS PrivateLink de service sécurisée.
5. La AWS Lambda fonction est accessible via les points de terminaison Amazon VPC pour les services Amazon Bedrock.
6. Les fonctions Lambda constituent le principal moteur d'exécution. Sur la base de la demande, la fonction Lambda appelle l'API pour effectuer des actions sur le. Services AWS La fonction Lambda gère également le routage et l'exécution des opérations.
7. La requête Services AWS get the API from the Lambda et les opérations correspondantes sont effectuées.
8. La fonction Lambda calcule une charge utile de sortie comprise par Amazon Bedrock.
9. Cette charge utile est envoyée à Amazon Bedrock à l'aide d'une communication PrivateLink de service sécurisée. Le modèle de langage étendu (LLM) utilisé par Amazon Bedrock comprend cette charge utile et la convertit dans un format compréhensible par l'homme.
10. Le résultat est ensuite présenté à l'utilisateur sur la console de discussion Amazon Bedrock.

La solution permet les opérations principales suivantes :

- Amazon S3 — Activez la gestion des versions des compartiments pour le contrôle des versions.
- Amazon RDS — Créez des instantanés de base de données à des fins de sauvegarde.
- Amazon EC2 — Répertoriez les instances et contrôlez le démarrage et l'arrêt des instances.

Outils

Services AWS

- Amazon Bedrock est un service entièrement géré qui met à votre disposition des modèles de base très performants (FMs) issus des principales startups d'IA et d'Amazon via une API unifiée.

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon OpenSearch Serverless est une configuration sans serveur à la demande pour Amazon OpenSearch Service.
- AWS PrivateLinkvous permet de créer des connexions privées unidirectionnelles entre vos clouds privés virtuels (VPCs) et des services extérieurs au VPC.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le. AWS Cloud
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Autres outils

- Git est un système de contrôle de version distribué et open source.
- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub infra-ops-orchestratoraws-samples/.

Bonnes pratiques

- Surveillez régulièrement les journaux d'exécution Lambda. Pour plus d'informations, consultez la section Surveillance et résolution des problèmes des fonctions Lambda. Pour plus d'informations sur les meilleures pratiques, voir Meilleures pratiques d'utilisation des AWS Lambda fonctions.
- Passez régulièrement en revue les configurations de sécurité pour vous assurer qu'elles sont conformes aux exigences de votre entreprise. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité.
- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Déployez la solution

Tâche	Description	Compétences requises

Pour cloner le référentiel.	Pour cloner le dépôt sur votre machine locale, exécutez la commande suivante :
	`git clone "git@github.com:aws-samples/infra-ops-orchestrator.git"`
	`cd infra-ops-orchestrator`
		AWS DevOps, DevOps ingénieur

Modifiez les variables d'environnement.	Modifiez le `terraform.tfvars` fichier. dans le répertoire racine du dépôt cloné. Passez en revue les espaces réservés indiqués par `[XXXXX]` et mettez-les à jour	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	en fonction de votre environnement.	

Créez l'infrastructure.	Pour créer l'infrastructure, exécutez les commandes suivantes :
	`terraform init`
	`terraform plan`
	Révisez attentivement le plan d'exécution. Si les modifications prévues sont acceptables, exécutez la commande suivante :
	`terraform apply --auto-approve`
		AWS DevOps, DevOps ingénieur

Accédez à la solution

Tâche	Description	Compétences requises
Accédez à la solution.	Une fois le déploiement réussi, procédez comme suit pour utiliser l'interface basée sur le chat : 1. Pour accéder à l'assistant Infrastructure Orchestrator, connectez-vous à l'AWS Management Console aide d'un rôle IAM avec	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	les autorisations Amazon Bedrock et ouvrez la console Amazon Bedrock à l'adresse. https://console.aws.amazon.com/bedrock/ Sélectionnez Agents dans le volet de navigation de gauche. Choisissez ensuite l'assistant Infrastructure Orchestrator dans la section Agents. 2. Assurez-vous que des ressources cibles existent dans votre AWS environnement pour les suggestions suivantes, puis essayez ces exemples d'opérations : • Créez une sauvegarde instantanée d'une instance Amazon RDS en demandant : « Créer un instantané de l'instance RDS [nom de l'instance] » • Activez le contrôle de version sur un compartiment Amazon S3 en demandant : « Activer le contrôle de version pour le compartiment [nom du compartiment] » • Répertoriez EC2 les instances Amazon en demandant : « Répertori	

Tâche	Description	Compétences requises
	er toutes les EC2 instances » • Démarrez ou arrêtez une EC2 instance Amazon en demandant : « Start EC2 instance [instance-id] » ou « Stop EC2 instance [instance-id] » Remarque : remplacez les valeurs entre crochets par les noms de ressources réels ou ceux IDs de votre AWS environnement.	

Nettoyage des ressources

Tâche	Description	Compétences requises

Supprimez les ressources créées.	Pour supprimer toute l'infrast ructure créée par ce modèle, exécutez la commande suivante :
	`terraform plan -destroy`
	Révisez attentivement le plan de destruction. Si les suppressions prévues sont acceptables, exécutez la commande suivante :
	`terraform destroy`
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	Remarque : Cette commande supprimera définitivement toutes les ressources créées par ce modèle. La commande demandera une confirmat ion avant de supprimer des ressources.	

Résolution des problèmes

Problème	Solution
Comportement des agents	Pour plus d'informations sur ce problème, consultez la section Tester et résoudre les problèmes du comportement des agents dans la documentation Amazon Bedrock.
Problèmes liés au réseau Lambda	Pour plus d'informations sur ces problèmes, consultez la section Résoudre les problèmes de réseau dans Lambda dans la documentation Lambda.
Autorisations IAM	Pour plus d'informations sur ces problèmes, consultez la section Résolution des problèmes liés à l'IAM dans la documentation IAM.

Ressources connexes

- Création d'un instantané de base de données pour une instance de base de données mono-AZ pour Amazon RDS
- Définissez des schémas OpenAPI pour les groupes d'action de votre agent dans Amazon Bedrock
- Activation de la gestion des versions sur les buckets
- Comment fonctionne Amazon Bedrock Agents

- Récupérez des données et générez des réponses basées sur l'IA avec les bases de connaissances Amazon Bedrock
- Accédez en toute sécurité à Services Over AWS PrivateLink
- Arrêtez et démarrez les EC2 instances Amazon
- Utilisez des groupes d'actions pour définir les actions à exécuter par votre agent

Automatisez les CloudFront mises à jour lorsque les points de terminaison de l'équilibreur de charge changent à l'aide de Terraform

Créée par Tamilselvan (AWS), Mohan Annam (AWS) et Naveen Suthar (AWS)

Récapitulatif

Lorsque les utilisateurs d'Amazon Elastic Kubernetes Service (Amazon EKS) suppriment et réinstallent leur configuration d'entrée via des graphiques Helm, un nouvel Application Load Balancer (ALB) est créé. Cela pose problème car Amazon CloudFront continue de faire référence à l'enregistrement DNS de l'ancien ALB. Par conséquent, les services destinés à ce point de terminaison ne seront pas accessibles. (Pour plus de détails sur ce flux de travail problématique, voir Informations supplémentaires.)

Pour résoudre ce problème, ce modèle décrit l'utilisation d'une AWS Lambda fonction personnalisée développée avec Python. Cette fonction Lambda détecte automatiquement lorsqu'un nouvel ALB est créé par le biais des règles Amazon. EventBridge À l'aide de AWS SDK pour Python (Boto3), la fonction met ensuite à jour la CloudFront configuration avec l'adresse DNS du nouvel ALB, garantissant ainsi que le trafic est acheminé vers le point de terminaison approprié.

Cette solution automatisée assure la continuité du service sans routage ni latence supplémentaires. Le processus permet de garantir qu'il fait CloudFront toujours référence au point de terminaison DNS ALB correct, même lorsque l'infrastructure sous-jacente change.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Exemple d'application Web de test et de validation déployée sur Amazon EKS à l'aide de Helm. Pour plus d'informations, consultez la section Déployer des applications avec Helm sur Amazon EKS dans la documentation Amazon EKS.
- Configurez CloudFront pour acheminer les appels vers un ALB créé par un contrôleur d'entrée Helm. Pour plus d'informations, consultez Installer le contrôleur AWS Load Balancer avec Helm dans la documentation Amazon EKS et Restreindre l'accès aux équilibreurs de charge d'application dans la documentation. CloudFront
- Terraform installé et configuré dans un espace de travail local.

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Terraform version 1.0.0 ou ultérieure
- Terraform AWS Provider version 4.20 ou ultérieure

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Cette solution exécute les étapes suivantes :

1. Le contrôleur d'entrée Amazon EKS crée un nouvel Application Load Balancer (ALB) à chaque redémarrage ou déploiement de Helm.
2. EventBridge recherche les événements de création d'ALB.
3. L'événement de création ALB déclenche la fonction Lambda.
4. La fonction Lambda a été déployée sur la base de python 3.9 et utilise l'API boto3 pour appeler. Services AWS La fonction Lambda met à jour l' CloudFront entrée avec le dernier nom DNS de l'équilibreur de charge, qui provient des événements de création de l'équilibreur de charge.

Outils

Services AWS

- Amazon CloudFront accélère la diffusion de votre contenu Web en le diffusant via un réseau mondial de centres de données, ce qui réduit le temps de latence et améliore les performances.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par

exemple, AWS Lambda des fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS

- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

Autres outils

- Python est un langage de programmation informatique polyvalent.
- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub aws-cloudfront-automation-terraform-samples.

Épopées

Configuration d'un poste de travail local

Tâche	Description	Compétences requises
Configurez et configurez la CLI Git.	Pour installer et configure r l'interface de ligne de commande (CLI) Git sur votre poste de travail local, suivez les instructions Getting Started — Install Git de la documenta tion Git.	DevOps ingénieur
Créez le dossier du projet et ajoutez les fichiers.	1. Accédez au GitHub référentiel du modèle, puis cliquez sur le bouton Code.	DevOps ingénieur

Tâche	Description	Compétences requises
	2. Dans la boîte de dialogue Cloner, choisissez l'onglet HTTPS. Dans Cloner à l'aide de l'URL Web, copiez l'URL affichée. 3. Créez un dossier sur votre ordinateur local. Nommez-le avec le nom de votre projet. 4. Ouvrez un terminal sur votre ordinateur local et accédez à ce dossier. 5. Pour cloner le dépôt git de ce modèle, exécutez la commande suivante : `git clone https://github.com/aws-samples/aws-cloudfront-automation-terraform-samples` 6. Une fois le dépôt cloné, utilisez la commande suivante pour accéder au répertoire cloné : `cd <directory name>/cloudfront-update` Ouvrez ce projet dans un environnement de développement intégré (IDE) de votre choix.	

Provisionner l'architecture cible à l'aide de la configuration Terraform

Tâche	Description	Compétences requises

Déployez la solution.	Pour déployer des ressources dans la cible Compte AWS, procédez comme suit :
	1. Accédez au dossier `cloudfront-update` .
	2. Mettez à jour le `terraform.tfvars` fichier avec le`cloudfront_distribution_id` .
	3. Pour définir le Région AWS pour votre AWS profil, exécutez la commande suivante :
	`export AWS_REGION={{ REGION }}`
	4. Pour initialiser Terraform, exécutez la commande suivante :
	`terraform init`
	5. Pour valider Terraform, exécutez la commande suivante :
	`terraform validate`
	6. Pour créer un plan d'exécution Terraform, exécutez la commande suivante :
		DevOps ingénieur

Tâche	Description	Compétences requises

	`terraform plan`
	7. Pour appliquer les actions depuis`terraform plan`, exécutez la commande suivante :
	`terraform apply`	

Vérification du déploiement

Tâche	Description	Compétences requises
Validez le déploiement.	1. Connectez-vous à la CloudFront console Amazon AWS Management Console et ouvrez-la sur https://console.aws.amazon.com/cloudfront/v4/home. 2. Dans le volet de navigation de gauche, choisissez Distributions, puis ouvrez la CloudFront distribution. 3. Dans l'onglet Origins, vérifiez que le nom d'origine et le mappage d'origine contiennent l'enregistrement DNS ALB mis à jour.	DevOps ingénieur

Nettoyer les infrastructures

Tâche	Description	Compétences requises
Nettoyez l'infrastructure.	Pour nettoyer l'infrast ructure que vous avez créée précédemment, procédez comme suit : 1. Exécutez la commande suivante: `terraform destroy` 2. Pour confirmer la commande de destruction, entrez `yes`.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Erreur lors de la validation des informations d'identification du fournisseur	Lorsque vous exécutez le Terraform `apply` ou `destroy` les commandes depuis votre machine locale, vous pouvez rencontrer une erreur similaire à la suivante : `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Cette erreur est due à l'expiration du jeton de sécurité pour les informations d'identification

Problème	Solution
	utilisées dans la configuration de votre machine locale. Pour résoudre l'erreur, consultez la section Définir et afficher les paramètres de configuration dans la documentation AWS Command Line Interface (AWS CLI).

Ressources connexes

AWS resources

- Restreindre l'accès aux équilibreurs de charge des applications
- Acheminez le trafic Internet avec le AWS Load Balancer Controller

Documentation Terraform

- AWS Fournisseur
- Installez Terraform
- État distant

Informations supplémentaires

Flux de travail problématique

Le schéma suivant illustre le flux de travail suivant :

1. Lorsque l'utilisateur accède à l'application, l'appel passe à CloudFront.
2. CloudFront achemine les appels vers l'Application Load Balancer (ALB) correspondant.
3. L'ALB inclut les adresses IP cibles qui sont les adresses IP du pod d'application. À partir de là, l'ALB fournit les résultats attendus à l'utilisateur.

Toutefois, ce flux de travail présente un problème. Les déploiements d'applications se font par le biais de diagrammes Helm. Chaque fois qu'il y a un déploiement ou si quelqu'un redémarre Helm, l'entrée correspondante est également recréée. Par conséquent, le contrôleur d'équilibrage de charge externe recrée l'ALB. De plus, lors de chaque recréation, l'ALB est recréé avec un nom DNS différent. De ce fait, l'entrée dans les paramètres d'origine CloudFront sera obsolète. En raison de cette entrée périmée, l'application ne sera pas accessible à l'utilisateur. Ce problème entraîne des interruptions de service pour les utilisateurs.

Solution alternative

Une autre solution possible consiste à créer un DNS externe pour l'ALB, puis à le pointer vers le point de terminaison de la zone hébergée privée Amazon Route 53. CloudFront Cependant, cette approche ajoute un autre saut dans le flux des applications, ce qui peut entraîner une latence des applications. La solution de fonction Lambda de ce modèle ne perturbe pas le flux de courant.

Automatisez les CodeGuru révisions Amazon pour les applications AWS CDK Python à l'aide d' GitHub Actions

Créée par Vanitha Dontireddy (AWS) et Sarat Chandra Pothula (AWS)

Récapitulatif

Ce modèle illustre l'intégration des révisions de code CodeGuru automatisées Amazon pour les applications AWS Cloud Development Kit (AWS CDK) Python, orchestrées par le biais GitHub d'actions. La solution déploie une architecture sans serveur définie en Python AWS CDK . En automatisant l'analyse du code expert au sein du pipeline de développement, cette approche permet d'obtenir les résultats suivants pour les projets AWS CDK Python :

- Améliorez la qualité du code.
- Simplifiez les flux de travail
- Maximisez les avantages de l'informatique sans serveur.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Command Line Interface (AWS CLI) version 2.9.11 ou ultérieure, installée et configurée.
- Un GitHub compte actif et un GitHub référentiel avec des autorisations de lecture et d'écriture dans le flux de travail et la création de pull requests (PR) par GitHub Actions pour garantir le bon fonctionnement du flux de travail des relations publiques.
- Un rôle OpenID Connect (OIDC) dans GitHub Actions pour déployer la solution dans le. Compte AWS Pour créer le rôle, utilisez la AWS CDK construction.

Limites

- Amazon CodeGuru Profiler prend en charge les applications écrites dans tous les langages de machine virtuelle Java (JVM) (tels que Scala et Kotlin) et les environnements d'exécution, ainsi que Python 3.6 ou version ultérieure.
- Amazon CodeGuru Reviewer prend en charge les associations avec les référentiels de code Java et Python provenant uniquement des fournisseurs de sources suivants : AWS CodeCommit

Bitbucket GitHub, GitHub Enterprise Cloud et GitHub Enterprise Server. En outre, les référentiels Amazon Simple Storage Service (Amazon S3) ne sont pris en charge que par le biais d'actions. GitHub

- Il n'existe aucun moyen automatique d'imprimer les résultats pendant le pipeline d'intégration continue et de déploiement continu (CI/CD). Ce modèle utilise plutôt GitHub les actions comme méthode alternative pour gérer et afficher les résultats.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant montre l'architecture de cette solution.

Comme le montre le schéma, lorsqu'un développeur crée une pull request (PR) à des fins de révision, GitHub Actions déclenche les étapes suivantes :

1. Hypothèse du rôle IAM — Le pipeline utilise le rôle IAM spécifié dans GitHub Secrets pour effectuer les tâches de déploiement.
2. Analyse du code
   - CodeGuru Reviewer analyse le code stocké dans le compartiment Amazon S3. Il identifie les défauts et fournit des recommandations pour les corriger et les optimiser.
   - CodeGuru Analyses de sécurité pour détecter les violations des politiques et les vulnérabilités.
3. Examen des résultats
   - Le pipeline imprime un lien vers le tableau de bord des résultats dans la sortie de la console.
   - Si des résultats critiques sont détectés, le pipeline tombe immédiatement en panne.
   - Pour les résultats de gravité élevée, normale ou faible, le pipeline passe à l'étape suivante.
4. Approbation PR
   - Un réviseur doit approuver manuellement le PR.
   - Si le PR est refusé, le pipeline échoue et interrompt les étapes de déploiement ultérieures.
5. Déploiement du CDK — Une fois le PR approuvé, le processus de déploiement du CDK commence. Il met en place les éléments suivants Services AWS et les ressources :

- CodeGuru Profileur
- AWS Lambda fonction
- File d'attente Amazon Simple Queue Service (Amazon SQS)

6. Génération de données de profilage — Pour générer suffisamment de données de profilage pour CodeGuru Profiler :
   - Le pipeline invoque la fonction Lambda à plusieurs reprises en envoyant régulièrement des messages à la file d'attente Amazon SQS.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- CDK Toolkit est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre AWS CDK application.
- Amazon CodeGuru Profiler collecte les données de performances d'exécution de vos applications en ligne et fournit des recommandations qui peuvent vous aider à affiner les performances de vos applications.
- Amazon CodeGuru Reviewer utilise l'analyse des programmes et l'apprentissage automatique pour détecter les défauts potentiels difficiles à détecter pour les développeurs. CodeGuru Profiler propose ensuite des suggestions pour améliorer votre code Java et Python.
- Amazon CodeGuru Security est un outil de sécurité des applications statique qui utilise l'apprentissage automatique pour détecter les violations des politiques de sécurité et les vulnérabilités. Il fournit des suggestions pour faire face aux risques de sécurité et génère des métriques afin que vous puissiez suivre le niveau de sécurité de vos applications.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- GitHub Actions est une plateforme d'intégration et de livraison continues (CI/CD) étroitement intégrée aux GitHub référentiels. Vous pouvez utiliser GitHub les actions pour automatiser votre pipeline de création, de test et de déploiement.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub amazon-codeguru-suite-cdk-python.

Bonnes pratiques

- Adhérez aux meilleures pratiques pour développer et déployer une infrastructure cloud avec le AWS CDK.
- Suivez les meilleures pratiques de sécurité dans IAM lors de l'utilisation des flux de travail Services AWS in GitHub Actions, notamment :
  - Ne stockez pas les informations d'identification dans le code de votre référentiel.
  - Assumez un rôle IAM pour recevoir des informations d'identification temporaires, et utilisez des informations d'identification temporaires lorsque cela est possible.
  - Accordez le moindre privilège au rôle IAM utilisé dans les flux de travail GitHub Actions. Accordez uniquement les autorisations nécessaires pour effectuer les actions dans vos flux de travail GitHub Actions.
  - Surveillez l'activité du rôle IAM utilisé dans les flux de travail GitHub Actions.
  - Effectuez régulièrement une rotation des informations d'identification à long terme que vous utilisez.

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises

Configurez les AWS informations d'identification.	Pour exporter les variables qui définissent la pile Compte AWS et Région AWS où vous la déployez, exécutez les commandes suivantes :
	`export CDK_DEFAULT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAULT_REGION=<AWS Region>`
	Les AWS informations d'identification AWS CDK sont fournies par le biais de variables d'environnement.
		AWS DevOps, DevOps ingénieur

Pour cloner le référentiel.	Pour cloner le dépôt sur votre machine locale, exécutez la commande suivante : `git clone https://github.com/aws-samples/amazon-codeguru-suite-cdk-python.git`	AWS DevOps, DevOps ingénieur
Installez le kit d'outils CDK.	Pour confirmer que le kit d'outils CDK est installé et pour vérifier la version, exécutez la commande suivante :	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	`cdk --version`
	
	Si la version du CDK Toolkit est antérieure à 2.27.0, entrez la commande suivante pour la mettre à jour vers la version 2.27.0 :
	
	`npm install -g aws-cdk@2.27.0`
	
	Si le kit d'outils CDK n'est pas installé, exécutez la commande suivante pour l'installer :
	
	`npm install -g aws-cdk@2.27.0 --force`	

Installez les dépendances obligatoires.	Pour installer les dépendances de projet requises, exécutez la commande suivante :
	
	`python -m pip install --upgrade pip`
	`pip install -r requirements.txt`
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

Démarrez l'environnement CDK.	Pour démarrer un environnement AWS CDK, exécutez les commandes suivantes :
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Une fois que vous avez réussi à démarrer l'environnement, le résultat suivant doit s'afficher :
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
		AWS DevOps, DevOps ingénieur

Déployez l'application CDK

Tâche	Description	Compétences requises
Synthétisez l' AWS CDK application.	Pour synthétiser une AWS CDK application, exécutez la commande suivante : `cdk synth` Pour plus d'informations sur cette commande, consultez cdk synthesize dans la AWS CDK documentation.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Déployez les ressources.	Pour déployer les ressources, exécutez la commande suivante : `cdk deploy --require-approval never` **Note** L'`--require-approval never`indicateur signifie que le CDK approuvera et exécutera automatiquement toutes les modifications. Cela inclut les modifications que le CDK signalerait normalement comme nécessitant une révision manuelle (telles que les modifications de la politique IAM ou la suppression de ressources). Assurez-vous que votre code CDK et votre pipeline CI/CD sont bien testés et sécurisés avant d'utiliser l'`--require-approval never`indicateur dans	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	les environnements de production.	

Créez des GitHub secrets et un jeton d'accès personnel

Tâche	Description	Compétences requises
Créez les secrets requis dans GitHub.	Pour permettre aux flux de travail GitHub Actions d'accéder aux AWS ressources en toute sécurité sans exposer d'informations sensibles dans le code de votre référentiel, créez des secrets. Pour créer les secrets dans GitHub for`ROLE_TO_ASSUME` , et `CodeGuruReviewArtifactBucketName` `AWS_ACCOUNT_ID` , suivez les instructions de la section Création de secrets pour un référentiel dans la documentation GitHub Actions. Vous trouverez ci-dessous des informations supplémentaires sur les variables : • `AWS_ACCOUNT_ID` — L' Compte AWS ID où le pipeline est exécuté. • `CodeGuruReviewArtifactBucketName` —	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	Le nom du compartiment S3 dans lequel les artefacts CodeGuru Reviewer sont stockés. Ce modèle utilise le nom du compartiment `codeguru-reviewer-build-artifacts-<ACCOUNT_ID>-<REGION>` . • `AWS_REGION` — L' Région AWS endroit où se trouvent les ressources. • `ROLE_TO_ASSUME` — Nom du rôle IAM assumé par le pipeline. Ce modèle utilise le nom du rôle `githubActionsDeployRole` .	

Tâche	Description	Compétences requises
Créez un jeton d'accès GitHub personnel.	Pour configurer un moyen sécurisé d'authentification et d'interaction avec vos flux de travail GitHub Actions GitHub, procédez comme suit : 1. Pour créer un jeton d'accès GitHub personnel doté d'un accès en lecture et en écriture à votre référentiel, suivez les instructions de la section Gestion de vos jetons d'accès personnels dans la GitHub documentation. 2. Pour enregistrer ce jeton en tant que secret de référentiel pour GitHub Actions, suivez les instructions de la section Création de secrets pour un référentiel dans la documentation GitHub Actions.	AWS DevOps, DevOps ingénieur

Nettoyage

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour nettoyer votre application AWS CDK Python, exécutez la commande suivante : `cdk destroy --all`	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Afficher le lien vers les résultats du tableau de bord.	Il n'existe aucun moyen d'imprimer les résultats pendant le pipeline CI/CD. Ce modèle utilise plutôt GitHub les actions comme méthode alternative pour gérer et afficher les résultats.

Ressources connexes

AWS resources

- AWS Kit de développement Cloud
- CodeGuru Documentation Amazon
- Amazon S3
- AWS Identity and Access Management
- Amazon Simple Queue Service
- Qu'est-ce que c'est AWS Lambda ?

GitHub documentation

- Configuration d'OpenID Connect dans Amazon Web Services
- GitHub Actions
- Réutilisation des flux de travail
- Déclenchement d'un workflow

Automatisez l'évaluation des ressources AWS

Créée par Naveen Suthar (AWS), Arun Bagal (AWS), Manish Garg (AWS) et Sandeep Gawande (AWS)

Récapitulatif

Ce modèle décrit une approche automatisée pour configurer les fonctionnalités d'évaluation des ressources à l'aide de l'AWS Cloud Development Kit (AWS CDK). En utilisant ce modèle, les équipes opérationnelles collectent les détails de l'audit des ressources de manière automatisée et consultent les détails de toutes les ressources déployées dans un compte AWS sur un tableau de bord unique. Cela est utile dans les cas d'utilisation suivants :

- Identifier les outils d'infrastructure en tant que code (IaC) et isoler les ressources créées par différentes solutions IaC telles que HashiCorp Terraform, AWS, CloudFormation AWS CDK et AWS Command Line Interface (AWS CLI)
- Récupération des informations relatives à l'audit des ressources

Cette solution aidera également l'équipe de direction à obtenir des informations sur les ressources et les activités d'un compte AWS à partir d'un tableau de bord unique.

> **Note**
>
> Amazon QuickSight est un service payant. Avant de l'exécuter pour analyser les données et créer un tableau de bord, consultez les QuickSight tarifs Amazon.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Rôles et autorisations AWS Identity and Access Management (IAM) avec accès aux ressources de provisionnement
- Un QuickSight compte Amazon créé avec accès à Amazon Simple Storage Service (Amazon S3) et Amazon Athena

- AWS CDK version 2.55.1 ou ultérieure installée
- Python version 3.9 ou ultérieure installée

Limites

- Cette solution est déployée sur un seul compte AWS.
- La solution ne suivra pas les événements survenus avant son déploiement, sauf si AWS CloudTrail a déjà été configuré et stocké des données dans un compartiment S3.

Versions du produit

- AWS CDK version 2.55.1 ou ultérieure
- Python version 3.9 ou ultérieure

Architecture

Pile technologique cible

- Amazon Athena
- AWS CloudTrail
- AWS Glue
- AWS Lambda
- Amazon QuickSight
- Amazon S3

Architecture cible

Le code AWS CDK déploiera toutes les ressources nécessaires pour configurer les fonctionnalités d'évaluation des ressources dans un compte AWS. Le schéma suivant montre le processus d'envoi de CloudTrail journaux vers AWS Glue, Amazon Athena et. QuickSight

1. CloudTrail envoie les journaux vers un compartiment S3 à des fins de stockage.
2. Une notification d'événement invoque une fonction Lambda qui traite les journaux et génère des données filtrées.

3. Les données filtrées sont stockées dans un autre compartiment S3.
4. Un robot d'exploration AWS Glue est configuré sur les données filtrées qui se trouvent dans le compartiment S3 afin de créer un schéma dans la table du catalogue de données AWS Glue.
5. Les données filtrées sont prêtes à être consultées par Amazon Athena.
6. Les données demandées sont accessibles à des QuickSight fins de visualisation.

Automatisation et mise à l'échelle

- Cette solution peut être étendue d'un compte AWS à plusieurs comptes AWS s'il existe une CloudTrail piste à l'échelle de l'organisation dans AWS Organizations. En déployant CloudTrail au niveau de l'organisation, vous pouvez également utiliser cette solution pour récupérer les détails de l'audit des ressources pour toutes les ressources requises.
- Ce modèle utilise les ressources sans serveur AWS pour déployer la solution.

Outils

Services AWS

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur les comptes AWS et les régions AWS.
- AWS vous CloudTrail aide à auditer la gouvernance, la conformité et le risque opérationnel de votre compte AWS.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données. Ce modèle utilise un robot d'exploration AWS Glue et une table du catalogue de données AWS Glue.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à approvisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub infrastructure-assessment-iac-automationréférentiel.

Le référentiel de code contient les fichiers et dossiers suivants :

- `lib`dossier — Le CDK AWS construit des fichiers Python utilisés pour créer des ressources AWS
- `src/lambda_code`— Le code Python exécuté dans la fonction Lambda
- `requirements.txt`— La liste de toutes les dépendances Python qui doivent être installées
- `cdk.json`— Le fichier d'entrée fournissant les valeurs requises pour faire tourner les ressources

Bonnes pratiques

Configurez la surveillance et les alertes pour la fonction Lambda. Pour plus d'informations, consultez la section Surveillance et résolution des problèmes des fonctions Lambda. Pour connaître les meilleures pratiques générales relatives à l'utilisation des fonctions Lambda, consultez la documentation AWS.

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises
Clonez le dépôt sur votre machine locale.	Pour cloner le référentiel, exécutez la commande `git clone https://github.com/aws-samples/infrastructure-assessment-iac-automation.git .`	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

Configurez l'environnement virtuel Python et installez les dépendances requises.	Pour configurer l'environnement virtuel Python, exécutez les commandes suivantes.
	`cd infrastructure-assessment-iac-automation`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	Pour configurer les dépendances requises, exécutez la commande`pip install -r requirements.txt .`
		AWS DevOps, DevOps ingénieur

Configurez l'environnement AWS CDK et synthétisez le code AWS CDK.	1. Pour configurer l'environnement AWS CDK dans votre compte AWS, exécutez la commande`cdk bootstrap aws://ACCOUNT-NUMBER/REGION .` 2. Pour convertir le code en configuration de CloudFormation pile AWS, exécutez la commande`cdk synth`.	AWS DevOps, DevOps ingénieur

Configurer les informations d'identification AWS sur votre machine locale

Tâche	Description	Compétences requises
Exportez des variables pour le compte et la région où la pile sera déployée.	Pour fournir des informations d'identification AWS pour AWS CDK à l'aide de variables d'environnement, exécutez les commandes suivantes. `export CDK_DEFAU LT_ACCOUNT=<12 Digit AWS Account Number> export CDK_DEFAU LT_REGION=<region>`	AWS DevOps, DevOps ingénieur
Configurez le profil de la CLI AWS.	Pour configurer le profil de la CLI AWS pour le compte, suivez les instructions de la documentation AWS.	AWS DevOps, DevOps ingénieur

Configuration et déploiement de l'outil d'évaluation des ressources

Tâche	Description	Compétences requises
Déployez des ressources dans le compte.	Pour déployer des ressource s dans le compte AWS à l'aide d'AWS CDK, procédez comme suit : 1. À la racine du référentiel cloné, dans le `cdk.json` fichier, entrez les paramètre s suivants : • `s3_context` • `ct_context`	AWS DevOps

Tâche	Description	Compétences requises
	• `kms_context` • `lambda_context` • `glue_context` • `qs_context` Ces valeurs définissent les configurations et la nomenclature des ressources. Les valeurs par défaut sont définies et peuvent être modifiées si nécessaire. **Note** Pour éviter une erreur indiquant que le compartiment S3 existe déjà, assurez-vous de fournir des noms uniques pour `s3_context` les `output` sections `ct` et. 2. Pour déployer des ressources, exécutez la commande`cdk deploy`. La `cdk deploy` commande crée une CloudTrail ressource pour consigner les événements et enregistrer le fichier	

Tâche	Description	Compétences requises
	journal dans le compartiment S3 d'entrée. Les fichiers journaux du parcours seront traités par la fonction Lambda. Les résultats filtrés sont stockés dans le compartiment S3 de sortie et sont prêts à être utilisés par Amazon Athena et Amazon. QuickSight	

Tâche	Description	Compétences requises
Exécutez le robot d'exploration AWS Glue et créez la table du catalogue de données.	Un robot d'exploration AWS Glue est utilisé pour maintenir le schéma de données dynamique. La solution crée et met à jour des partitions dans la table du catalogue de données AWS Glue en exécutant régulièrement le robot d'exploration, comme défini par le planificateur de robots d'exploration AWS Glue. Une fois les données disponibles dans le compartiment S3 de sortie, procédez comme suit pour exécuter le robot d'exploration AWS Glue et créer le schéma de table du catalogue de données à des fins de test : 1. Connectez-vous à l'AWS Management Console et accédez à la console AWS Glue. 2. Dans le volet de navigation, sous Catalogue de données, sélectionnez Crawlers. 3. Sélectionnez le `iac-tool-qa-resource-iac-json-crawler` crawler. 4. Lancez le crawler. 5. Une fois le robot d'exploration exécuté avec succès, il	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	crée une table du catalogue de données AWS Glue. AWS QuickSight utilisera le tableau pour visualiser les données. **Note** Le code AWS CDK configure le robot d'exploration AWS Glue pour qu'il s'exécute à un moment précis, mais vous pouvez également l'exécuter à la demande.	
Déployez la QuickSight construction.	1. Pour déployer la QuickSight construction, décommentez le code entre `#QuickSight setup - start` et `#QuickSight setup – ends` dans`resource_iac_tool_stack.py` . 2. Après avoir décommenté, exécutez la `cdk deploy` commande pour créer `QuickSight DataSource` et `QuickSight DataSet` dans le QuickSight compte.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Créez le QuickSight tableau de bord.	Pour créer l'exemple de QuickSight tableau de bord et d'analyse, procédez comme suit : 1. Accédez à la QuickSigh t console et sélection nez la région AWS dans laquelle les ressources sont déployées. 2. Dans le volet de navigatio n, choisissez Datasets et vérifiez qu'un ensemble de données nommé `ct-operations-iac-ds` a été créé dans le jeu de QuickSight données Amazon. Si vous ne voyez pas le jeu de données, redéployez la QuickSight construction. 3. Sélectionnez le `ct-operations-iac-ds` jeu de données, puis choisissez UTILISER DANS L'ANALYSE. 4. Sélectionnez la feuille par défaut. 5. Sélectionnez les colonnes correspondantes dans la liste des champs sur le côté gauche.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	6. Après avoir sélectionné les colonnes requises, sélectionnez le type visuel approprié pour afficher les données. Pour plus d'informations, consultez Démarrage d'une analyse dans Amazon QuickSight et Types visuels dans Amazon QuickSight.	

Nettoyez toutes les ressources AWS de la solution

Tâche	Description	Compétences requises
Supprimez les ressources AWS.	1. Pour supprimer les ressources AWS déployées par la solution, exécutez la commande`cdk destroy`. 2. Supprimez tous les objets des deux compartim ents S3, puis retirez les compartiments. Pour plus d'informations, consultez la section Suppression d'un bucket.	AWS DevOps, DevOps ingénieur

Configurez des fonctionnalités supplémentaires en plus de l'automatisation de l'outil d'évaluation des ressources AWS

Tâche	Description	Compétences requises
Surveillez et nettoyez les ressources créées manuellement.	(Facultatif) Si votre organisation a des exigences de conformité pour créer des ressources à l'aide des outils IaC, vous pouvez garantir la conformité en utilisant l'automatisation des outils d'évaluation des ressources AWS pour récupérer les ressources provisionnées manuellement. Vous pouvez également utiliser l'outil pour importer les ressources dans un outil IaC ou pour les recréer. Pour surveiller les ressources provisionnées manuellement, effectuez les tâches de haut niveau suivantes : 1. Déployez l'automatisation de l'outil d'évaluation des ressources AWS. 2. Configurez une fonction Lambda pour interroger quotidiennement les tables Athena, trouver les données pertinentes sur les ressources provisionnées manuellement et les exporter vers un fichier de	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	valeurs séparées par des virgules (CSV). 3. Une fois la fonction Lambda exécutée, une notification contenant les données requises peut être envoyée aux parties prenantes concernées. 4. Pour une conservation plus longue, le fichier .csv peut être stocké dans le compartiment S3. 5. Sur la base des informati ons contenues dans le fichier .csv, supprimez les ressources créées manuellement ou importez-les dans une solution iAc existante.	

Résolution des problèmes

Problème	Solution
AWS CDK renvoie des erreurs.	Pour obtenir de l'aide concernant les problèmes liés au CDK AWS, consultez la section Résolution des problèmes courants liés au CDK AWS.

Ressources connexes

- Création de fonctions Lambda avec Python
- Commencez avec AWS CDK

- Utilisation d'AWS CDK en Python
- Création d'un CloudTrail journal
- Commencez avec Amazon QuickSight

Informations supplémentaires

Comptes multiples

Pour configurer les informations d'identification de l'interface de ligne de commande AWS pour plusieurs comptes, utilisez les profils AWS. Pour plus d'informations, consultez la section Configurer plusieurs profils dans Configuration de l'interface de ligne de commande AWS.

Commandes AWS CDK

Lorsque vous travaillez avec AWS CDK, gardez à l'esprit les commandes utiles suivantes :

- Répertorie toutes les piles de l'application

```
cdk ls
```

- Émet le modèle AWS synthétisé CloudFormation

```
cdk synth
```

- Déploie la pile sur votre compte AWS et votre région par défaut

```
cdk deploy
```

- Compare la pile déployée avec l'état actuel

```
cdk diff
```

- Ouvre la documentation du kit AWS CDK

```
cdk docs
```

Installez automatiquement les systèmes SAP à l'aide d'outils open source

Créée par Guilherme Sesterheim (AWS)

Récapitulatif

Ce modèle montre comment automatiser l'installation des systèmes SAP en utilisant des outils open source pour créer les ressources suivantes :

- Une base de données SAP S/4HANA 1909
- Une instance des services centraux SAP ABAP (ASCS)
- Une instance du serveur d'applications principal (PAS) SAP

HashiCorp Terraform crée l'infrastructure du système SAP et Ansible configure le système d'exploitation (OS) et installe les applications SAP. Jenkins exécute l'installation.

Cette configuration transforme l'installation des systèmes SAP en un processus reproductible, ce qui peut contribuer à améliorer l'efficacité et la qualité du déploiement.

> **Note**
>
> L'exemple de code fourni dans ce modèle fonctionne à la fois pour les systèmes à haute disponibilité (HA) et pour les systèmes non HA.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un bucket Amazon Simple Storage Service (Amazon S3) contenant tous vos fichiers multimédia SAP
- Un responsable d'AWS Identity and Access Management (IAM) doté d'une clé d'accès et d'une clé secrète et disposant des autorisations suivantes :
  - Autorisations en lecture seule : Amazon Route 53, AWS Key Management Service (AWS KMS)
  - Autorisations de lecture et d'écriture : Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB

- Une zone hébergée privée sur la Route 53
- Un abonnement à Red Hat Enterprise Linux pour SAP avec HA et Update Services 8.2 Amazon Machine Image (AMI) sur Amazon Marketplace
- Une clé gérée par le client AWS KMS
- Une paire de clés Secure Shell (SSH)
- Un groupe EC2 de sécurité Amazon qui autorise la connexion SSH sur le port 22 à partir du nom d'hôte sur lequel vous installez Jenkins (le nom d'hôte est probablement localhost)
- Vagrant by HashiCorp installé et configuré
- VirtualBoxinstallé et configuré par Oracle
- Connaissance de Git, Terraform, Ansible et Jenkins

Limites

- Seul SAP S/4HANA 1909 est entièrement testé pour ce scénario spécifique. L'exemple de code Ansible de ce modèle doit être modifié si vous utilisez une autre version de SAP HANA.
- L'exemple de procédure décrit dans ce modèle fonctionne pour les systèmes d'exploitation Mac OS et Linux. Certaines commandes ne peuvent être exécutées que sur des terminaux UNIX. Cependant, vous pouvez obtenir un résultat similaire en utilisant des commandes différentes et un système d'exploitation Windows.

Versions du produit

- SPA S/4HANA 1909
- Red Hat Enterprise Linux (RHEL) 8.2 ou versions supérieures

Architecture

Le schéma suivant montre un exemple de flux de travail qui utilise des outils open source pour automatiser l'installation des systèmes SAP dans un compte AWS :

Le schéma suivant illustre le flux de travail suivant :

1. Jenkins orchestre l'installation du système SAP en exécutant le code Terraform et Ansible.
2. Le code Terraform construit l'infrastructure du système SAP.

3. Le code Ansible configure le système d'exploitation et installe les applications SAP.
4. Une base de données SAP S/4HANA 1909, une instance ASCS et une instance PAS incluant tous les prérequis définis sont installées sur une instance Amazon. EC2

> **Note**
>
> L'exemple de configuration de ce modèle crée automatiquement un compartiment Amazon S3 dans votre compte AWS pour stocker le fichier d'état Terraform.

Pile technologique

- Terraform
- Ansible
- Jenkins
- Une base de données SAP S/4HANA 1909
- Une instance SAP ASCS
- Une instance SAP PAS
- Amazon EC2

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les faire rapidement évoluer vers le haut ou vers le bas.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Autres outils

- HashiCorp Terraform est une application d'interface en ligne de commande qui vous aide à utiliser du code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- Ansible est un outil open source de configuration sous forme de code (CAc) qui permet d'automatiser les applications, les configurations et l'infrastructure informatique.
- Jenkins est un serveur d'automatisation open source qui permet aux développeurs de créer, de tester et de déployer leurs logiciels.

Code

Le code de ce modèle est disponible dans le dépôt GitHub aws-install-sap-with-jenkins-ansible.

Épopées

Configuration des prérequis

Tâche	Description	Compétences requises
Ajoutez vos fichiers multimédia SAP à un compartiment Amazon S3.	Créez un compartiment Amazon S3 contenant tous vos fichiers multimédia SAP. **⚠ Important** Assurez-vous de suivre la hiérarchie des dossiers de l'AWS Launch Wizard pour S/4HANA dans la documentation de Launch Wizard.	Administrateur du cloud
Installez VirtualBox.	Installation et configuration VirtualBoxpar Oracle.	DevOps ingénieur

Tâche	Description	Compétences requises
Installez Vagrant.	Installez et configurez Vagrant par HashiCorp.	DevOps ingénieur

Tâche	Description	Compétences requises
Configurez votre compte AWS.	1. Vérifiez que vous disposez d'un principal IAM doté d'une clé d'accès et d'une clé secrète, et que vous disposez des autorisations suivantes : • Autorisations en lecture seule : Amazon Route 53, AWS Key Management Service (AWS KMS) • Autorisations de lecture et d'écriture : Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic File System (Amazon EFS), IAM, Amazon CloudWatch, Amazon DynamoDB 2. Enregistrez la clé d'accès et la clé secrète du principal IAM pour référence ultérieure. 3. Créez une zone hébergée privée Route 53, si vous n'en avez pas déjà une. Enregistrez le nom de la zone (par exemple, sapteam.net) pour référence ultérieure. 4. Abonnez-vous à l'AMI Red Hat Enterprise Linux pour SAP avec HA et Update Services 8.2 sur	AWS général

Tâche	Description	Compétences requises
	Amazon Marketplace. Enregistrez l'ID AMI (par exemple, ami-0000000) pour référence ultérieure. 5. Créez une clé gérée par le client AWS KMS. Enregistrez le nom de ressource Amazon (ARN) de la clé KMS pour référence ultérieure. **Note** Voici un exemple d'ARN de clé géré par le client AWS KMS : arn:aws:kms:us-east- 1:123412341234:key/uuid 6. Créez une paire de clés SSH. Enregistrez le nom de la paire de clés et le fichier .pem pour référence ultérieure. 7. Créez un groupe EC2 de sécurité Amazon qui autorise la connexion SSH sur le port 22 à partir du nom d'hôte sur lequel vous installez Jenkins. Enregistrez l'ID du groupe de sécurité pour référence ultérieure.	

Tâche	Description	Compétences requises
	Note Le nom d'hôte est probablement localhost.	

Créez et exécutez votre installation SAP

Tâche	Description	Compétences requises
Clonez le référentiel de code à partir de GitHub.	Clonez le dépôt aws-install-sap-with-jenkins-ansible sur. GitHub	DevOps ingénieur
Démarrez le service Jenkins.	Ouvrez le terminal Linux. Accédez ensuite au dossier local qui contient le dossier du référentiel de code cloné et exécutez la commande suivante : `sudo vagrant up` **Note** Le démarrage de Jenkins prend environ 20 minutes. La commande renvoie un message « Service is up and running » en cas de succès.	DevOps ingénieur

Tâche	Description	Compétences requises
Ouvrez Jenkins dans un navigateur Web et connectez-vous.	1. Dans un navigateur Web, saisissez http://localhost:5555. Jenkins ouvre. 2. Connectez-vous à Jenkins en utilisant admin pour le nom d'utilisateur et my_secret_pass_from_vault pour le mot de passe.	DevOps ingénieur

Tâche	Description	Compétences requises
Configurez les paramètres d'installation de votre système SAP.	1. Dans Jenkins, choisissez Manage Jenkins. Choisissez ensuite Gérer les informations d'identification. La liste des variables d'identification que vous pouvez configurer apparaît. 2. Configurez toutes les variables d'identification suivantes : • Pour AWS_ACCOUNT_CREDENTIALS, entrez l'ID de clé d'accès et l'ID de clé d'accès secrète de votre principal IAM. • Pour AMI_ID, entrez l'ID AMI de Red Hat Enterprise Linux pour SAP avec HA et de l'AMI Update Services 8.2. • Pour KMS_KEY_ARN, entrez l'ARN de votre clé gérée par le client AWS KMS. • Pour SSH_KEYPAIR_NAME, entrez le nom de votre paire de clés SSH, sans saisir le type de fichier .pem. • Pour SSH_KEYPAIR_FILE, entrez le nom complet du fichier .pem de votre	Administrateur système AWS, DevOps ingénieur

Tâche	Description	Compétences requises
	paire de clés (par exemple, mykeypair.pem). Assurez-vous de télécharger également le fichier .pem des paires de clés sur Jenkins. • Pour S3_ROOT_FOLDER_INSTALL_FILES, entrez le nom du compartiment Amazon S3 et du dossier, le cas échéant (par exemple, s3 :///S4H1909) qui contient vos fichiers multimédia SAP. my-media-bucket • Pour PRIVATE_DNS_ZONE_NAME, entrez le nom de votre zone hébergée privée Route 53 (par exemple, myprivate companyurl.net). • Pour VPC_ID, entrez l'ID VPC (par exemple, vpc-12345) du VPC Amazon dans lequel vous créez les ressources SAP. • Pour SUBNET_IDS, entrez deux sous-réseaux publics IDs si vous travaillez dans un environnement de test (pour les futures fonctionnalités HA). Si vous travaillez dans un environnement de production, il est	

Tâche	Description	Compétences requises
	recommandé d'utiliser deux sous-réseaux privés avec un hôte bastion. • Pour SECURITY_GROUP_ID, entrez l'ID du groupe de EC2 sécurité Amazon qui autorise la connexion SSH sur le port 22 à partir du nom d'hôte sur lequel vous avez installé Jenkins. **Note** Vous pouvez configurer les autres paramètres non obligatoires selon vos besoins, en fonction de votre cas d'utilisation. Par exemple, vous pouvez modifier l'ID système SAP (SID) des instances, le mot de passe par défaut, les noms et les balises de votre système SAP. Toutes les variables requises ont (Obligatoire) au début de leur nom.	

Tâche	Description	Compétences requises
Lancez l'installation de votre système SAP.	1. Dans Jenkins, choisissez Jenkins Home. Choisissez ensuite les instances SAP Hana+ASCS+PAS 3. 2. Choisissez Spin up et installez. Choisissez ensuite Main. 3. Choisissez Construire maintenant. Pour plus d'informations sur les étapes du pipeline, consultez la section Comprendre les étapes du pipeline de la section Automatisation de l'installation de SAP avec des outils open source sur le blog AWS. **Note** En cas d'erreur, déplacez votre curseur sur la case d'erreur rouge qui apparaît et choisissez Logs. Les journaux de l'étape du pipeline qui a donné lieu à une erreur apparaissent. La plupart des erreurs sont dues	DevOps ingénieur, administrateur système AWS

Tâche	Description	Compétences requises
	à des réglages de paramètres incorrects.	

Ressources connexes

- DevOps pour SAP — Installation de SAP : de 2 mois à 2 heures (vidéothèque DevOps Enterprise Summit)

Automatisez le déploiement du portefeuille et des produits AWS Service Catalog à l'aide d'AWS CDK

Créée par Sandeep Gawande (AWS), RAJNEESH TYAGI (AWS) et Viyoma Sachdeva (AWS)

Récapitulatif

AWS Service Catalog vous permet de gérer de manière centralisée les catalogues de services ou de produits informatiques dont l'utilisation est approuvée dans l'environnement AWS de votre organisation. Un ensemble de produits est appelé portefeuille, et un portefeuille contient également des informations de configuration. Avec AWS Service Catalog, vous pouvez créer un portefeuille personnalisé pour chaque type d'utilisateur de votre organisation, puis accorder l'accès au portefeuille approprié. Ces utilisateurs peuvent ensuite déployer rapidement tous les produits dont ils ont besoin au sein du portefeuille.

Si vous disposez d'une infrastructure réseau complexe, telle que des architectures multirégions et multicomptes, il est recommandé de créer et de gérer les portefeuilles Service Catalog dans un seul compte central. Ce modèle décrit comment utiliser AWS Cloud Development Kit (AWS CDK) pour automatiser la création de portefeuilles Service Catalog dans un compte central, autoriser les utilisateurs finaux à y accéder, puis, éventuellement, fournir des produits sur un ou plusieurs comptes AWS cibles. Cette ready-to-use solution crée les portefeuilles Service Catalog dans le compte source. Il fournit également, en option, des produits dans des comptes cibles à l'aide d'AWS CloudFormation Stacks et vous aide à configurer TagOptions les produits :

- AWS CloudFormation StackSets — Vous pouvez les utiliser StackSets pour lancer des produits Service Catalog dans plusieurs régions et comptes AWS. Dans cette solution, vous avez la possibilité de provisionner automatiquement les produits lorsque vous déployez cette solution. Pour plus d'informations, consultez Using AWS CloudFormation StackSets (documentation Service Catalog) et StackSets concepts (CloudFormation documentation).
- TagOption bibliothèque — Vous pouvez gérer les balises des produits approvisionnés à l'aide de la TagOption bibliothèque. A TagOptionest une paire clé-valeur gérée dans AWS Service Catalog. Il ne s'agit pas d'une balise AWS, mais elle sert de modèle pour créer une balise AWS basée sur le TagOption. Pour plus d'informations, consultez TagOption la bibliothèque (documentation Service Catalog).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif que vous souhaitez utiliser comme compte source pour administrer les portefeuilles Service Catalog.
- Si vous utilisez cette solution pour approvisionner des produits sur un ou plusieurs comptes cibles, le compte cible doit déjà exister et être actif.
- Autorisations AWS Identity and Access Management (IAM) pour accéder à AWS Service Catalog CloudFormation, AWS et AWS IAM.

Versions du produit

- Version 2.27.0 du kit de développement logiciel AWS

Architecture

Pile technologique cible

- Portefeuilles Service Catalog dans un compte AWS centralisé
- Produits Service Catalog déployés sur le compte cible

Architecture cible

1. Dans le compte portfolio (ou source), vous mettez à jour le fichier config.json avec le compte AWS, la région AWS, le rôle IAM, le portefeuille et les informations sur le produit correspondant à votre cas d'utilisation.
2. Vous déployez l'application AWS CDK.
3. L'application AWS CDK assume le rôle IAM de déploiement et crée les portefeuilles et les produits Service Catalog définis dans le fichier config.json.

   Si vous avez configuré StackSets pour déployer des produits dans un compte cible, le processus se poursuit. Si vous n'avez pas configuré StackSets pour approvisionner des produits, le processus est terminé.
4. L'application AWS CDK assume le rôle d'StackSet administrateur et déploie le CloudFormation stack set AWS que vous avez défini dans le fichier config.json.
5. Dans le compte cible, StackSets assume le rôle StackSet d'exécution et approvisionne les produits.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS CDK Toolkit est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre application AWS CDK.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Service Catalog vous permet de gérer de manière centralisée les catalogues de services informatiques approuvés pour AWS. Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.

Référentiel de code

Le code de ce modèle est disponible sur GitHub, dans le aws-cdk-servicecatalog-automationréférentiel. Le référentiel de code contient les fichiers et dossiers suivants :

- cdk-sevicecatalog-app— Ce dossier contient l'application AWS CDK pour cette solution.
- config — Ce dossier contient le fichier config.json et le CloudFormation modèle de déploiement des produits du portefeuille Service Catalog.
- config/config.json — Ce fichier contient toutes les informations de configuration. Vous mettez à jour ce fichier pour personnaliser cette solution en fonction de votre cas d'utilisation.
- config/templates — Ce dossier contient les CloudFormation modèles pour les produits Service Center.
- setup.sh — Ce script déploie la solution.
- uninstall.sh — Ce script supprime la pile et toutes les ressources AWS créées lors du déploiement de cette solution.

Pour utiliser l'exemple de code, suivez les instructions de la section Epics.

Bonnes pratiques

- Les rôles IAM utilisés pour déployer cette solution doivent respecter le principe du moindre privilège (documentation IAM).
- Respectez les meilleures pratiques pour développer des applications cloud avec AWS CDK (article de blog AWS).
- Respectez les CloudFormation meilleures pratiques d'AWS (CloudFormation documentation).

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises

Installez le kit d'outils AWS CDK.	Assurez-vous qu'AWS CDK Toolkit est installé. Entrez la commande suivante pour vérifier s'il est installé et vérifier la version.
	`cdk --version`
	Si AWS CDK Toolkit n'est pas installé, entrez la commande suivante pour l'installer.
	`npm install -g aws-cdk@2.27.0`
	Si la version d'AWS CDK Toolkit est antérieure à 2.27.0, entrez la commande suivante pour la mettre à jour vers la version 2.27.0.
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	`npm install -g aws-cdk@2.27.0 --force`	

Pour cloner le référentiel.	Entrez la commande suivante. Dans Cloner le référentiel, dans la section Informations supplémentaires, vous pouvez copier la commande complète contenant l'URL du référentiel. Cela clone le aws-cdk-servicecatalog-automationdépôt à partir de. GitHub
	`git clone <repository-URL>.git`
	Cela crée un `cd aws-cdk-servicecatalog-automation` dossier dans le répertoire cible. Entrez la commande suivante pour accéder à ce dossier.
	`cd aws-cdk-servicecatalog-automation`
		AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

Configurez les informations d'identification AWS.	Entrez les commandes suivantes : Ils exportent les variables suivantes, qui définissent le compte AWS et la région dans lesquels vous déployez la pile.
	`export CDK_DEFAU LT_ACCOUNT=<12-digit AWS account number>`
	`export CDK_DEFAU LT_REGION=<AWS Region>`
	Les informations d'identif ication AWS pour AWS CDK sont fournies par le biais de variables d'environnement.
		AWS DevOps, DevOps ingénieur

Configurez les autorisations pour les rôles IAM des utilisate urs finaux.	Si vous comptez utiliser des rôles IAM pour accorder l'accès au portefeuille et aux produits qu'il contient, les rôles doivent disposer d'autoris ations pour être assumés par le principal du service servicecatalog.amazonaws.co m. Pour savoir comment accorder ces autorisat ions, consultez Enabling trusted access with Service Catalog (documentation AWS Organizations).	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Configurez les rôles IAM requis par StackSets.	Si vous avez l'habitude StackSets de provisionner automatiquement des produits dans des comptes cibles, vous devez configurer les rôles IAM qui administrent et exécutent le stack set. 1. Dans le compte source, vérifiez s'il existe `AWSCloudFormationStackSetAdministrationRole` déjà. Dans les comptes cibles, vérifiez s'ils existent `AWSCloudFormationStackSetExecutionRole` déjà. Si ces rôles existent déjà, vous pouvez passer à l'épopée suivante. 2. Suivez les instructions de la section Autorisations autogérées de Grant (documentation IAM) pour créer le rôle d'administration du stack set dans le compte de portefeuille et créer le rôle d'exécution dans chaque compte cible.	AWS DevOps, DevOps ingénieur

Personnalisez et déployez la solution

Tâche	Description	Compétences requises
Créez les CloudFormation modèles.	Dans le `config/templates` dossier, créez des CloudFormation modèles pour tous les produits que vous souhaitez inclure dans vos portefeuilles. Pour plus d'informations, consultez la section Utilisation des CloudFormation modèles AWS (CloudFormation documentation).	Développeur d'applications, AWS DevOps, DevOps ingénieur
Personnalisez le fichier de configuration.	Dans le `config` dossier, ouvrez le fichier config.json et définissez les paramètres adaptés à votre cas d'utilisation. Les paramètres suivants sont obligatoires, sauf indication contraire : Dans `portfolios` cette section, définissez les paramètres suivants pour créer un ou plusieurs portefeuilles Service Catalog : • `portfolioName` — Le nom du portefeuille. • `providerName` — Le nom de la personne, de l'équipe ou de l'organisation qui gère le portefeuille.	Développeur d'applications, DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	• `description` — Une brève description du portefeuille. • `roles`— (Facultatif) Noms de tous les rôles IAM qui devraient avoir accès à ce portefeuille. Les utilisateurs dotés de ce rôle peuvent accéder aux produits de ce portefeuille. • `users`— (Facultatif) Noms de tous les utilisateurs IAM qui devraient avoir accès à ce portefeuille et à ses produits. • `groups`— (Facultatif) Noms de tous les groupes d'utilisateurs IAM qui devraient avoir accès à ce portefeuille et à ses produits. ⚠ Warning Les utilisateurs IAM disposent d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin	

Tâche	Description	Compétences requises
	pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires. ⚠ Important `roles`,`users`, et `groups` sont tous des paramètres facultatifs, mais si vous ne définissez aucun de ces paramètres, personne ne peut consulter le portefeuille de produits dans la console Service Catalog. Définissez au moins l'un de ces paramètres. Pour plus d'informations, consultez la section Accorder des autorisations aux utilisateurs finaux de Service Catalog (documentation Service Catalog). • (Facultatif) Dans la `tagOption` section, définissez TagOptions pour les produits :	

Tâche	Description	Compétences requises
	• `key`— Nom de la TagOption clé • `value`— Valeurs de chaîne autorisées pour TagOption Pour plus d'informations, consultez TagOption la bibliothèque (documentation Service Catalog). • Dans la **`products`**section, définissez les paramètres suivants pour les produits : • `portfolioName` — Le nom du portefeuille dans lequel vous souhaitez ajouter le produit. Vous ne pouvez spécifier qu'un seul portefeuille. • `productName` — Le nom du produit. • `owner`— Le propriétaire du produit. • `productVersionName` — Le nom de la version du produit sous forme de chaîne, par exemple`v1`. • `templatePath` — Le chemin du fichier pour le CloudFormation modèle du produit. • `deployWithStackSets` — (Facultatif) Spécifiez	

Tâche	Description	Compétences requises
	un ou plusieurs comptes et régions que vous souhaitez utiliser StackSets pour approvisionner automatiquement les produits des portefeuilles. Si vous utilisez cette option de déploiement, tous les paramètres suivants de cette section sont obligatoires : • `accounts`— Les comptes cibles. • `regions`— Les régions cibles. • `stackSetAdministrationRoleName` — Le nom du rôle IAM utilisé pour administrer la StackSets configuration. Ne modifiez pas cette valeur. Ce rôle doit porter ce nom exact. • `stackSetExecutionRoleName` — Le nom du rôle IAM dans le compte cible qui déploie les instances de stack. Ne modifiez pas cette valeur. Ce	

Tâche	Description	Compétences requises
	rôle doit porter ce nom exact. Pour un exemple de fichier de configuration terminé, voir Exemple de fichier de configuration dans la section Informations supplémentaires.	
Déployez la solution.	Entrez la commande suivante. Cela permet de déployer l'application AWS CDK et de provisionner les portefeuilles et les produits Service Catalog comme indiqué dans le fichier config.json. `sh +x setup.sh`	Développeur d'applications, DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
Vérifier le déploiement.	Vérifiez la réussite du déploiement en procédant comme suit : 1. Connectez-vous à l'AWS Management Console avec des informations d'identif ication qui peuvent accéder à un ou plusieurs des portefeuilles que vous avez définis dans le fichier de configuration. 2. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/. 3. Dans le volet de navigation, sous Provisioning, sélection nez Products. Vérifiez que la liste des produits que vous avez spécifiés pour le portefeuille s'affiche. 4. Suivez les instructions de la section Lancer un produit (documentation du Service Catalog) pour lancer l'un des produits disponibles. Vérifiez que les versions de produit et les balises disponibles correspondent aux valeurs que vous avez fournies dans le fichier de configuration.	AWS général

Tâche	Description	Compétences requises
	5. Si vous avez choisi de provisionner automatiquement les produits sur un ou plusieurs comptes cibles en utilisant StackSets, procédez comme suit : a. Connectez-vous avec des informations d'identification qui vous autorisent à consulter les produits fournis sur l'un des comptes cibles. b. Dans la console Service Catalog, dans le volet de navigation, sous Provisioning, choisissez Provisioned products. c. Vérifiez que les produits attendus apparaissent dans la liste.	

Tâche	Description	Compétences requises
(Facultatif) Mettez à jour les portefeuilles et les produits.	Si vous souhaitez utiliser cette solution pour mettre à jour les portefeuilles ou les produits ou pour fournir de nouveaux produits : 1. Apportez les modifications requises dans le fichier config.json. 2. Ajoutez ou modifiez les CloudFormation modèles nécessaires dans le `config/template` dossier. 3. Redéployez la solution. Par exemple, vous pouvez ajouter des portefeuilles supplémentaires ou allouer davantage de ressource s. L'application AWS CDK implémente uniquement les modifications. Si aucune modification n'est apportée aux portefeuilles ou aux produits précédemment déployés, le redéploiement ne les affectera pas.	Développeur d'applications, DevOps ingénieur, AWS général

Nettoyez la solution

Tâche	Description	Compétences requises
(Facultatif) Supprimez les ressources AWS déployées par cette solution.	Si vous souhaitez supprimer un produit approvisionné, suivez les instructions de la section Supprimer des produits approvisionnés (documentation Service Catalog). Si vous souhaitez supprimer toutes les ressources créées par cette solution, entrez la commande suivante. `sh uninstall.sh`	AWS DevOps, DevOps ingénieur, développeur d'applications

Ressources connexes

- Bibliothèque AWS Service Catalog Construct (référence d'API AWS)
- StackSets concepts (CloudFormation documentation)
- AWS Service Catalog (AWS marketing)
- Utilisation du Service Catalog avec le kit AWS CDK (atelier AWS)

Informations supplémentaires

Cloner le référentiel

Entrez la commande suivante pour cloner le référentiel GitHub.

```
git clone https://github.com/aws-samples/aws-cdk-servicecatalog-automation.git
```

Exemple de fichier de configuration

Voici un exemple de fichier config.json avec des exemples de valeurs.

```
{
    "portfolios": [
        {
            "displayName": "EC2 Product Portfolio",
            "providerName": "User1",
            "description": "Test1",
            "roles": [
                "<Names of IAM roles that can access the products>"
            ],
            "users": [
                "<Names of IAM users who can access the products>"
            ],
            "groups": [
                "<Names of IAM user groups that can access the products>"
            ]
        },
        {
            "displayName": "Autoscaling Product Portfolio",
            "providerName": "User2",
            "description": "Test2",
            "roles": [
                "<Name of IAM role>"
            ]
        }
    ],
    "tagOption": [
        {
            "key": "Group",
            "value": [
                "finance",
                "engineering",
                "marketing",
                "research"
            ]
        },
        {
            "key": "CostCenter",
            "value": [
                "01",
                "02",
                "03",
                "04"
```

```
            ]
        },
        {
            "key": "Environment",
            "value": [
                "dev",
                "prod",
                "stage"
            ]
        }
    ],
    "products": [
        {
            "portfolioName": "EC2 Product Profile",
            "productName": "Ec2",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template1.json"
        },
        {
            "portfolioName": "Autoscaling Product Profile",
            "productName": "autoscaling",
            "owner": "owner1",
            "productVersionName": "v1",
            "templatePath": "../../config/templates/template2.json",
            "deployWithStackSets": {
                "accounts": [
                    "012345678901",
                ],
                "regions": [
                    "us-west-2"
                ],
                "stackSetAdministrationRoleName":
 "AWSCloudFormationStackSetAdministrationRole",
                "stackSetExecutionRoleName": "AWSCloudFormationStackSetExecutionRole"
            }
        }
    ]
}
```

Automatisez les sauvegardes basées sur les événements depuis Amazon S3 CodeCommit à l'aide CodeBuild de and Events CloudWatch

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), vous pouvez utiliser AWS CodeCommit pour héberger des référentiels sécurisés basés sur Git. CodeCommit est un service de contrôle de source entièrement géré. Toutefois, si un CodeCommit dépôt est supprimé accidentellement, son contenu est également supprimé et ne peut pas être restauré.

Ce modèle décrit comment sauvegarder automatiquement un CodeCommit référentiel dans un compartiment Amazon Simple Storage Service (Amazon S3) après qu'une modification a été apportée au référentiel. Si le CodeCommit référentiel est supprimé ultérieurement, cette stratégie de sauvegarde vous propose une option point-in-time de restauration.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un CodeCommit référentiel existant, avec un accès utilisateur configuré en fonction de vos besoins. Pour plus d'informations, consultez la section Configuration d'AWS CodeCommit dans la CodeCommit documentation.
- Un compartiment S3 pour le téléchargement des CodeCommit sauvegardes.

Limites

- Ce modèle sauvegarde automatiquement tous vos CodeCommit référentiels. Si vous souhaitez sauvegarder des CodeCommit référentiels individuels, vous devez modifier la règle Amazon CloudWatch Events.

Architecture

Le schéma suivant illustre le flux de travail pour ce modèle.

Le flux de travail se compose des étapes suivantes :

1. Le code est transféré vers un CodeCommit dépôt.
2. Le CodeCommit référentiel informe CloudWatch Events d'une modification du référentiel (par exemple, une `git push` commande).
3. CloudWatch Events invoque AWS CodeBuild et lui envoie les informations du CodeCommit référentiel.
4. CodeBuild clone l'intégralité du CodeCommit dépôt et l'empaquette dans un fichier .zip.
5. CodeBuild télécharge le fichier .zip dans un compartiment S3.

Pile technologique

- CloudWatch Événements
- CodeBuild
- CodeCommit
- Amazon S3

Outils

- Amazon CloudWatch Events — CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS CodeBuild CodeBuild est un service d'intégration continue entièrement géré qui compile le code source, exécute des tests et produit des packages logiciels prêts à être déployés.
- AWS CodeCommit CodeCommit est un service de contrôle de source entièrement géré qui héberge des référentiels sécurisés basés sur Git.
- AWS Identity and Access Management (IAM) — IAM est un service Web qui vous permet de contrôler en toute sécurité l'accès aux ressources AWS.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.

Épopées

Création d'un CodeBuild projet

Tâche	Description	Compétences requises
Créez un rôle CodeBuild de service.	Connectez-vous à AWS Management Console et ouvrez la console IAM. Choisissez Rôles, puis sélectionnez Créer un rôle. Créez un rôle de service CodeBuild pour cloner le CodeCommit référentiel, télécharger des fichiers dans le compartiment S3 et envoyer des journaux à Amazon CloudWatch. Pour plus d'informations, consultez la section Créer un rôle de CodeBuild service dans la CodeBuild documentation.	Administrateur du cloud
Créez un CodeBuild projet.	Sur la CodeBuild console, choisissez Create CodeBuild project. Créez un CodeBuild projet en utilisant le `buildspec.yml` modèle de la section Informations supplémentaires. Pour obtenir de l'aide sur cette histoire, voir Créer un projet de construct ion dans la CodeBuild documentation.	Administrateur du cloud

Création et configuration de la règle CloudWatch Événements

Tâche	Description	Compétences requises
Créez un rôle IAM pour les CloudWatch événements.	Sur la console IAM, choisissez Rôles et créez un rôle IAM pour les CloudWatch événements. Pour plus d'informations à ce sujet, consultez la section Rôle IAM CloudWatch des événements dans la documentation IAM. **⚠ Important** Vous devez ajouter `codebuild:StartBuild` des autorisations au rôle IAM pour les CloudWatch événements.	Administrateur du cloud
Créez une règle d' CloudWatch événements.	1. Sur la CloudWatch console, choisissez Events, puis Rules. Choisissez Créer une règle, puis utilisez la règle CloudWatch Événements dans la section Informations supplémentaires. Cela crée une règle qui écoute les modifications d'événements (par exemple, `git push` ou `git commit` les commandes) dans vos CodeCommit référentiels.	Administrateur du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Créer une règle d' CloudWatch événements pour une CodeCommit source dans la CodePipeline documentation AWS. 2. Choisissez Cibles, sélectionnez Sujet, puis sélectionnez Configurer la saisie. Choisissez Transformateur d'entrée, puis utilisez le chemin d'entrée et le modèle d'entrée de la section Informations supplémentaires. Cela garantit que les détails de votre CodeCommit dépôt sont analysés et envoyés sous forme de variables d'environnement au CodeBuild projet. Pour plus d'informations, consultez le didacticiel sur le transformateur d'entrée dans la CloudWatch documentation. 3. Choisissez Configurer les détails, puis entrez le nom et la description de la règle. Choisissez Créer une règle.	

Tâche	Description	Compétences requises
	Important Cette règle CloudWatch relative aux événements décrit les modifications apportées à tous vos CodeCommit référentiels. Vous devez modifier la règle CloudWatch des événements si vous souhaitez sauvegarder des CodeCommit référentiels individuels ou utiliser des compartiments S3 distincts pour différentes sauvegardes de référentiels.	

Ressources connexes

Création d'un CodeBuild projet

- Création d'un rôle CodeBuild de service
- Création d'un CodeBuild projet
- Autorisations requises pour les commandes du client Git

Création et configuration d'une règle d' CloudWatch événements

- Création d'une règle d' CloudWatch événements pour une CodeCommit source
- Utilisez le transformateur d'entrée pour personnaliser ce qui est transmis à la cible de l'événement

- Création d'une règle d' CloudWatch événements qui démarre lors d'un événement
- Création d'un rôle IAM dans les CloudWatch événements

Informations supplémentaires

CodeBuild modèle buildspec.yml

```
version: 0.2
phases:
  install:
    commands:
      - pip install git-remote-codecommit
  build:
    commands:
       - env
       - git clone -b $REFERENCE_NAME codecommit::$REPO_REGION://$REPOSITORY_NAME
       - dt=$(date '+%d-%m-%Y-%H:%M:%S');
       - echo "$dt"
       - zip -yr $dt-$REPOSITORY_NAME-backup.zip ./
       - aws s3 cp $dt-$REPOSITORY_NAME-backup.zip s3:// #substitute a valid S3 Bucket
 Name here
```

CloudWatch Règle des événements

```
{
  "source": [
    "aws.codecommit"
  ],
  "detail-type": [
    "CodeCommit Repository State Change"
  ],
  "detail": {
    "event": [
      "referenceCreated",
      "referenceUpdated"
    ]
  }
}
```

Exemple de transformateur d'entrée pour la cible de la règle CloudWatch Events

Chemin d'entrée :

```
{"referenceType":"$.detail.referenceType","region":"$.region","repositoryName":"$.detail.reposi
```

Modèle de saisie (veuillez renseigner les valeurs appropriées) :

```
{
    "environmentVariablesOverride": [
        {
            "name": "REFERENCE_NAME",
            "value": ""
        },
        {
            "name": "REFERENCE_TYPE",
            "value": ""
        },
        {
            "name": "REPOSITORY_NAME",
            "value": ""
        },
        {
            "name": "REPO_REGION",
            "value": ""
        },
        {
            "name": "ACCOUNT_ID",
            "value": ""
        }
    ]
}
```

Automatisez la suppression des AWS CloudFormation piles et des ressources associées

Créée par SANDEEP SINGH (AWS) et James Jacob (AWS)

Récapitulatif

AWS CloudFormationest un service largement utilisé pour gérer l'infrastructure cloud en tant que code (iAc). Lorsque vous utilisez CloudFormation, vous gérez les ressources associées en tant qu'unité unique appelée pile. Pour créer, mettre à jour et supprimer un ensemble de ressources, vous créez, mettez à jour et supprimez des piles.

Parfois, vous n'avez plus besoin des ressources d'une CloudFormation pile. En fonction des ressources et de leurs configurations, il peut être compliqué de supprimer une pile et les ressources associées. Dans les systèmes de production réels, les suppressions échouent parfois ou prennent du temps en raison de conditions contradictoires ou de restrictions impossibles à annuler CloudFormation . Cela peut nécessiter une planification et une exécution minutieuses pour s'assurer que toutes les ressources sont correctement supprimées de manière efficace et cohérente.
Ce modèle décrit comment configurer une structure qui vous aide à gérer la suppression de CloudFormation piles impliquant les complexités suivantes :

- Ressources protégées contre la suppression : la protection contre la suppression peut être activée sur certaines ressources. Les tables Amazon DynamoDB et les compartiments Amazon Simple Storage Service (Amazon S3) en sont des exemples courants. La protection contre la suppression empêche la suppression automatique, telle que la suppression via CloudFormation. Si vous souhaitez supprimer ces ressources, vous devez annuler ou désactiver temporairement la protection contre la suppression manuellement ou par programmation. Vous devez examiner attentivement les implications de la suppression de ces ressources avant de continuer.
- Ressources soumises à des politiques de rétention : certaines ressources, telles que les clés AWS Key Management Service (AWS KMS) et les compartiments Amazon S3, peuvent être soumises à des politiques de rétention qui spécifient la durée pendant laquelle elles doivent être conservées après la demande de suppression. Vous devez tenir compte de ces politiques dans la stratégie de nettoyage afin de garantir la conformité aux politiques organisationnelles et aux exigences réglementaires.
- Suppression différée des fonctions Lambda associées à un VPC — La suppression d'une AWS Lambdafonction attachée à un cloud privé virtuel (VPC) peut prendre 5 à 40 minutes, selon les

multiples dépendances interconnectées impliquées dans le processus. Si vous détachez la fonction du VPC avant de supprimer la pile, vous pouvez réduire ce délai à moins d'une minute.

- Ressources non directement créées par CloudFormation : dans certaines conceptions d'applications, les ressources peuvent être créées en dehors de la CloudFormation pile d'origine, soit par l'application elle-même, soit par des ressources fournies via la pile. En voici deux exemples :
  - CloudFormation peut fournir une instance Amazon Elastic Compute Cloud (Amazon EC2) qui exécute un script de données utilisateur. Ce script peut ensuite créer un AWS Systems Managerparamètre pour stocker les données relatives à l'application. Ce paramètre n'est pas géré via CloudFormation.
  - CloudFormation peut fournir une fonction Lambda qui génère automatiquement un groupe Amazon CloudWatch Logs pour le stockage des journaux. Ce groupe de journaux n'est pas géré via CloudFormation.

  Même si ces ressources ne sont pas directement gérées par CloudFormation, elles ont souvent besoin d'être nettoyées lorsque la pile est supprimée. S'ils ne sont pas gérés, ils peuvent devenir orphelins et entraîner une consommation inutile de ressources.

Bien que ces glissières de sécurité puissent être complexes, elles sont intentionnelles et critiques. CloudFormation Permettre de contourner toutes les contraintes et de supprimer des ressources sans discernement pourrait avoir des conséquences néfastes et imprévues dans de nombreux scénarios. Cependant, en tant DevOps qu'ingénieur cloud responsable de la gestion de l'environnement, il peut parfois être nécessaire de contourner ces contraintes, en particulier dans les environnements de développement, de test ou de test.

Résultats commerciaux ciblés

En mettant en œuvre ce cadre, vous pouvez obtenir les avantages suivants :

- Gestion des coûts — Le nettoyage régulier et efficace des environnements temporaires, tels que les environnements de test end-to-end d'acceptation par les utilisateurs, permet d'éviter que les ressources ne s'épuisent plus que nécessaire. Cela permet de réduire considérablement les coûts.
- Sécurité — Le nettoyage automatique des ressources obsolètes ou inutilisées réduit la surface d'attaque et contribue à maintenir un AWS environnement sécurisé.
- Efficacité opérationnelle — Un nettoyage régulier et automatisé peut apporter les avantages opérationnels suivants :

- Les scripts automatisés qui suppriment les anciens groupes de journaux ou les compartiments Amazon S3 vides peuvent améliorer l'efficacité opérationnelle en préservant la propreté et la gestion de l'environnement.
- La suppression et la recréation rapides des piles permettent une itération rapide pour la conception et la mise en œuvre, ce qui peut conduire à une architecture plus robuste et résiliente.
- La suppression et la reconstruction régulières d'environnements peuvent vous aider à identifier et à résoudre les problèmes potentiels. Cela peut vous aider à vous assurer que l'infrastructure peut résister aux scénarios du monde réel.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Python version 3.6 ou ultérieure, installé
- AWS Command Line Interface (AWS CLI), installé et configuré

Limites

- Une convention de dénomination est utilisée pour identifier les ressources qui doivent être supprimées. L'exemple de code de ce modèle utilise un préfixe pour le nom de la ressource, mais vous pouvez définir votre propre convention de dénomination. Les ressources qui n'utilisent pas cette convention de dénomination ne seront pas identifiées ni supprimées ultérieurement.

Architecture

Le schéma suivant montre comment ce framework identifie la CloudFormation pile cible et les ressources supplémentaires qui y sont associées.

Le schéma suivant illustre le flux de travail suivant :

1. Rassemblez des ressources : le framework d'automatisation utilise une convention de dénomination pour renvoyer toutes les CloudFormation piles pertinentes, les référentiels Amazon Elastic Container Registry (Amazon ECR), les tables DynamoDB et les compartiments Amazon S3.

> **Note**
>
> Les fonctions de cette étape utilisent des paginateurs, une fonctionnalité de Boto3 qui résume le processus d'itération sur un ensemble de résultats d'API tronqué. Cela permet de s'assurer que toutes les ressources sont traitées. Pour optimiser davantage les performances, envisagez d'appliquer un filtrage côté serveur ou envisagez de l'utiliser JMESPath pour effectuer un filtrage côté client.

2. Prétraitement — Le cadre d'automatisation identifie et traite les contraintes de service qui doivent être contournées afin de CloudFormation permettre la suppression des ressources. Par exemple, il modifie le `DeletionProtectionEnabled` paramètre des tables DynamoDB en. `False` Dans l'interface de ligne de commande, pour chaque ressource, vous recevez un message vous demandant si vous souhaitez annuler la contrainte.
3. Supprimer la pile : le framework d'automatisation supprime la CloudFormation pile. Dans l'interface de ligne de commande, vous recevez un message vous demandant si vous souhaitez supprimer la pile.
4. Post-traitement — Le cadre d'automatisation supprime toutes les ressources associées qui n'ont pas été directement approvisionnées dans le CloudFormation cadre de la pile. Les paramètres de Systems Manager et les groupes de CloudWatch journaux sont des exemples de ces types de ressources. Des fonctions distinctes rassemblent ces ressources, les prétraitent, puis les suppriment. Dans l'interface de ligne de commande, pour chaque ressource, vous recevez un message vous demandant si vous souhaitez supprimer la ressource.

> **Note**
>
> Les fonctions de cette étape utilisent des paginateurs, une fonctionnalité de Boto3 qui résume le processus d'itération sur un ensemble de résultats d'API tronqué. Cela permet de s'assurer que toutes les ressources sont traitées. Pour optimiser davantage les performances, envisagez d'appliquer un filtrage côté serveur ou envisagez de l'utiliser JMESPath pour effectuer un filtrage côté client.

Automatisation et mise à l'échelle

Si votre CloudFormation pile inclut d'autres ressources qui ne sont pas incluses dans l'exemple de code, ou si la pile comporte une contrainte qui n'a pas été prise en compte dans ce modèle, vous

pouvez adapter le cadre d'automatisation à votre cas d'utilisation. Suivez la même méthodologie de collecte des ressources, de prétraitement, de suppression de la pile, puis de post-traitement.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- CloudFormation L'interface de ligne de commande (CFN-CLI) est un outil open source qui vous permet de développer et de tester AWS des extensions tierces, puis de les enregistrer pour les utiliser dans. CloudFormation
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

Autres outils

- Click est un outil Python qui permet de créer des interfaces de ligne de commande.
- Poetry est un outil de gestion des dépendances et d'empaquetage en Python.
- Pyenv est un outil qui vous aide à gérer et à passer d'une version à l'autre de Python.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub cloudformation-stack-cleanupréférentiel.

Bonnes pratiques

- Étiquetez les ressources pour les identifier facilement : mettez en œuvre une stratégie de balisage pour identifier les ressources créées pour différents environnements et objectifs. Les balises peuvent simplifier le processus de nettoyage en vous aidant à filtrer les ressources en fonction de leurs balises.
- Configurer les cycles de vie des ressources : définissez les cycles de vie des ressources afin de supprimer automatiquement les ressources après une certaine période. Cette pratique vous permet de vous assurer que les environnements temporaires ne deviennent pas des coûts permanents.

Épopées

Outils d'installation

Tâche	Description	Compétences requises
Pour cloner le référentiel.	1. Créez un dossier dans votre environnement virtuel. Nommez-le avec le nom de votre projet. 2. Ouvrez un terminal sur votre ordinateur local et accédez à ce dossier. 3. Entrez la commande suivante pour cloner le cloudformation-stack-cleanup référentiel dans le répertoire de votre projet : `git clone https://github.com/aws-samples/cloudformation-stack-cleanup.git`	DevOps ingénieur
Installez Poetry.	Suivez les instructions (documentation Poetry) pour installer Poetry dans l'environnement virtuel cible.	DevOps ingénieur
Installez les dépendances.	1. Entrez la commande suivante pour accéder au répertoire du projet : `cd cloudformation-stack-cleanup` 2. Entrez la commande suivante :	DevOps ingénieur

Tâche	Description	Compétences requises
	`poetry install` Cela installe toutes les dépendances requises, telles que Boto3, click et le code source de la CLI. CloudFormation	
(Facultatif) Installez Pyenv.	Suivez les instructions (GitHub) pour installer Pyenv.	DevOps ingénieur

(Facultatif) Personnalisez le cadre

Tâche	Description	Compétences requises
Créez des fonctions qui collectent, prétraitent et suppriment les ressources cibles.	1. Dans le référentiel cloné, entrez la commande suivante pour accéder au `cli` répertoire : `cd cfncli/cli` 2. Ouvrez le fichier cleanup_environment.py. 3. Créez une nouvelle fonction Python qui regroupe le type de ressource que vous souhaitez modifier. Pour un exemple, consultez la `gather_ddb_tables` fonction dans ce fichier. 4. Créez une nouvelle fonction Python qui remplace les contraintes de service pour	DevOps ingénieur, Python

Tâche	Description	Compétences requises
	la ressource cible. Pour un exemple, consultez la `remove_ddb_deletion_protection` fonction dans ce fichier. 5. Créez une nouvelle fonction Python qui collecte les ressources cibles non gérées. Pour un exemple, consultez la `gather_log_groups` fonction dans ce fichier. 6. Créez une nouvelle fonction Python qui supprime les ressources cibles non gérées. Pour un exemple, consultez la `delete_log_group` fonction dans ce fichier. 7. Enregistrez et fermez le fichier cleanup_enviornment.py.	

Création d'exemples de ressources

Tâche	Description	Compétences requises
Créez une CloudFormation pile.	1. Accédez au répertoire du projet . 2. Entrez la commande suivante pour créer une CloudFormation pile qui approvisionne une table	AWS DevOps

Tâche	Description	Compétences requises
	DynamoDB et un groupe de sécurité. Mettez à jour la valeur pour <VPCID> : `aws cloudformation create-stack \ --stack-name sampleforcleanup-Stack \ --template-body file://samples/sample-cfn-stack.yaml \ --parameters ParameterKey=VpcId,ParameterValue=<VPCID> \ --region us-east-1`	
Créez un paramètre Systems Manager.	Entrez la commande suivante pour créer un paramètre Systems Manager qui n'est pas provisionné via CloudFormation : `aws ssm put-parameter \ --name "/samplefor cleanup/database/password" \ --value "your_db_password" \ --type "SecureString" \ --description "Database password for my app" \ --tier "Standard" \ --region "us-east-1"`	AWS DevOps

Tâche	Description	Compétences requises
Créez un compartiment Amazon S3.	Entrez la commande suivante pour créer un compartiment Amazon S3 qui n'est pas provisionné via CloudFormation : `aws s3api create-bucket \ --bucket samplesorcleanup-unmanagedbucket-<UniqueIdentifier> \ --region us-east-1 \ --create-bucket-configuration LocationConstraint=us-east-1`	AWS DevOps

Supprimer les exemples de ressources

Tâche	Description	Compétences requises
Supprimez la CloudFormation pile.	1. Entrez la commande suivante pour supprimer la CloudFormation pile d'échantillons, le paramètre Systems Manager et le compartiment Amazon S3 que vous avez créés : `cfncli --region us-east-1 \ dev cleanup-env \ --prefix-list sampleforcleanup`	AWS DevOps

Tâche	Description	Compétences requises
	2. Lorsque vous y êtes invité, entrez Y pour continuer.	
Validez la suppression des ressources.	Dans le résultat, confirmez que tous les exemples de ressources ont été supprimés. Pour un exemple de sortie, consultez la section Ressources supplémentaires de ce modèle.	AWS DevOps

Ressources connexes

- Supprimer une pile (CloudFormation documentation)
- Résolution des problèmes CloudFormation (CloudFormation documentation)
- Permettre aux fonctions Lambda d'accéder aux ressources d'un Amazon VPC (documentation Lambda)
- Comment supprimer une AWS CloudFormation pile bloquée dans le statut DELETE_FAILED ? (Centre de AWS connaissances)

Informations supplémentaires

Voici un exemple de sortie de la `cfncli` commande :

```
cfncli --region aus-east-1  dev cleanup-env --prefix-list sampleforcleanup


https://sts.us-east-1.amazonaws.com
Cleaning up: ['sampleforcleanup'] in xxxxxxxxxx:us-east-1
Do you want to proceed? [Y/n]: Y
No S3 buckets
No ECR repositories
No Lambda functions in VPC
The following DynamoDB tables will have their deletion protection removed:
sampleforcleanup-MyDynamoDBTable
Do you want to proceed with removing deletion protection from these tables? [Y/n]: Y
```

```
Deletion protection disabled for DynamoDB table 'sampleforcleanup-MyDynamoDBTable'.
The following CloudFormation stacks will be deleted:
sampleforcleanup-Stack
Do you want to proceed with deleting these CloudFormation stacks? [Y/n]: Y
Initiated deletion of CloudFormation stack: `sampleforcleanup-Stack`
Waiting for stack `sampleforcleanup-Stack` to be deleted...
CloudFormation stack `sampleforcleanup-Stack` deleted successfully.
The following ssm_params will be deleted:
/sampleforcleanup/database/password
Do you want to proceed with deleting these ssm_params? [Y/n]: Y
Deleted SSM Parameter: /sampleforcleanup/database/password
Cleaned up: ['sampleforcleanup']
```

Automatisez la gestion dynamique du pipeline pour le déploiement de solutions de correctifs dans les environnements Gitflow en utilisant et AWS Service CatalogAWS CodePipeline

Créée par Balaji Vedagiri (AWS), Faisal Shahdad (AWS), Shanmugam Shanker (AWS) et Vivek Thangamuthu (AWS)

Récapitulatif

> **Note**
>
> AWS CodeCommit n'est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle concerne un scénario de gestion d'un pipeline de correctifs dynamiques dédié uniquement au déploiement sécurisé de solutions de correctifs dans un environnement de production. La solution est mise en œuvre et gérée à l'aide d'un AWS Service Catalog portefeuille et d'un produit. Une EventBridge règle Amazon est utilisée pour l'automatisation des événements. Les restrictions sont appliquées en utilisant les contraintes du portefeuille Service Catalog et les rôles AWS Identity and Access Management (IAM) pour les développeurs. Seule une AWS Lambda fonction est autorisée à lancer le produit Service Catalog, déclenchée par la EventBridge règle. Ce modèle est conçu pour les environnements dotés d'une configuration Gitflow spécifique, décrite dans Informations supplémentaires.

Généralement, un correctif est déployé pour résoudre les problèmes critiques ou de sécurité signalés dans un environnement réel, tel que le mode de production. Les correctifs doivent être déployés directement dans les environnements de préparation et de production uniquement. Les pipelines de préparation et de production sont largement utilisés pour les demandes de développement régulières. Ces pipelines ne peuvent pas être utilisés pour déployer des correctifs car certaines fonctionnalités permanentes de l'assurance qualité ne peuvent pas être promues en production. Pour publier des correctifs, ce modèle décrit un pipeline dynamique de courte durée doté des fonctionnalités de sécurité suivantes :

- Création automatique : un pipeline de correctifs est automatiquement créé chaque fois qu'une branche de correctifs est créée dans un AWS CodeCommit référentiel.

- Restrictions d'accès — Les développeurs n'ont pas accès à la création de ce pipeline en dehors du processus de correctif.
- Étape contrôlée — Le pipeline possède une étape contrôlée avec un jeton d'accès spécial, ce qui garantit qu'une pull request (PR) ne peut être créée qu'une seule fois.
- Étapes d'approbation — Les étapes d'approbation sont incluses dans le pipeline pour obtenir les approbations nécessaires des parties prenantes concernées.
- Suppression automatique — Le pipeline de correctifs est automatiquement supprimé chaque fois qu'une `hotfix` branche est supprimée du CodeCommit référentiel après sa fusion avec un PR.

Conditions préalables et limitations

Prérequis

- Trois actifs Comptes AWS sont requis comme suit :
  - Compte d'outils - Pour la configuration de l'intégration continue et de la livraison continue (CI/CD).
  - Compte Stage : pour les tests d'acceptation par les utilisateurs.
  - Compte de production : pour un utilisateur final professionnel.
  - (Facultatif) Ajoutez un Compte AWS pour faire office de compte QA. Ce compte est requis si vous souhaitez à la fois une configuration de pipeline principal, y compris l'assurance qualité, et une solution de pipeline de correctifs pour les tests.
- Une AWS CloudFormation pile avec une condition facultative à déployer dans le compte QA en utilisant le pipeline principal, si nécessaire. Le modèle peut toujours être testé sans la configuration du pipeline principal en créant et en supprimant une `hotfix` branche.
- Un bucket Amazon Simple Storage Service (Amazon S3) pour stocker CloudFormation les modèles utilisés pour créer les produits Service Catalog.
- Créez des règles d'approbation des relations publiques pour le CodeCommit référentiel conformément aux exigences de conformité (après avoir créé le référentiel).
- Limitez les autorisations IAM des développeurs et des chefs d'équipe pour refuser l'exécution de la fonction Lambda prcreation-lambda, car elle ne doit être invoquée que depuis le pipeline.

Limites

- Le CloudFormation fournisseur est utilisé lors de la phase de déploiement et l'application est déployée à l'aide d'un ensemble de CloudFormation modifications. Si vous souhaitez utiliser une autre option de déploiement, modifiez la CodePipeline pile selon vos besoins.
- Ce modèle utilise AWS CodeBuild d'autres fichiers de configuration pour déployer un exemple de microservice. Si vous avez un autre type de charge de travail (par exemple, des charges de travail sans serveur), vous devez mettre à jour toutes les configurations pertinentes.
- Ce modèle déploie l'application en une seule fois Région AWS (par exemple, USA East (Virginie du Nord) us-east-1). Comptes AWS Pour effectuer un déploiement dans plusieurs régions, modifiez la référence de région dans les commandes et les piles.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Les diagrammes de cette section fournissent des flux de travail pour un événement de création de cycle de vie et pour un événement de suppression du cycle de vie.

Le schéma précédent relatif à la création d'un événement du cycle de vie montre ce qui suit :

1. Le développeur crée une `hotfix-*` branche dans le CodeCommit référentiel pour développer une solution liée au correctif.
2. L'événement de création de `hotfix-*` branche est capturé par le biais de la EventBridge règle. Les détails de l'événement incluent le nom du référentiel et le nom de la branche.
3. La EventBridge règle invoque la AWS Lambda fonction. `hotfix-lambda-function` La EventBridge règle transmet les informations d'événement à la fonction Lambda en entrée.
4. La fonction Lambda traite l'entrée pour récupérer le nom du référentiel et le nom de la branche. Il lance le produit Service Catalog avec les valeurs extraites des entrées traitées.
5. Le produit Service Catalog inclut une configuration de pipeline qui déploiera la solution dans les environnements de scène et de production. Le bloc de pipeline inclut les étapes de source, de construction et de déploiement. Il existe également une étape d'approbation manuelle pour promouvoir le déploiement dans l'environnement de production.
6. L'étape source récupère le code du référentiel et de la `hotfix-*` branche créés lors de la première étape. Le code est transmis à la phase de construction via un compartiment Amazon S3

pour les artefacts. Au cours de la phase de construction, une image de conteneur est créée qui inclut le correctif logiciel développé dans la `hotfix-*` branche et introduit dans Amazon Elastic Container Registry (Amazon ECR).

7. De phase de déploiement en phase, l'environnement met à jour Amazon Elastic Container Service (Amazon ECS) avec la dernière image de conteneur incluant le correctif logiciel. Le correctif est déployé en créant et en exécutant un ensemble de CloudFormation modifications.
8. La fonction `prcreation-lambda` Lambda est invoquée après un déploiement réussi dans l'environnement Stage. Cette fonction Lambda crée un PR à partir de la `hotfix-*` branche vers les `main` branches `develop` et du référentiel. La fonction Lambda garantit que le correctif développé dans la `hotfix-*` branche est rétrofusionné et inclus dans les déploiements ultérieurs.
9. Une étape d'approbation manuelle permet de garantir que les parties prenantes concernées examinent le correctif et approuvent le déploiement en production.
10. La phase de déploiement dans l'environnement de production met à jour Amazon ECS avec la dernière image de conteneur incluant le correctif. Le correctif est déployé en créant et en exécutant un ensemble de CloudFormation modifications.

Le schéma précédent relatif à la suppression d'un événement du cycle de vie montre ce qui suit :

1. Le développeur supprime la `hotfix-*` branche après le déploiement réussi du correctif dans l'environnement de production.
2. L'événement de suppression de `hotfix-*` branche est capturé par le biais d'une EventBridge règle. Les détails de l'événement incluent le nom du référentiel et le nom de la branche.
3. La EventBridge règle invoque la fonction Lambda. La EventBridge règle transmet les informations d'événement à la fonction Lambda en entrée.
4. La fonction Lambda traite l'entrée pour récupérer le nom du référentiel et le nom de la branche. La fonction Lambda détermine le produit Service Catalog correspondant à partir de l'entrée transmise, puis met fin au produit.
5. La résiliation du produit provisionné par le Service Catalog supprime le pipeline et les ressources pertinentes qui ont été créées précédemment dans ce produit.

Automatisation et mise à l'échelle

- Le modèle inclut une EventBridge règle et une fonction Lambda, qui peuvent gérer plusieurs demandes de création de branche Hotfix en parallèle. La fonction Lambda approvisionne le produit Service Catalog pour la règle d'événement correspondante.
- La configuration du pipeline est gérée à l'aide du produit Service Catalog, qui fournit des fonctionnalités de contrôle de version. La solution s'adapte également automatiquement pour gérer en parallèle plusieurs développements de correctifs pour la même application.
- La fonction prcreation-lambda garantit que ces modifications du correctif sont également fusionnées dans les `develop` branches `main` et par le biais d'une création automatique de pull request. Cette approche est essentielle pour maintenir les branches `main` et les `develop` branches à jour avec tous les correctifs et éviter d'éventuelles régressions de code. Ce processus permet de maintenir la cohérence entre les branches et d'empêcher les régressions de code en garantissant que toutes les branches à longue durée de vie disposent des derniers correctifs.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source. AWS CodeCommit n'est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. Pour plus d'informations, consultez Comment migrer votre AWS CodeCommit dépôt vers un autre fournisseur Git.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.

- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.
- AWS Service Catalogvous permet de gérer de manière centralisée les catalogues de services informatiques approuvés. AWS Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- AWS CloudFormation Linter (cfn-lint) est un linter qui vérifie les modèles CloudFormation YAML ou JSON par rapport à la spécification des ressources. CloudFormation Il effectue également d'autres contrôles, tels que la vérification de la validité des valeurs des propriétés des ressources et le respect des meilleures pratiques.
- cfn-nag est un outil open source qui identifie les problèmes de sécurité potentiels dans les CloudFormation modèles en recherchant des modèles.
- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs. Ce modèle utilise Docker pour créer et tester des images de conteneurs localement.
- Git est un système de contrôle de version distribué et open source.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub dynamic_hotfix_codepipeline.

Bonnes pratiques

Passez en revue et ajustez les rôles IAM et les politiques de contrôle des services (SCP) dans votre environnement afin de vous assurer qu'ils limitent l'accès de manière appropriée. Cela est essentiel pour empêcher toute action susceptible de passer outre aux mesures de sécurité incluses dans ce modèle. Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Configuration de l'environnement de travail

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner l'exemple de référentiel dans un nouveau répertoire de votre lieu de travail, exécutez la commande suivante : `git clone git@github.com:aws-samples/dynamic_hotfix_codepipeline.git`	AWS DevOps
Exportez les variables d'environnement pour le déploiement de la CloudFormation pile.	Définissez les variables d'environnement suivantes qui seront utilisées comme entrée dans les CloudFormation piles ultérieurement dans ce modèle. • `ApplicationName` — Cette variable est utilisée pour nommer les ressources créées pour une application, afin de faciliter leur suivi. Utilisez la commande suivante, en `Applicationname` remplaçant par le nom réel de votre application : `export ApplicationName=<Applicationname>`	AWS DevOps

Tâche	Description	Compétences requises
	• `BucketStartName` — Cette variable permet de nommer un compartiment Amazon S3. Les noms des compartiments S3 doivent être globalement uniques Comptes AWS. Utilisez la commande suivante, en la `BucketName` remplaçant par un nom unique pour votre compartiment S3 : `export BucketStartName=<BucketName>` • Numéros de compte et régions : ces variables stockent Compte AWS les numéros des différents environnements et de la région de déploiement. Utilisez les commandes suivantes, en remplaçant les espaces réservés (tels que `prodaccountnumber` `etregion`) par vos Compte AWS chiffres réels et ceux Région AWS que vous utilisez. **Note** Le paramètre `QAAccount` est facultatif. Si	

Tâche	Description	Compétences requises
	vous souhaitez l'utiliser`QAAccount` , configurez-le en utilisant les paramètres de la pile de pipeline principale. `export ProdAccou nt=<prodaccountnum ber> export StageAcco unt=<stage/preprod accountnumber> export QAAccount =<qaccountnumber> export ToolsAcco unt=<toolsaccountn umber> export DepRegion =<region>`	

Configurer les prérequis requis dans Comptes AWS

Tâche	Description	Compétences requises
Créez les ressources requises pour le CI/CD dans le compte d'outils.	Pour déployer la CloudForm ation pile dans le compte Tools, utilisez les commandes suivantes. (Supprimez le `QAAccount` paramètre si vous n'utilisez pas le compte QA pour la configuration.) `#InToolsAccount`	AWS DevOps

Tâche	Description	Compétences requises
	`aws cloudformation deploy \ --template-file pre-requisites/pre-reqs.yaml \ --stack-name prereqs \ --parameter-overrides BucketStartName=${BucketStartName} \ ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \ StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \ QAAccount=${QAAccount} \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`  Notez les ressources créées par le CodeCommit référentiel et Amazon ECR à partir de la pile précédente. Ces paramètres sont nécessaires pour configurer la `main` branche du pipeline lors des prochaines étapes.	

Tâche	Description	Compétences requises

Créez les ressources requises pour le CI/CD dans les comptes de charge de travail.	1. Pour intégrer le CloudFormation modèle dans chaque compte de charge de travail (étape, production et assurance qualité facultative), utilisez les commandes suivantes. Dans la commande suivante, remplacez-le `S3bucketpackage` par le nom du compartiment Amazon S3 que vous souhaitez utiliser pour le packaging.
	
	`#InStageAccount`
	`aws cloudformation package \`
	`--template-file pre-requisites/infrastack.yaml \`
	`--s3-bucket <S3bucketpackage> \`
	`--s3-prefix infraStack \`
	`--region ${DepRegion} \`
	`--output-template-file pre-requisites/infrastructure_stage.template`
	
	`#InProdAccount`
	`aws cloudformation package \`
		AWS DevOps

Tâche	Description	Compétences requises
	--template-file pre-requisites/infrastack.yaml \ --s3-bucket <S3bucketpackage> \ --s3-prefix infraStack \ --region ${DepRegion} \ --output-template-file pre-requisites/infrastructure_prod.template 2. Pour déployer le CloudFormation modèle dans chaque compte de charge de travail, utilisez les commandes suivantes : #InStageAccount aws cloudformation deploy --stack-name inframainstack \ --parameter-overrides ApplicationName=${ApplicationName} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \ --template-file pre-requisites/infrastructure_stage.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM	

Tâche	Description	Compétences requises

	`#InProdAccount`
	`aws cloudformation deploy --stack-name inframainstack \`
	`--parameter-overrides ApplicationName=${ApplicationName} ToolsAccount=${ToolsAccount} DepRegion=${DepRegion} \`
	`--template-file pre-requisites/infrastructure_prod.template --region ${DepRegion} --capabilities CAPABILITY_NAMED_IAM`	

Tâche	Description	Compétences requises

Mettez à jour la politique du compartiment d'artefacts S3 pour autoriser l'accès aux comptes de charge de travail.	Pour mettre à jour les prérequis relatifs à la CloudFormation pile dans le compte d'outils, utilisez les commandes suivantes pour ajouter toutes les autorisations requises pour les comptes de charge de travail de scène et de production. (Supprimez le `QAAccount` paramètre si vous ne l'utilisez pas pour la configuration.)
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/pre-reqs.yaml \`
	`--stack-name prereqs \`
	`--parameter-overrides BucketStartName=${BucketStartName} \`
	`ApplicationName=${ApplicationName} ProdAccount=${ProdAccount} \`
	`StageAccount=${StageAccount} ToolsAccount=${ToolsAccount} \`
	`QAAccount=${QAAccount} PutPolicy=true \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
		AWS DevOps

Configurer la fonction Lambda et les ressources Service Catalog dans le compte d'outils

Tâche	Description	Compétences requises

Configurez le portefeuille et les produits du Service Catalog.	Pour configurer le portefeuille et les produits du Service Catalog, procédez comme suit :
	
	1. Téléchargez les modèles pipeline-main.yaml et pipeline-hotfix.yaml depuis le référentiel du répertoire vers CodePipeline un compartiment Amazon S3 (`Bucketname`) existant dans la région vers laquelle vous souhaitez effectuer le déploiement (). `DepRegion`
	
	`#InToolsAccount`
	`aws s3 cp ./codepipeline/pipeline-main.yaml s3://<Bucketname>/pipeline-main.yaml`
	`aws s3 cp ./codepipeline/pipeline-hotfix.yaml s3://<Bucketname>/pipeline-hotfix.yaml`
	
	2. Configurez le portefeuille et le produit Service Catalog qui géreront le pipeline pour les `hotfix` succursales `main` et. Notez les détails de la `Outputs`
		AWS DevOps

Tâche	Description	Compétences requises

	section pour `MainProductId` et `MainProductArtifactId` de la pile suivante. Les informations sont requises lors des étapes ultérieures de la configuration du pipeline pour la `main` succursale.
	
	`#InToolsAccount`
	`aws cloudformation deploy \`
	`--template-file pre-requisites/servicecatalogsetup.yaml \`
	`--stack-name servicecatalogsetup \`
	`--parameter-overrides TemplateBucket=<Bucketname> \`
	`--capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM --region ${DepRegion}`
	
	3. Donnez accès à un rôle IAM qui déploiera les ressources du compte d'outils vers le portefeuille de pipeline principal du portefeuille Service Catalog. Utilisez ce portefeuille pour déployer l'application à l'aide de la `main` branche. Pour plus d'informations	

Tâche	Description	Compétences requises
	sur la manière de fournir un accès, consultez la section According Access to Users dans la documentation du Service Catalog.	

Tâche	Description	Compétences requises
Configurez les fonctions Lambda.	Cette solution utilise les fonctions Lambda suivantes pour gérer les flux de travail liés aux correctifs : • `hotfix-lambda-function` gère le provisionnement des produits Service Catalog lors de la création d'une `hotfix` succursale. • `hotfix-cleanup-lambda-function` gère la résiliation du produit lorsqu'une `hotfix` branche est supprimée. • `prcreation-lambda` crée des pull requests de la `hotfix` branche vers les `main` branches `develop` et. Pour permettre aux fonctions Lambda de provisionner et de résilier les produits Service Catalog lorsque `hotfix` des branches sont créées ou supprimées par le biais de la EventBridge règle associée, procédez comme suit : 1. Pour créer les rôles et autorisations IAM pour les fonctions Lambda, utilisez la commande suivante pour	AWS DevOps

Tâche	Description	Compétences requises
	déployer CloudFormation une pile : `#InToolsAccount aws cloudformation deploy \ --templat e-file pre-requi sites/lambdasetup. yaml \ --stack-n ame prsclambdasetup \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_I AM --region ${DepRegi on}` 2. Après le déploiement de la pile, accordez l'`hotfix-lambda-execution-role` accès au portefeui lle de pipelines de correctif s du portefeuille Service Catalog en utilisant le AWS Management Console. Cet accès permet à la fonction Lambda de lancer ou de mettre fin au produit Service Catalog pour les branches de correctifs.	

Création d'un pipeline pour la succursale principale et déploiement de l'application dans les comptes de charge de travail

Tâche	Description	Compétences requises
Configurez le pipeline pour `main` la succursale.	Pour configurer le pipeline pour la branche principal	AWS DevOps

Tâche	Description	Compétences requises

	e, exécutez la commande suivante dans le compte tools. Remplacez les paramètres pour `MainProductId` et par `MainProductArtifactId` les valeurs issues des sorties de la `servicecatalogsetup` pile.
	
	`#InToolsAccount`
	`aws servicecatalog provision-product \`
	`--product-id <MainProductId> \`
	`--provisioning-artifact-id <MainProductArtifactId> \`
	`--provisioned-product-name "${ApplicationName}-main-pipeline" \`
	`--provisioning-parameters Key=CodeCommitRepoName,Value="${ApplicationName}-repository" Key=ECRRepository,Value="${ApplicationName}-app" \`
	`--region=${DepRegion}`	

Tâche	Description	Compétences requises
Déployez l'application à l'aide de la `main` branche.	1. Pour cloner le CodeCommit dépôt créé dans les prérequis, utilisez la `git clone` commande. Pour plus d'informations, voir Se connecter au CodeCommit référentiel en clonant le référentiel comme décrit dans la CodeCommit documentation. 2. Copiez tous les fichiers d'application depuis le `repotemplates` répertoire disponible dans le référentiel vers le clone (`${ApplicationName}-repository`) de votre dépôt local. Modifiez les fichiers suivants pour mettre à jour l'`ToolsAccount` ID. Dans chaque fichier, localisez le `RegistryAccountid` paramètre et définissez sa valeur selon votre `ToolsAccount` identifiant. Validez les modifications dans le CodeCommit référentiel et transférez les fichiers vers les `develop` branches `main` et. • ecs-configuration-prod.yaml • ecs-configuration-qa.yaml	AWS DevOps

Tâche	Description	Compétences requises
	• ecs-configuration-stage.yaml 3. Pour vérifier le déploiement de l'application, surveillez CodePipeline son exécution à l'aide du AWS Management Console. Une fois le déploiement terminé, accédez à l'application à l'aide du FQDN Application Load Balancer dans l'environnement de stage. Vérifiez que l'application fonctionne comme prévu. 4. Pour approuver le déploiement en production, utilisez la CodePipeline console pour localiser le pipeline de votre application. Trouvez la `ApprovalToStart` scène. Passez en revue les modifications et, si elles sont satisfaisantes, autorisez manuellement le déploiement en production.	

Créez le pipeline pour une branche hotfix-* et déployez le correctif

Tâche	Description	Compétences requises
Créez une `hotfix-*` branche et validez les modifications.	Pour créer un pipeline pour la `hotfix-*` branche et déployer le correctif sur les	AWS DevOps

Tâche	Description	Compétences requises
	comptes de charge de travail, procédez comme suit : 1. Créez une branche en utilisant un nom commençant par le mot clé`hotfix`. Par exemple, ce modèle utilise la `hotfix-check1` branche du référentiel CodeCommit d'applications (`${ApplicationName}-repository`). Pour des étapes plus détaillées, consultez Connect to an AWS CodeCommit repository et Basic Git commands dans la CodeCommit documentation. 2. Vérifiez que le produit Service Catalog `Hotfix CICD Pipeline` est correctement approvisionné dynamiquement pour la `hotfix-check1` succursale. Le nom du produit provisionné est nommé d'après le nom de la branche de ce correctif logiciel et le nom du CodeCommit référentiel de l'application. 3. Apportez quelques modifications mineures dans le fichier index.htm	

Tâche	Description	Compétences requises
	l et transférez-les vers le CodeCommit référentiel. 4. Vérifiez que l' CodePipeline exécution est réussie dans l'environnement de scène. Pour effectuer un déploiement dans l'environnement de production, veuillez fournir une approbation manuelle dans CodePipeline. 5. Vérifiez que les modifications sont visibles sur la page d'accueil de l'application en utilisant le nom de domaine complet (FQDN) Application Load Balancer. Le FQDN est disponible dans la `Outputs` section de. `inframainstack-ALBStack-*`	

Tâche	Description	Compétences requises
Supprimez la `hotfix-check1` branche.	Pour supprimer la `hotfix-check1` branche créée précédemment, procédez comme suit : 1. Supprimez la `hotfix-check1` branche qui se trouve dans le référentiel de CodeCommit l'application. 2. Vérifiez que le produit Service Catalog fourni pour la `hotfix-check1` succursale s'est correctement arrêté.	AWS DevOps

Nettoyage des ressources

Tâche	Description	Compétences requises
Nettoyez les ressources déployées.	Pour nettoyer les ressources déployées précédemment, procédez comme suit : 1. Pour réduire le service Amazon ECS à zéro réplication dans les comptes de charge de travail, utilisez la commande suivante : `aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}`	AWS DevOps

Tâche	Description	Compétences requises
	`-Service-stage --desired-count 0 --region ${DepRegion} aws ecs update-service --cluster ${ApplicationName}-Cluster --service ${ApplicationName}-Service-prod --desired-count 0 --region ${DepRegion}` 2. Mettez fin au produit Service Catalog qui a été fourni pour la `main` succursale. 3. Nettoyez les objets créés dans les compartiments Amazon S3 dans le compte Tools. Supprimez toutes les images Docker dans Amazon ECR avant de supprimer le registre lui-même. 4. Supprimez les rôles IAM dans la section Accès accordé des portefeuilles Service Catalog avant de supprimer le portefeuille Service Catalog. 5. Supprimez les CloudFormation piles déployées dans le compte d'outils et dans les comptes de charge de travail.	

Tâche	Description	Compétences requises
	``` ##In Tools Account## aws cloudformation delete-stack --stack-n ame servicecatalogsetu p --region ${DepRegi on} aws cloudformation delete-stack --stack- name prlambdasetup -- region ${DepRegion} aws cloudformation delete-stack --stack- name prereqs --region ${DepRegion} ```	
	``` ##In Workload Accounts# # aws cloudformation delete-stack --stack- name inframainstack -- region ${DepRegion} ```	
	Pour plus d'informations, consultez la section Suppression de produits provisionnés dans la documentation du Service Catalog.	

Résolution des problèmes

Problème	Solution
Les modifications que vous avez apportées au CodeCommit référentiel ne sont pas déployées.	Vérifiez les CodeBuild journaux pour détecter les erreurs lors de l'action de compilation de Docker. Pour plus d'informations, consultez la documentation CodeBuild .

Problème	Solution
Le produit Service Catalog n'est pas approvisionné.	Passez en revue les CloudFormation piles associées pour détecter les événements ayant échoué. Pour plus d'informations, consultez la documentation CloudFormation .

Ressources connexes

- Commandes Git de base
- Configurer une politique IAM pour limiter les transferts et les fusions vers une succursale
- Se connecter à un AWS CodeCommit référentiel
- Octroi d'accès aux utilisateurs
- Transférer une image Docker vers un référentiel privé Amazon ECR
- Dépannage AWS CodeBuild
- Qu'est-ce que c'est AWS CodePipeline ?

Informations supplémentaires

Ce modèle est conçu pour les environnements dont la configuration Gitflow est adoptée pour le flux de travail de développement. La CI/CD process. The pipelines follow the deployment cycle that starts from development and moves through quality assurance (QA), stage, and production environments. The CI/CD configuration inclut deux branches git avec des déploiements promotionnels dans les environnements comme suit :

- La `develop` branche se déploie dans l'environnement de développement.
- La `main` succursale effectue des déploiements dans les environnements d'assurance qualité, de scène et de production.

Dans cette configuration, il est difficile d'appliquer un correctif ou un correctif de sécurité plus rapidement que le cycle de déploiement habituel alors que le développement actif de nouvelles fonctionnalités est en cours. Un processus dédié est nécessaire pour traiter les correctifs ou les demandes de sécurité, afin de garantir le bon fonctionnement et la sécurité des environnements en direct.

Toutefois, vous pouvez utiliser les autres options disponibles sans avoir besoin d'un processus de déploiement dédié si :

- Le CI/CD process is well-equipped with automated testing, such as functional and end-to-end tests, which eliminate the need for manual testing and prevent delays in deployments to production. However, if automated testing isn't well integrated into the CI/CD processus, qui consiste à apporter une petite correction à l'environnement de production, peut devenir complexe et fastidieux pour les développeurs. Cela est dû au fait que de nouvelles fonctionnalités peuvent être en attente d'approbation et de validation dans l'environnement d'assurance qualité. Un correctif logiciel ou un correctif de sécurité ne peuvent pas être mis en production de manière simple et simultanée.
- Les équipes de développement déploient en permanence de nouvelles fonctionnalités dans l'environnement de production, en intégrant des correctifs ou des correctifs de sécurité dans le déploiement planifié de chaque nouvelle fonctionnalité. En d'autres termes, la prochaine mise à jour des fonctionnalités de l'environnement de production comprend deux composants : l'ajout d'une nouvelle fonctionnalité et l'inclusion du correctif logiciel ou du correctif de sécurité. Toutefois, si le cycle de déploiement n'est pas continu, plusieurs nouvelles fonctionnalités peuvent déjà être en attente d'approbation dans l'environnement d'assurance qualité. Gérer les différentes versions et s'assurer que les modifications appropriées sont réappliquées peut alors devenir complexe et source d'erreurs.

> **Note**
>
> Si vous utilisez la version 2 de AWS CodePipeline avec des déclencheurs appropriés configurés sur la `hotfix` branche, vous avez toujours besoin d'un processus dédié pour traiter les demandes imprévues. Dans la version 2, vous pouvez configurer des déclencheurs pour les requêtes push ou pull. L'exécution sera soit mise en file d'attente, soit exécutée immédiatement, selon l'état précédent du pipeline. Cependant, avec un pipeline dédié, les correctifs sont appliqués immédiatement à l'environnement de production, ce qui garantit que les problèmes urgents sont résolus sans délai.

Automatisez l'ingestion et la visualisation des métriques personnalisées Amazon MWAA sur Amazon Managed Grafana à l'aide de Terraform

Créée par Faisal Abdullah (AWS) et Satya Vajrapu (AWS)

Récapitulatif

Ce modèle explique comment utiliser Amazon Managed Grafana pour créer et surveiller des métriques personnalisées qui sont ingérées par Amazon Managed Workflows pour Apache Airflow (Amazon MWAA). Amazon MWAA sert d'orchestrateur pour les flux de travail, en utilisant des graphes acycliques dirigés (DAGs) écrits en Python. Ce modèle est centré sur la surveillance de mesures personnalisées, notamment le nombre total d'exécutions DAGs effectuées au cours de la dernière heure, le nombre de réussites et DAGs d'échecs par heure et la durée moyenne de ces processus. Cette analyse montre comment Amazon Managed Grafana s'intègre à Amazon MWAA pour permettre une surveillance complète et des informations sur l'orchestration des flux de travail au sein de cet environnement.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS disposant des autorisations utilisateur nécessaires pour créer et gérer les éléments suivants Services AWS :
  - AWS Identity and Access Management Rôles et politiques (IAM)
  - AWS Lambda
  - Amazon Managed Grafana
  - Amazon Managed Workflows for Apache Airflow (Amazon MWAA)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Timestream
- Accès à un environnement shell qui peut être un terminal sur votre machine locale ou AWS CloudShell.
- Un environnement shell avec Git installé et la dernière version de AWS Command Line Interface (AWS CLI) installée et configurée. Pour plus d'informations, consultez la section Installation ou mise à jour vers la dernière version AWS CLI de la AWS CLI documentation.
- La version suivante de Terraform est installée : `required_version = ">= 1.6.1, < 2.0.0"` vous pouvez utiliser tfswitch pour basculer entre les différentes versions de Terraform.

- Source d'identité configurée AWS IAM Identity Center pour votre Compte AWS. Pour plus d'informations, voir Confirmer vos sources d'identité dans IAM Identity Center dans la documentation d'IAM Identity Center. Vous pouvez choisir entre Active Directory par défaut Répertoire IAM Identity Center ou un fournisseur d'identité (IdP) externe tel qu'Okta. Pour plus d'informations, consultez la section Ressources connexes.

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Terraforme `required_version = ">= 1.6.1, < 2.0.0"`
- Amazon Managed Grafana version 9.4 ou ultérieure. Ce modèle a été testé sur la version 9.4.

Architecture

Le schéma d'architecture suivant met en évidence les éléments Services AWS utilisés dans la solution.

Le schéma précédent décrit le flux de travail suivant :

1. Les métriques personnalisées d'Amazon MWAA proviennent de DAGs celles qui sont exécutées dans l'environnement. Les métriques sont téléchargées dans le compartiment Amazon S3 au format de fichier CSV. Les éléments suivants DAGs utilisent les fonctionnalités d'interrogation de base de données d'Amazon MWAA :
   - `run-example-dag`— Ce DAG contient un exemple de code Python qui définit une ou plusieurs tâches. Il fonctionne toutes les 7 minutes et affiche la date. Après l'impression de la date, le DAG inclut une tâche dont l'exécution doit être interrompue pendant une durée spécifique.
   - `other-sample-dag`— Ce DAG s'exécute toutes les 10 minutes et imprime la date. Après l'impression de la date, le DAG inclut une tâche dont l'exécution doit être interrompue pendant une durée spécifique.

- `data-extract`— Ce DAG s'exécute toutes les heures, interroge la base de données Amazon MWAA et collecte des métriques. Une fois les métriques collectées, ce DAG les écrit dans un compartiment Amazon S3 pour un traitement et une analyse ultérieurs.

2. Pour rationaliser le traitement des données, les fonctions Lambda s'exécutent lorsqu'elles sont déclenchées par des événements Amazon S3, ce qui facilite le chargement des métriques dans Timestream.
3. Timestream est intégré en tant que source de données dans Amazon Managed Grafana où sont stockées toutes les métriques personnalisées d'Amazon MWAA.
4. Les utilisateurs peuvent interroger les données et créer des tableaux de bord personnalisés pour visualiser les indicateurs de performance clés et obtenir des informations sur l'orchestration des flux de travail au sein d'Amazon MWAA.

Outils

Services AWS

- AWS IAM Identity Centervous permet de gérer de manière centralisée l'accès par authentification unique (SSO) à toutes vos applications Comptes AWS et à celles du cloud.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez. Dans ce modèle, AWS Lambda exécute le code Python en réponse aux événements Amazon S3 et gère automatiquement les ressources de calcul.
- Amazon Managed Grafana est un service de visualisation de données entièrement géré que vous pouvez utiliser pour interroger, corréler, visualiser et émettre des alertes sur vos métriques, journaux et traces. Ce modèle utilise Amazon Managed Grafana pour créer un tableau de bord pour la visualisation des métriques et les alertes.
- Amazon Managed Workflows for Apache Airflow (Amazon MWAA) est un service d'orchestration géré pour Apache Airflow que vous pouvez utiliser pour configurer et exploiter des pipelines de données dans le cloud à grande échelle. Apache Airflow est un outil open source utilisé pour créer, planifier et surveiller par programmation des séquences de processus et de tâches appelées flux de travail. Dans ce modèle, un échantillon DAGs et un extracteur de métriques DAG sont déployés dans Amazon MWAA.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de

données. Dans ce modèle, Amazon S3 est utilisé pour stocker DAGs des scripts et des métriques personnalisées au format CSV.

- Amazon Timestream LiveAnalytics for is est une base de données de séries chronologiques rapide, évolutive, entièrement gérée et spécialement conçue qui facilite le stockage et l'analyse de milliards de points de données de séries chronologiques par jour. Timestream for s'intègre LiveAnalytics également aux services couramment utilisés pour la collecte de données, la visualisation et l'apprentissage automatique. Dans ce modèle, il est utilisé pour ingérer les métriques personnalisées Amazon MWAA générées.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud. Ce modèle utilise un module Terraform pour automatiser le provisionnement de l'infrastructure dans. AWS

Référentiel de code

Le code de ce modèle est disponible GitHub dans le dépôt visualize-amazon-mwaa-custom-metrics-grafana. Le `stacks/Infra` dossier contient les éléments suivants :

- Fichiers de configuration Terraform pour toutes les ressources AWS
- Fichier .json du tableau de bord Grafana dans le dossier `grafana`
- Amazon Managed Workflows pour Apache Airflow DAGs dans le dossier `mwaa/dags`
- Code Lambda pour analyser le fichier .csv et stocker les métriques dans le dossier de la base de données Timestream `src`
- Fichiers .json de politique IAM dans le dossier `templates`

Bonnes pratiques

Terraform doit stocker l'état de votre infrastructure et de votre configuration gérées afin de pouvoir mapper les ressources du monde réel à votre configuration. Par défaut, Terraform stocke l'état localement dans un fichier nommé. `terraform.tfstate` Il est essentiel de garantir la sécurité et l'intégrité de votre fichier d'état Terraform, car il maintient l'état actuel de votre infrastructure. Pour plus d'informations, consultez Remote State dans la documentation Terraform.

Épopées

Déployez l'infrastructure à l'aide de Terraform

Tâche	Description	Compétences requises

Déployez l'infrastructure.	Pour déployer l'infrastructure de la solution, procédez comme suit :
	1. Ouvrez un terminal ou une invite de commande sur votre ordinateur local ou en utilisant AWS CloudShell.
	2. Accédez au répertoire dans lequel vous souhaitez cloner le référentiel.
	3. Pour cloner le dépôt, exécutez la commande suivante :
	`git clone https://github.com/aws-samples/visualize-amazon-mwaa-custom-metrics-grafana`
	4. Une fois le processus de clonage terminé, exécutez la commande suivante pour accéder au répertoire du référentiel cloné :
	`cd visualize-amazon-mwaa-custom-metrics-grafana/stacks/infra`
	5. Pour télécharger et initialiser les fournisseurs requis,
		AWS DevOps

Tâche	Description	Compétences requises

	exécutez la commande suivante :
	`terraform init`
	6. Pour obtenir une vue complète de toutes les ressources que Terraform créera, exécutez la commande suivante :
	`terraform plan`
	Terraform fournit les ressources suivantes :
	• Amazon Virtual Private Cloud (Amazon VPC) et composants réseau associés
	• Ressources Amazon S3
	• AWS Lambda fonctions
	• Ressources Amazon Managed Grafana (espace de travail, tableaux de bord, source de données)
	• Soutenir les ressources IAM (rôles et politiques)
	7. Pour créer les AWS ressources à partir de la sortie du plan, exécutez la commande suivante :	

Tâche	Description	Compétences requises

	`terraform apply -auto-approve`
	
	Le provisionnement de l'infrastructure est terminé en 20 minutes environ.
	8. Pour créer les AWS ressources spécifiées conformément à la configuration définie dans vos fichiers Terraform, exécutez la commande suivante :
	
	`terraform apply`	

Valider les ressources d'infrastructure déployées

Tâche	Description	Compétences requises
Validez l'environnement Amazon MWAA.	Pour valider l'environnement Amazon MWAA, procédez comme suit : 1. Connectez-vous au AWS Management Console, accédez à la console du tableau de bord Amazon MWAA et sélectionnez Open Airflow UI. 2. Vous devriez voir les trois éléments suivants DAGs dans le statut Actif :	AWS DevOps, ingénieur de données

Tâche	Description	Compétences requises
	• extrait de données • run-example-dag • other-sample-dag 3. Si un DAG n'est pas actif, vous pouvez l'activer en activant le commutateur situé à côté du nom du DAG.	
Vérifiez les horaires du DAG.	Pour consulter le calendrier de chaque DAG, accédez à l'onglet Planification de l'interface utilisateur d'Airflow. Chacun des programmes suivants DAGs possède un calendrier préconfiguré, qui s'exécute dans l'environnement Amazon MWAA et génère des métriques personnalisées : • run-example-dag- Fonctionne toutes les 7 minutes • other-sample-dag- Fonctionne toutes les 10 minutes • data-extract - Fonctionne toutes les heures Vous pouvez également voir les exécutions réussies de chaque DAG dans la colonne Exécutions.	Ingénieur de données, AWS DevOps

Configuration de l'environnement Amazon Managed Grafana

Tâche	Description	Compétences requises
Configurez l'accès à l'espace de travail Amazon Managed Grafana.	Les scripts Terraform ont créé l'espace de travail, les tableaux de bord et la page de statistiques Amazon Managed Grafana requis. Pour configure r l'accès afin de pouvoir les consulter, procédez comme suit : 1. Ouvrez la console Amazon Managed Grafana. 2. Dans Workspaces, sélectionnez l'espace de travail `grafana-ws-dev` et accédez à l'onglet Authentification dans le volet inférieur. 3. Cliquez sur le bouton Attribuer un nouvel utilisate ur ou un nouveau groupe. 4. Ajoutez votre groupe dans l'onglet Groupes ou un utilisateur dans l'onglet Utilisateurs, puis cliquez sur le bouton Attribuer un utilisateur et des groupes. 5. Une fois l'utilisateur (ou le groupe) ajouté, faites de cet utilisateur (ou de ce groupe) un administr ateur. Sélectionnez l'utilisa teur dans Utilisateurs	AWS DevOps

Tâche	Description	Compétences requises
	assignés ou groupe dans l'onglet Groupe d'utilisateurs assignés et choisissez Make admin dans le menu déroulant. Pour plus d'informations, consultez Utiliser AWS IAM Identity Center avec votre espace de travail Amazon Managed Grafana dans la documentation Amazon Managed Grafana. 6. Accédez à Workspaces, puis choisissez l'URL de l'espace de travail Grafana. Pour vous connecter à Amazon Managed Grafana en tant qu'administrateur, choisissez Se connecter avec. AWS IAM Identity Center	

Tâche	Description	Compétences requises
Installez le plugin Amazon Timestream.	Les métriques personnalisées Amazon MWAA sont chargées dans la base de données Timestream. Vous utilisez le plugin Timestream pour visualiser les métriques avec les tableaux de bord Amazon Managed Grafana. Pour installer le plugin Timestream, procédez comme suit : 1. Dans la console Amazon Managed Grafana, développez le menu dans le volet de navigation de gauche et accédez à Administration, Plugins. 2. Recherchez puis installez la dernière version du plugin Amazon Timestream. 3. Une fois le plugin installé, allez dans Administration, Sources de données pour voir la source de données Timestream. Si la source de données n'est pas répertoriée, actualisez la page. Pour plus d'informations, consultez la section Étendez votre espace de travail avec des plug-ins dans la	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	documentation Amazon Managed Grafana.	

Visualisez les métriques personnalisées dans le tableau de bord Amazon Managed Grafana

Tâche	Description	Compétences requises
Consultez le tableau de bord Amazon Managed Grafana.	Pour consulter les statistiq ues qui ont été ingérées dans l'espace de travail Amazon Managed Grafana, procédez comme suit : 1. Dans la console Amazon Managed Grafana, choisissez Dashboards dans le volet de navigation de gauche. 2. Pour afficher les métriques , choisissez les tableaux de bord des événements MWAA, puis sélectionnez mwaa_metrics. La page des statistiques du tableau de bord affiche les informations suivantes : • Nombre total de DAG exécutés au cours de la dernière heure • Nombre total d'exécutions DAG réussies, échouées	AWS DevOps

Tâche	Description	Compétences requises
	et en cours d'exécution au cours de la dernière heure • Durée moyenne de toutes les exécutions DAG réussies et échouées	
Personnalisez le tableau de bord Amazon Managed Grafana.	Pour personnaliser les tableaux de bord en vue de futures améliorations, procédez comme suit : 1. Sur la `mwaa_metrics` page du tableau de bord Amazon Managed Grafana, choisissez l'icône des paramètres du tableau de bord. 2. Pour afficher la structure de données qui définit le tableau de bord, choisisse z le modèle JSON. Vous pouvez personnaliser le tableau de bord en modifiant ce modèle JSON directement dans la console. Le code source de ce tableau de bord est également disponible dans le `dashboard.json` fichier du `stacks/infra/grafana` dossier du GitHub référentiel.	AWS DevOps

Nettoyer les AWS ressources

Tâche	Description	Compétences requises
Suspendez les exécutions du DAG Amazon MWAA.	Pour suspendre les exécutions du DAG, procédez comme suit : 1. Dans la console Amazon MWAA, accédez aux environnements Airflow et choisissez Open Airflow UI. 2. Pour suspendre le DAG, utilisez le commutateur situé à côté de chaque DAG. 3. Actualisez la page d'interface utilisateur Airflow, qui devrait en répertorier trois DAGs dans la section Suspendu.	AWS DevOps, ingénieur de données
Supprimez les objets dans les compartiments Amazon S3.	Pour supprimer les compartiments Amazon S3 mwaa-events-bucket-* et mwaa-metrics-bucket-*, suivez les instructions d'utilisation de la console Amazon S3 dans Supprimer un compartiment dans la documentation Amazon S3.	AWS DevOps
Détruisez les ressources créées par Terraform.	Pour détruire les ressources créées par Terraform et le fichier d'état local Terraform associé, procédez comme suit :	AWS DevOps

Tâche	Description	Compétences requises
	1. (Facultatif) Avant de supprimer les ressource s, vous pouvez prévisual iser les modifications que Terraform apportera. Pour générer un plan, exécutez la commande suivante : `terraform plan -destroy` Le résultat de la `destroy` commande indique que la commande supprimera toutes les AWS ressources créées précédemment. 2. `terraform destroy -auto-approve` Cette commande prend environ 20 minutes pour détruire l'infrastructure. **Note** Pour détruire toutes les ressource s gérées par Terraform, exécutez la commande suivante. : Le `-auto-approve` tag n'attend pas la confirmation de l'utilisateur	

Tâche	Description	Compétences requises

	pour commencer à détruire les ressources.
	3. Pour supprimer le fichier d'état Terraform local, exécutez les commandes suivantes :
	`rm .terraform.lock.hcl`
	`rm -rf .terraform`
	`rm terraform.tfstate*`	

Résolution des problèmes

Problème	Solution
`null_resource.plugin_mgmt (local-exec): aws: error: argument operation: Invalid choice, valid choices are:`	Passez AWS CLI à la dernière version.
Erreur lors du chargement des sources de données - `Fetch error: 404 Not Found Instantiating…`	L'erreur est intermittente. Patientez quelques minutes, puis actualisez vos sources de données pour afficher la source de données Timestream répertoriée.

Ressources connexes

AWS documentation

- Amazon Managed Grafana pour les tableaux de bord et la visualisation

- Configurer Amazon Managed Grafana pour utiliser Okta
- À utiliser AWS IAM Identity Center avec votre espace de travail Amazon Managed Grafana
- Travailler avec DAGs sur Amazon MWAA

AWS vidéos

- Configurez IAM Identity Center avec Amazon Managed Grafana pour l'authentification, comme indiqué dans la vidéo suivante.

https://www.youtube-nocookie.com/embed/XX2Xcz-Ps9U ? contrôles = 0

- Si IAM Identity Center n'est pas disponible, vous pouvez également intégrer l'authentification Amazon Managed Grafana en utilisant un fournisseur d'identité externe (IdP) tel qu'Okta, comme le montre la vidéo suivante.

https://www.youtube-nocookie.com/embed/A4 Oh JHxl2xp ? contrôles = 0

Informations supplémentaires

Vous pouvez créer une solution complète de surveillance et d'alerte pour votre environnement Amazon MWAA, permettant une gestion proactive et une réponse rapide aux problèmes ou anomalies potentiels. Amazon Managed Grafana inclut les fonctionnalités suivantes :

Alertes — Vous pouvez configurer des alertes dans Amazon Managed Grafana en fonction de seuils ou de conditions prédéfinis. Configurez des notifications par e-mail pour avertir les parties prenantes concernées lorsque certains indicateurs dépassent ou tombent en dessous des seuils spécifiés. Pour plus d'informations, consultez la section Alertes Grafana dans la documentation Amazon Managed Grafana.

Intégration — Vous pouvez intégrer Amazon Managed Grafana à divers outils tiers tels que OpsGenie PagerDuty, ou Slack pour des fonctionnalités de notification améliorées. Par exemple, vous pouvez configurer des webhooks ou les intégrer APIs pour déclencher des incidents et des notifications sur ces plateformes en fonction des alertes générées dans Amazon Managed Grafana. De plus, ce modèle fournit un GitHub référentiel pour créer des AWS ressources. Vous pouvez intégrer davantage ce code aux flux de travail de déploiement de votre infrastructure.

Simplifiez le développement et le déploiement des robots Amazon Lex à l'aide d'un flux de travail automatisé

Créée par Balaji Panneerselvam (AWS), Anand Jumnani (AWS), Attila Dancso (AWS), James O'Hara (AWS) et Pavan Dusanapudi (AWS)

Récapitulatif

Le développement et le déploiement de robots conversationnels Amazon Lex peuvent s'avérer difficiles lorsque vous essayez de gérer plusieurs fonctionnalités, développeurs et environnements. Un flux de travail automatisé utilisant les principes de l'infrastructure en tant que code (IaC) peut aider à rationaliser le processus. Ce modèle peut contribuer à améliorer la productivité des développeurs Amazon Lex et à permettre une gestion efficace du cycle de vie des bots de la manière suivante :

- Permettre le développement simultané de plusieurs fonctionnalités - Grâce à un flux de travail automatisé, les développeurs peuvent travailler sur différentes fonctionnalités en parallèle dans des branches distinctes. Les modifications peuvent ensuite être fusionnées et déployées sans bloquer d'autres tâches.
- Utilisez l'interface utilisateur de la console Amazon Lex : les développeurs peuvent utiliser la console conviviale Amazon Lex pour créer et tester des robots. Les robots sont ensuite décrits dans le code d'infrastructure pour le déploiement.
- Promouvoir les robots dans tous les environnements - Le flux de travail automatise la promotion des versions de robots provenant d'environnements inférieurs, tels que le développement, les tests et la production. Cette approche réduit les risques et les frais généraux liés aux promotions manuelles.
- Maintenir le contrôle des versions : la gestion des définitions de bots dans Git, plutôt que uniquement via le service Amazon Lex, vous permet de contrôler les versions et d'établir une piste d'audit. Les modifications sont suivies auprès des développeurs individuels, contrairement à ce qui se passe lorsque vous utilisez AWS Management Console ou APIs modifiez uniquement les robots stockés dans AWS.

En automatisant le processus de publication du bot Amazon Lex, les équipes peuvent fournir des fonctionnalités plus rapidement, tout en réduisant les risques et les efforts. Les bots restent sous contrôle de version plutôt qu'isolés dans la console Amazon Lex.

Conditions préalables et limitations

Prérequis

- Le flux de travail implique plusieurs Comptes AWS environnements (développement, production et DevOps), ce qui nécessite une gestion des comptes et des configurations d'accès entre comptes.
- Python 3.9 est disponible dans votre environnement de déploiement ou votre pipeline.
- Git est installé et configuré sur un poste de travail local pour le contrôle du code source.
- AWS Command Line Interface (AWS CLI) installé et configuré pour s'authentifier à l'aide de la ligne de commande ou de Python.

Limites

- Accès au référentiel — Le flux de travail suppose que le pipeline d'intégration continue et de livraison continue (CI/CD) dispose des autorisations nécessaires pour valider les modifications apportées au référentiel de code source.
- Version initiale du bot : l'outillage nécessite qu'une version initiale du bot soit déployée à l'aide de AWS CloudFormation modèles. Vous devez créer la première itération du bot et la valider dans le dépôt avant que le flux de travail automatisé puisse prendre le relais.
- Conflits de fusion — Bien que le flux de travail vise à permettre le développement simultané, il existe toujours un risque de conflits de fusion lors de l'intégration de modifications provenant de différentes branches. La résolution des conflits dans les configurations des robots peut nécessiter une intervention manuelle.

Versions du produit

- Python 3.9 ou supérieur
- AWS CDK v2 2.124.0 ou supérieur
- AWS SDK pour Python (Boto3)1,28 ou supérieur

Architecture

Le schéma suivant présente l'architecture de haut niveau et les principaux composants de la solution.

Les principaux composants sont les suivants :

- Repo de robots Lex : référentiel Git qui stocke les définitions iAc pour les robots Amazon Lex.
- DevOps— Un site Compte AWS dédié à l'hébergement des pipelines CI/CD et des ressources connexes pour le processus de développement et de déploiement.
- Pipelines : AWS CodePipeline instances qui automatisent les différentes étapes du cycle de développement et de déploiement du bot, telles que la création d'un nouveau bot, l'exportation de la définition d'un bot, l'importation d'une définition de bot et la suppression d'un bot.
- Bots de tickets et bot principal : les ressources du bot Amazon Lex, où les bots de ticket sont des robots spécifiques aux fonctionnalités développés par des équipes ou des développeurs individuels et le bot principal est le bot de base qui intègre toutes les fonctionnalités.

Le schéma d'architecture illustre le flux de travail suivant :

1. Bot principal de référence : le point de départ du flux de travail consiste à définir la base de référence du bot principal dans l'environnement de développement (Dev). Le bot principal sert de base au développement futur et aux ajouts de fonctionnalités.
2. Créer un bot de tickets : lorsqu'une nouvelle fonctionnalité ou une modification est requise, un bot de tickets est créé. Le bot de tickets est essentiellement une copie ou une branche du bot principal sur laquelle les développeurs peuvent travailler sans affecter la version principale.
3. Exporter le bot de tickets : une fois le travail sur le bot de tickets terminé, celui-ci est exporté depuis le service Amazon Lex. Ensuite, la branche qui contient le ticket bot est rebasée à partir de la branche principale. Cette étape garantit que toutes les modifications apportées au bot principal pendant le développement du bot de tickets sont incorporées, réduisant ainsi les conflits potentiels.
4. Importer un bot de tickets rebasé et valider — Le bot de tickets rebasé est réimporté dans l'environnement de développement et validé pour garantir qu'il fonctionne correctement avec les dernières modifications apportées par la branche principale. Si la validation est réussie, une pull request (PR) est créée pour fusionner les modifications du ticket bot dans la branche principale.
5. Supprimer le bot de tickets — Une fois que les modifications ont été fusionnées avec succès dans la branche principale, le bot de tickets n'est plus nécessaire. Le bot de tickets peut être supprimé pour que l'environnement reste propre et gérable.
6. Déployer le bot principal dans l'environnement de développement et le tester : le bot principal mis à jour, qui inclut désormais les nouvelles fonctionnalités ou modifications, est déployé dans l'environnement de développement. Ici, il est soumis à des tests approfondis pour s'assurer que toutes les fonctionnalités fonctionnent comme prévu.
7. Déployer le bot principal dans l'environnement de production : une fois que les tests dans l'environnement de développement sont terminés et réussis, le bot principal est déployé dans

l'environnement de production. Cette étape est la dernière étape du flux de travail, au cours de laquelle les nouvelles fonctionnalités sont mises à la disposition des utilisateurs finaux.

Automatisation et mise à l'échelle

Le flux de travail automatisé permet aux développeurs de travailler sur différentes fonctionnalités en parallèle, chacune dans des branches distinctes. Cela facilite le développement simultané, permettant aux équipes de collaborer efficacement et de fournir des fonctionnalités plus rapidement. Les branches étant isolées les unes des autres, les modifications peuvent être fusionnées et déployées sans bloquer ou interférer avec les autres travaux en cours.

Le flux de travail automatise le déploiement et la promotion des versions de bots dans différents environnements, tels que le développement, les tests et la production.

Le stockage des définitions de bots dans un système de contrôle de version tel que Git fournit une piste d'audit complète et permet une collaboration efficace. Les modifications sont suivies auprès des développeurs individuels, ce qui garantit la transparence et la responsabilité tout au long du cycle de développement. Cette approche facilite également les révisions du code, permettant aux équipes d'identifier et de résoudre les problèmes avant le déploiement en production.

En utilisant une autre AWS CodePipeline méthode Services AWS, le flux de travail automatisé peut évoluer pour s'adapter à l'augmentation des charges de travail et à la taille des équipes.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement de logiciels open source permettant de définir AWS Cloud l'infrastructure dans le code en utilisant des langages de programmation familiers et en la provisionnant via. AWS CloudFormation L'exemple d'implémentation de ce modèle utilise Python.
- AWS CDK Interface de ligne de commande (AWS CDK CLI) - Le AWS CDK kit d'outils est le principal outil d'interaction avec votre AWS CDK application. Il exécute votre application, interroge le modèle d'application que vous avez défini, produit et déploie les AWS CloudFormation modèles générés par le CDK.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS. Ce modèle est utilisé CloudFormation pour déployer les configurations du bot Amazon Lex et les ressources associées en utilisant l'infrastructure sous forme de code.

- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés. Ce modèle est utilisé CodeBuild pour créer et empaqueter les artefacts de déploiement.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles. Ce modèle est utilisé CodePipeline pour orchestrer le pipeline de livraison continue.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS via des commandes dans votre interface de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Lex V2 permet de créer Service AWS des interfaces conversationnelles (bots) pour les applications utilisant la voix et le texte.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

Autres outils

- Git est un système de contrôle de version distribué open source.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub management-framework-sample-for-amazon-lex. Le dépôt de code contient les dossiers et fichiers suivants :

- `prerequisite`dossier — Contient les définitions de CloudFormation pile (à l'aide du AWS CDK) pour configurer les ressources et les environnements requis.
- `prerequisite/lexmgmtworkflow`dossier — Répertoire principal du projet Lex Management Workflow, y compris les définitions des piles et le code Python.
- `prerequisite/tests`— Contient des tests unitaires.
- `src`dossier : répertoire du code source, y compris le wrapper de gestion des robots Amazon Lex et les utilitaires.

- `src/dialogue_lambda`— Répertoire du code source de la fonction Lambda du crochet de dialogue qui intercepte et traite les entrées des utilisateurs lors d'une conversation avec un bot Amazon Lex.

Bonnes pratiques

- Séparation des préoccupations
  - Maintenez une séparation claire des responsabilités entre DevOps les environnements de développement et de production.
  - Utilisez-les séparément Comptes AWS pour chaque environnement afin de garantir une isolation et des limites de sécurité appropriées.
  - Utilisez les rôles entre comptes et les principes du moindre privilège d'accès pour garantir un accès contrôlé entre les environnements.
- L'infrastructure en tant que code
  - Passez régulièrement en revue et mettez à jour le code de l'infrastructure pour l'aligner sur les meilleures pratiques et les exigences en constante évolution.
  - Établissez une stratégie de branchement et de fusion claire pour le référentiel de code source
- Tests et validation
  - Mettez en œuvre des tests automatisés à différentes étapes du pipeline afin de détecter les problèmes dès le début du cycle de développement.
  - Utilisez la console Amazon Lex ou des frameworks de test automatisés pour valider les configurations et les fonctionnalités des robots avant de passer à des environnements supérieurs.
  - Envisagez de mettre en place des portes d'approbation manuelles pour les déploiements dans des environnements de production ou critiques.
- Surveillance et journalisation
  - Configurez des mécanismes de surveillance et de journalisation pour les pipelines, les déploiements et les interactions entre robots.
  - Surveillez les événements du pipeline, les statuts de déploiement et les indicateurs de performance des bots pour identifier et résoudre les problèmes rapidement.
  - Utilisez les services AWS tels qu'Amazon CloudWatch et AWS X-Ray pour une journalisation et une surveillance centralisées. AWS CloudTrail

  - Passez régulièrement en revue et analysez les performances, l'efficience et l'efficacité du flux de travail automatisé.
- Sécurité et conformité
  - Mettez en œuvre des pratiques de codage sécurisées et suivez les meilleures pratiques de AWS sécurité pour le développement et le déploiement de robots Amazon Lex.
  - Passez régulièrement en revue et mettez à jour les rôles, les politiques et les autorisations IAM afin de respecter le principe du moindre privilège.
  - Envisagez d'intégrer l'analyse de sécurité et les contrôles de conformité dans les pipelines.

Épopées

Configurer iAC pour la gestion des bots Amazon Lex

Tâche	Description	Compétences requises

Configurez l'environnement CDK local.	1. Pour cloner le dépôt de ce modèle et accéder au `prerequisite` répertoire, exécutez la commande suivante :
	`git clone https://github.com/aws-samples/management-framework-sample-for-amazon-lex.git`
	`cd management-framework-sample-for-amazon-lex`
	2. Pour installer et activer l'environnement virtuel Python, exécutez la commande suivante qui installe les dépendances du CDK localement dans le
		AWS DevOps

Tâche	Description	Compétences requises

	dossier du projet, plutôt que globalement :
	
	`pip install virtualenv`
	`python<version> -m venv .venv`
	`source .venv/bin/activate`
	`python -m pip install -r requirements.txt`	

Créez un rôle multicompte dans l'`devops`environnement.	Le `devops` compte est chargé d'héberger et de gérer les CI/CD pipelines. To enable the CI/CD pipelines permettant d'interagir avec les `prod` environnements `dev` et. Exécutez les commandes suivantes pour créer un rôle multi-comptes dans le `devops` compte.
	
	`cdk bootstrap --profile=devops`
	
	`cdk deploy LexMgmtDevopsRoleStack -c dev-account-id=222222222222 -c prod-account-id=333333333333 --profile=devops`
		AWS DevOps

Tâche	Description	Compétences requises

Créez un rôle multicompte dans l'`dev`environnement.	Créez un rôle IAM dans le `dev` compte avec les autorisations nécessaires pour permettre au `devops` compte d'assumer ce rôle. Le pipeline CI/CD utilise ce rôle pour effectuer des actions dans le `dev` compte, telles que le déploiement et la gestion des ressources du bot Amazon Lex.
	
	Pour créer le rôle IAM, exécutez les commandes suivantes :
	
	`cdk bootstrap --profile =dev`
	
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=dev`
		AWS DevOps

Tâche	Description	Compétences requises

Créez un rôle multicompte dans l'`prod`environnement.	Créez un rôle IAM dans le `prod` compte avec les autorisations nécessaires pour permettre au `devops` compte d'assumer ce rôle. Le pipeline CI/CD utilise ce rôle pour effectuer des actions dans le `prod` compte, telles que le déploiement et la gestion des ressources du bot Amazon Lex.
	`cdk bootstrap --profile =prod`
	`cdk deploy LexMgmtCr ossaccountRoleStac k -c devops-account- id=1111111111111 -- profile=prod`
		AWS DevOps

Créez des pipelines dans l'`devops`environnement.	Pour gérer le flux de travail de développement des robots Amazon Lex, exécutez la commande suivante pour configurer des pipelines dans l'`devops`environnement. `cdk deploy LexMgmtWo rkflowStack -c devops- account-id=111111111 1111 -c dev-account- id=2222222222222 -c prod-account-id=33 3333333333 --profile =devops`	AWS DevOps

Établir la base de référence pour le bot principal

Tâche	Description	Compétences requises
Définissez la version initiale du bot principal.	Pour définir la version initiale du bot principal, déclenchez le `BaselineBotPipeline` pipeline. Le pipeline déploie la définitio n de bot de base définie dans le CloudFormation modèle, exporte la définition principale du bot sous forme de fichiers .json et stocke le code du bot principal dans un système de contrôle de version.	AWS DevOps

Mettre en œuvre le flux de travail de développement des fonctionnalités

Tâche	Description	Compétences requises
Créez le bot de tickets pour développer et tester une fonctionnalité.	`TicketBot` est une nouvelle instance de bot importée à partir de la définition de bot principale existante dans la branche de fonctionnalités. Cette approche garantit que le nouveau bot dispose de toutes les fonctionnalités et configura tions actuelles du bot principal. Pour définir la version initiale du bot de tickets, déclenchez le `CreateTicketBotPip eline` pipeline.	Développeur Lex Bot

Tâche	Description	Compétences requises
	Le pipeline crée une nouvelle branche de fonctionnalités dans le système de contrôle de version et crée une nouvelle instance de bot de tickets basée sur le bot principal.	
Développez et testez la fonctionnalité Ticket Bot.	Pour développer et tester cette fonctionnalité, connectez-vous à la console Amazon Lex AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lex/. Pour plus d'informations, consultez Tester un bot à l'aide de la console dans la documentation Amazon Lex. Avec l'`TicketBot` instance, vous pouvez désormais ajouter, modifier ou étendre les fonctionnalités du bot pour implémenter la nouvelle fonctionnalité. Par exemple, vous pouvez créer ou modifier des intentions, des énoncés, des créneaux et des flux de dialogue. Pour plus d'informations, consultez la section Ajouter des intentions dans la documentation Amazon Lex.	Développeur Lex Bot

Tâche	Description	Compétences requises
Exportez la définition du bot de tickets.	La définition du bot exportée est essentiellement une représentation de la configuration et des fonctionnalités du bot au format JSON. Pour exporter la définition du bot de tickets, déclenchez le `ExportTicketBotPipeline` pipeline. Le pipeline exporte la définition du bot de ticket sous forme de fichiers .json et stocke le code du bot de ticket dans une branche de fonctionnalité du système de contrôle de version.	Développeur Lex Bot

Tâche	Description	Compétences requises
Rebasez la branche de fonctionnalités à partir de la dernière branche principale.	Au cours du développement d'une nouvelle fonctionnalité, la branche principale peut avoir reçu d'autres modificat ions de la part de différents développeurs ou équipes. Pour intégrer ces modificat ions dans la branche des fonctionnalités, effectuez une `rebase` opération Git. Cette opération reproduit essentiel lement les validations de la branche de fonctionnalités en plus des dernières validatio ns de la branche principal e, garantissant ainsi que la branche de fonctionnalités inclut toutes les dernières modifications	Développeur Lex Bot

Tâche	Description	Compétences requises
Importez et validez le bot de tickets rebasé.	Après avoir rebasé la branche de fonctionnalités, vous devez l'importer dans l'instance du bot de tickets. Cette importation met à jour le bot de tickets existant avec les dernières modifications apportées par la branche rebasée. Pour importer le bot de tickets rebasé, déclenchez le `ImportTicketBotPipeline` pipeline. Le pipeline importe les fichiers .json de définition du bot ticket situés dans la branche des fonctionnalités du système de contrôle de version dans l'`TicketBot` instance.	Développeur Lex Bot

Tâche	Description	Compétences requises
Validez la définition du bot rebasée.	Après avoir importé la définitio n du bot rebasée, il est essentiel de valider ses fonctionnalités. Vous devez vous assurer que la nouvelle fonctionnalité fonctionn e comme prévu et qu'elle n'entre pas en conflit avec les fonctionnalités existantes. Cette validation implique généralement de tester le bot avec différents scénarios d'entrée, de vérifier les réponses et de vérifier que le bot se comporte comme prévu. Vous pouvez effectuer la validation de l'une des manières suivantes : • Testez le bot manuellem ent à l'aide de la console Amazon Lex. • Utilisez une approche automatisée en utilisant des cadres de test et des outils capables de simuler les interactions des utilisateurs et d'affirmer les réponses attendues.	Développeur Lex Bot

Tâche	Description	Compétences requises
Fusionnez la branche de fonction dans la branche principale.	Après avoir développé et testé la nouvelle fonctionnalité dans l'`TicketBot` instance isolée, procédez comme suit : 1. Apportez les modifications à la branche de fonctionn alité correspondante dans le système de contrôle de version. 2. Pour fusionner la branche de fonctionnalité avec la branche principale, créez une pull request (PR). Ce PR sert de demande pour examiner et intégrer les modifications dans la base de code principale.	Développeur Lex Bot, administrateur de référentiels

Tâche	Description	Compétences requises
Supprimez la branche de fonctionnalités et le bot de tickets.	Une fois qu'une branche de fonctionnalités a été fusionnée avec succès dans la branche principale, supprimez la branche de fonctionnalités et le bot de tickets du référentiel de code source. Pour supprimer la branche de fonctionnalités et le bot de tickets, déclenchez le `DeleteTicketBotPipeline` pipeline. Le pipeline supprime les ressources temporaires du bot créées au cours du processus de développement (par exemple, le bot de tickets). Cette action permet de maintenir un dépôt propre et d'éviter toute confusion ou tout conflit avec les futures branches de fonctionnalités.	Développeur Lex Bot

Maintenir le bot principal

Tâche	Description	Compétences requises
Importez la dernière définition du bot principal dans l'`dev`environnement.	Pour importer la dernière définition du bot principal de la branche principale dans l'`dev`environnement, déclenchez le `DeployBotDevPipeline` pipeline.	AWS DevOps

Tâche	Description	Compétences requises
	Le pipeline crée également une balise git lors de l'approbation.	
Importez la dernière définition du bot principal dans l'`prod`environnement.	Pour importer dans l'`prod`environnement la dernière définition de bot de la branche principale, fournissez la référence de balise de la tâche précédente en tant que paramètre et déclenchez le `DeployBotProdPipeline` pipeline. Le pipeline importe la dernière définition de bot d'une balise spécifique dans l'`prod`environnement.	AWS DevOps

Résolution des problèmes

Problème	Solution
Lorsque vous déployez des robots Amazon Lex sur différents comptes Comptes AWS, les services d'outillage doivent disposer des autorisations nécessaires pour accéder aux ressources de ces comptes.	Pour accorder un accès entre comptes, utilisez les rôles et les politiques IAM. Créez des rôles IAM dans les comptes cibles et associez des politiques aux rôles qui accordent les autorisations requises. Ensuite, assumez ces rôles depuis le compte sur lequel le bot Amazon Lex est déployé. Pour plus d'informations, consultez les sections Autorisations IAM requises pour importer et Autorisations IAM requises pour exporter des

Problème	Solution
	robots dans Lex V2 dans la documentation Amazon Lex.

Ressources connexes

- Importation de robots dans Amazon Lex V2
- Démarrez un pipeline dans CodePipeline
- Utilisation des robots Amazon Lex V2

Automatisez le déploiement d'ensembles de piles à l'aide d'AWS CodePipeline et d'AWS CodeBuild

Créée par Thiyagarajan Mani (AWS), Mihir Borkar (AWS) et Raghu Gowda (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Dans le cadre de votre solution d'intégration et de livraison continues (CI/CD) processes, you might want to deploy applications automatically into all your existing AWS accounts and into new accounts that you add to your organization in AWS Organizations. When you architect a CI/CDsolution pour répondre à cette exigence), la fonction d'administrateur délégué d'AWS CloudFormation est utile car elle fournit un niveau de sécurité en restreignant l'accès au compte de gestion. AWS CodePipeline utilise toutefois le modèle d'autorisations gérées par les services pour déployer des applications sur plusieurs comptes et régions. Vous devez utiliser le compte de gestion AWS Organizations pour effectuer un déploiement avec des ensembles de piles, car AWS CodePipeline ne prend pas en charge la fonctionnalité d'administrateur délégué des ensembles de piles.

Ce modèle décrit comment contourner cette limitation. Le modèle utilise AWS CodeBuild et un script personnalisé pour automatiser le déploiement d'ensembles de piles avec AWS CodePipeline. Il automatise les activités de déploiement d'applications suivantes :

- Déployer une application sous forme d'ensembles de piles dans des unités organisationnelles existantes (OUs)
- Étendre le déploiement d'une application à OUs d'autres régions
- Supprimer une application déployée de toutes les applications ou de certaines OUs régions

Conditions préalables et limitations

Prérequis

Avant de suivre les étapes de ce modèle :

- Créez des organisations dans votre compte de gestion AWS Organizations. Pour obtenir des instructions, consultez la documentation d'AWS Organizations.

- Activez un accès sécurisé entre AWS Organizations et utilisez CloudFormation des autorisations gérées par les services. Pour obtenir des instructions, consultez la section Activer l'accès sécurisé avec AWS Organizations dans la CloudFormation documentation.

Limites

Le code fourni avec ce modèle présente les limites suivantes :

- Vous ne pouvez déployer qu'un seul CloudFormation modèle pour une application ; le déploiement de plusieurs modèles n'est actuellement pas pris en charge.
- La personnalisation de la mise en œuvre actuelle nécessite de l' DevOps expertise.
- Ce modèle n'utilise pas les clés du système de gestion des clés AWS (AWS KMS). Toutefois, vous pouvez activer cette fonctionnalité en reconfigurant le CloudFormation modèle inclus dans ce modèle.

Architecture

Cette architecture pour le pipeline de déploiement CI/CD gère les opérations suivantes :

- Limite l'accès direct au compte de gestion en déléguant la responsabilité du déploiement du stack set à un compte CI/CD dédié en tant qu'administrateur du stack set pour les déploiements d'applications.
- Utilise le modèle d'autorisation géré par le service pour déployer l'application automatiquement chaque fois qu'un nouveau compte est créé et mappé sous une unité d'organisation.
- Garantit la cohérence des versions des applications sur tous les comptes au niveau de l'environnement.
- Utilise plusieurs étapes d'approbation au niveau du référentiel et du pipeline pour fournir des niveaux supplémentaires de sécurité et de gouvernance à l'application déployée.
- Surmonte la limite actuelle CodePipeline en utilisant un script de déploiement personnalisé pour déployer ou CodeBuild supprimer automatiquement des ensembles de piles et des instances de pile. Pour une illustration du contrôle du flux et de la hiérarchie des appels d'API implémentés par le script personnalisé, consultez la section Informations supplémentaires.
- Crée des ensembles de piles individuels pour les environnements de développement, de test et de production. En outre, vous pouvez créer des ensembles de piles combinant plusieurs OUs régions

à chaque étape. Par exemple, vous pouvez combiner sandbox et développement OUs dans le cadre d'une phase de développement et de déploiement.

- Prend en charge le déploiement ou l'exclusion d'applications dans un sous-ensemble de comptes ou une liste de OUs comptes.

Automatisation et mise à l'échelle

Vous pouvez utiliser le code fourni avec ce modèle pour créer un CodeCommit référentiel AWS et un pipeline de code pour votre application. Vous pouvez ensuite les déployer sous forme de stack sets sur plusieurs comptes au niveau de l'unité d'organisation. Le code automatise également des composants tels que les rubriques Amazon Simple Notification Service (Amazon SNS) destinées à informer les approbateurs, les rôles AWS Identity and Access Management (IAM) requis et la politique de contrôle des services (SCP) à appliquer au compte de gestion.

Outils

Services AWS

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur les comptes et les régions AWS.
- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS CodeDeploy automatise les déploiements vers Amazon Elastic Compute Cloud EC2 (Amazon) ou des instances sur site, les fonctions AWS Lambda ou les services Amazon Elastic Container Service (Amazon ECS).
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS Organizations est un service de gestion de comptes qui vous aide à consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub automated-code-pipeline-stackset-deployment. Pour la structure des dossiers et d'autres informations, consultez le fichier readme du référentiel.

Bonnes pratiques

Ce modèle restreint l'accès direct au compte de gestion lors du déploiement de l'application au niveau de l'unité d'organisation. L'ajout de plusieurs étapes d'approbation au processus de pipeline et de référentiel permet de renforcer la sécurité et la gouvernance des applications et des composants que vous déployez en utilisant cette approche.

Épopées

Configuration de comptes dans AWS Organizations

Tâche	Description	Compétences requises
Activez toutes les fonctionn alités du compte de gestion.	Activez toutes les fonctionn alités du compte de gestion de votre organisation en suivant les instructions de la documentation AWS Organizations.	Administrateur AWS, administr ateur de plateforme
Créez un compte CI/CD.	Dans AWS Organizations, dans votre organisation, créez un compte CI/CD dédié et désignez une équipe chargée de détenir et de contrôler l'accès au compte.	Administrateur AWS
Ajoutez un administrateur délégué.	Dans le compte de gestion, enregistrez le compte CI/CD que vous avez créé à l'étape précédente en tant qu'admini strateur délégué du stack set. Pour obtenir des instructions,	Administrateur AWS, administr ateur de plateforme

Tâche	Description	Compétences requises
	consultez la CloudFormation documentation AWS.	

Création d'un référentiel d'applications et d'un pipeline CI/CD

Tâche	Description	Compétences requises
Clonez le référentiel de code.	1. Clonez le référentiel de code fourni avec ce modèle sur votre ordinateur : `git clone https://github.com/aws-samples/automated-code-pipeline-stackset-deployment.git` 2. Consultez le fichier readme pour comprendre la structure du répertoire et d'autres détails.	AWS DevOps
Créez des rubriques SNS.	Vous pouvez utiliser le `sns-template.yaml` modèle fourni dans le GitHub référentiel pour créer des rubriques SNS et configurer des abonnements pour les demandes d'approbation. 1. Sur la console AWS, connectez-vous au compte CI/CD. 2. Ouvrez la CloudFormation console à l'adresse https://	AWS DevOps

Tâche	Description	Compétences requises
	console.aws.amazon.com/cloudformation. 3. Créez une nouvelle pile avec de nouvelles ressources (option standard). 4. Pour Spécifier le modèle, choisissez Télécharger un fichier modèle, Choisir un fichier, puis sélectionnez le `sns-template.yaml` fichier `templates` dans le dossier du GitHub référentiel cloné. Choisissez Suivant. 5. Fournissez un nom de pile d'applications significatif. 6. Spécifiez un préfixe pour les ressources. 7. Choisissez Next, Next et Submit. 8. Lorsque la pile a été créée avec succès, choisissez l'onglet Outputs et notez les Amazon Resource Names (ARNs) des rubriques SNS relatives aux pull requests, à l'environnement de test et à l'environnement de production. Vous utiliserez ces informations dans les étapes suivantes.	

Tâche	Description	Compétences requises
Créez des rôles IAM pour les composants CI/CD.	Vous pouvez utiliser le `cicd-role-template.yaml` modèle fourni dans le GitHub référentiel pour créer les rôles et les politiques IAM requis par les composants CI/CD. 1. Sur la console AWS, connectez-vous au compte CI/CD. 2. Ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation. 3. Créez une nouvelle pile avec de nouvelles ressources (option standard). 4. Pour Spécifier le modèle, choisissez Télécharger un fichier modèle, Choisir un fichier, puis sélectionnez le `cicd-role-template.yaml` fichier `templates` dans le dossier du GitHub référentiel cloné. Choisissez Suivant. 5. Fournissez un nom de pile d'applications significatif. 6. Entrez des valeurs pour les paramètres suivants : • L'ARN de la politique de limite d'autorisation. Vous pouvez obtenir	AWS DevOps

Tâche	Description	Compétences requises
	cet ARN dans la section Détails de la politique de votre politique de limites d'autorisations sur la console IAM. • L'ARN de la rubrique d'approbation de production SNS que vous avez mentionnée précédemment. • L'ARN du sujet d'approbation des tests SNS que vous avez indiqué précédemment. • Préfixe pour les ressources créées par le modèle. 7. Choisissez Next, Next et Submit. 8. Lorsque la pile a été créée avec succès, choisissez l'onglet Sorties et notez les ARNs rôles IAM qui ont été créés. Vous utiliserez ces informations dans les étapes suivantes.	

Tâche	Description	Compétences requises
Créez un CodeCommit référentiel et un pipeline de code pour votre application.	Vous pouvez utiliser le `cicd-pipeline-template.yaml` modèle fourni dans le GitHub référentiel pour créer un CodeCommit référentiel et un pipeline de code pour votre application. 1. Sur la console AWS, connectez-vous au compte CI/CD. 2. Ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation. 3. Créez une nouvelle pile avec de nouvelles ressources (option standard). 4. Pour Spécifier le modèle, choisissez Télécharger un fichier modèle, Choisir un fichier, puis sélectionnez le `cicd-pipeline-template.yaml` fichier `templates` dans le dossier du GitHub référentiel cloné. Choisissez Suivant. 5. Fournissez un nom de pile d'applications significatif. 6. Entrez des valeurs pour les paramètres suivants :	AWS DevOps

Tâche	Description	Compétences requises
	• AppRepositoryName— Nom du CodeCommit référentiel qui sera créé pour l'application. • AppRepositoryDescription— Brève description du CodeCommit référentiel qui sera créé pour l'application. • ApplicationName— Le nom de votre application. Cette chaîne est utilisée comme nom du CodeCommit dépôt et comme préfixe du pipeline CI/CD. • CloudWatchEventRoleARN — L'ARN du rôle d'CloudWatch événement de la tâche précédente. • CodeBuildProjectRoleARN — L'ARN du rôle de CodeBuild projet associé à la tâche précédente. • CodePipelineRoleARN — L'ARN du CodePipeline rôle de la tâche précédente. • DeploymentConfigBucket— Le nom du compartiment Amazon Simple Storage Service	

Tâche	Description	Compétences requises
	(Amazon S3) dans lequel les fichiers de configuration de déploiement et le fichier de script .zip seront stockés. • DeploymentConfigKey— Le chemin et le nom de fichier .zip (clé Amazon S3). • PRApprovalSNSARN — L'ARN de la rubrique SNS pour les notifications de pull request. • ProdApprovalSNSARN — L'ARN de la rubrique SNS pour les approbations de production. • TESTApprovalSNSARN — L'ARN de la rubrique SNS pour les approbations de test. • TemplateBucket— Le nom du compartiment S3 dans le modèle de création du CI/CD account where the CI/CD pipeline sera enregistré. 7. Choisissez Next, Next et Submit. 8. Lorsque la pile est terminée avec succès, elle crée un CodeCommit référentiel portant le nom spécifié et	

Tâche	Description	Compétences requises
	une structure de répertoire par défaut, des fichiers de configuration de déploiement, des scripts et un pipeline de code pour le référentiel.	

Déployer un ensemble de piles

Tâche	Description	Compétences requises
Clonez le référentiel d'applications.	Le modèle de pipeline CI/CD que vous avez utilisé précédemment crée un exemple de référentiel d'applications et de pipeline de code. Pour cloner et vérifier le référentiel : 1. Connectez-vous au compte CI/CD. 2. Trouvez le référentiel d'applications et le pipeline CI/CD que vous avez créés dans l'épopée précédente. 3. Copiez l'URL du dépôt et utilisez la commande git clone pour cloner le dépôt sur votre machine locale. 4. Vérifiez que la structure du répertoire et les fichiers correspondent aux éléments suivants : `root`	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises

	<pre>|- deploy_configs
	| |- deployment_config.json
	|- parameters
	| |- template-parameter-dev.json
	| |- template-parameter-test.json
	| |- template-parameter-prod.json
	|- templates
	| |- template.yml
	|- buildspec.yml</pre> où le `deploy_configs` dossier contient le fichier de configuration du déploiement et les `parameters` dossiers `templates` et incluent les fichiers par défaut que vous remplacerez par vos propres fichiers de CloudFormation modèles et de paramètres.
	
	⚠ Important
	Ne personnalisez pas la structure des dossiers.
	
	5. Créez une branche de fonctionnalités.	

Tâche	Description	Compétences requises
Ajoutez des artefacts d'application.	Mettez à jour le référentiel d'applications à l'aide d'un CloudFormation modèle. **Note** Cette solution prend en charge le déploiement d'un seul CloudFormation modèle. 1. Créez votre CloudFormation modèle pour déployer les modifications du code de votre application et nommez-le `<application-name>.yaml` . 2. Remplacez le `template.yml` fichier dans le `templates` dossier du référentiel de l'application par le CloudFormation modèle que vous avez créé à l'étape 1. 3. Préparez des fichiers de paramètres pour chaque environnement (développement, test et production). 4. Nommez les fichiers de paramètres en utilisant le format `<cloudformation-template-na`	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises
	me>-parameter-<environment-name>.json . 5. Remplacez les fichiers de paramètres par défaut du parameters dossier par les fichiers de l'étape 4.	

Tâche	Description	Compétences requises
Mettez à jour le fichier de configuration de déploiement.	Mettez à jour le `deploymen t_config.json` fichier : 1. Dans le référentiel de l'application, accédez au `deploy_configs` dossier. 2. Ouvrez le fichier `deployment_config. json` : `{ "deployme nt_action": "<deploy/delete>", "stack_set_name": "<stack set name>", "stack_se t_desciption": "<stack set descripti on>", "deployme nt_targets": { "dev": { "org_units": ["list of OUs"], "regions": ["list of regions"], "filter_accounts": ["list of accounts" ],`	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises

	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"test": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],
	"filter_accounts": ["list of accounts"],
	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	},
	"prod": {
	"org_units": ["list of OUs"],
	"regions": ["list of regions"],	

Tâche	Description	Compétences requises

	<pre>"filter_accounts": ["list of accounts"],
	
	"filter_type": "<DIFFERENCE/INTERSECTION/UNION>"
	}
	
	},
	"cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
	"auto_deployement": "<True/False>",
	"retain_stacks_on_account_removal": "<True/False>",
	"region_deployment_concurrency": "<SEQUENTIAL/PARALLEL>"
	}</pre> 3. Mettez à jour les valeurs de l'action de déploiement, du nom de l'ensemble de piles, de la description de l'ensemble de piles et des cibles de déploiement.
	
	Par exemple, vous pouvez définir sur `deploymen t_action delete` pour	

Tâche	Description	Compétences requises
	supprimer l'ensemble de piles dans son intégralité et ses instances de pile associées. `deploy`À utiliser pour créer un nouvel ensemble de piles, pour mettre à jour un ensemble de piles existant ou pour ajouter ou supprimer des instances de pile pour des régions OUs ou des régions supplémentaires. Pour plus d'exemples, consultez la section Informations supplémentaires. Ce modèle crée des ensembles de piles individuels pour chaque environnement en ajoutant le nom de l'environnement au nom du stack set que vous fournissez dans le fichier de configuration de déploiement.	

Tâche	Description	Compétences requises
Validez les modifications et déployez le stack set.	Validez les modifications que vous avez spécifiées dans votre modèle d'application, puis fusionnez et déployez le stack set dans plusieurs environnements étape par étape : 1. Enregistrez tous vos fichiers et validez les modificat ions dans la branche des fonctionnalités de votre référentiel d'applications local. 2. Transférez la branche de fonctionnalités vers le référentiel distant. 3. Créez une pull request pour fusionner les modifications apportées à la branche principale. Lorsque la pull request a été approuvée et que les modifications ont été fusionnées dans la branche principale, le pipeline CI/CD sera lancé. 4. Lorsque l'étape de déploiement du développe ment est terminée avec succès, consultez l'onglet Service-Managed de la	Développeur d'applications, ingénieur de données

Tâche	Description	Compétences requises
	CloudFormation console. StackSets Vous verrez un nouveau set de piles avec le suffixe`dev`. 5. Consultez les CodeBuild journaux de la phase de déploiement du développement pour détecter tout problème. 6. Déployez le stack set dans les environnements de test et de production en demandant à vos approbateurs d'approuver les déploiements pour ces étapes et en répétant les étapes 5 et 6. Les ensembles de piles pour les environnements de test et de production portent les suffixes `test` et. `prod`	

Résolution des problèmes

Problème	Solution
Le déploiement échoue à l'exception suivante : Changez le nom du fichier de paramètres du modèle en -parameter- .json avec, les noms par défaut ne sont pas autorisés <application name><evn>	Les fichiers CloudFormation de paramètres du modèle doivent respecter la convention de dénomination spécifiée. Mettez à jour les noms des fichiers de paramètres et réessayez.

Problème	Solution
Le déploiement échoue à l'exception suivante : Changez le nom du CloudFormation modèle en .yml, les modèles par défaut .yml ou template.yaml ne sont pas autorisés <application name>	Le nom du CloudFormation modèle doit respecter la convention de dénomination spécifiée. Mettez à jour le nom du fichier et réessayez.
Le déploiement échoue à l'exception suivante : Aucun CloudFormation modèle valide et son fichier de paramètres n'ont été trouvés pour l'environnement {nom de l'environnement}	Vérifiez les conventions de dénomination des fichiers pour le CloudFormation modèle et son fichier de paramètres pour l'environnement spécifié.
Le déploiement échoue à l'exception suivante : Action de déploiement non valide fournie dans le fichier de configuration de déploiement. Les options valides sont « déployer » et « supprimer ».	Vous avez spécifié une valeur non valide pour le `deployment_action` paramètre dans le fichier de configuration de déploiement. Le paramètre possède deux valeurs valides : `deploy` et`delete`. `deploy`À utiliser pour créer et mettre à jour les ensembles de piles et leurs instances de pile associées. À utiliser `delete` uniquement lorsque vous souhaitez supprimer l'ensemble complet de piles et les instances de pile associées.

Ressources connexes

- GitHub automated-code-pipeline-stackset-référentiel de déploiement
- Activation de toutes les fonctionnalités de votre organisation (documentation AWS Organizations)
- Enregistrer un administrateur délégué (CloudFormation documentation AWS)
- Objectifs au niveau du compte pour les Stack Sets gérés par des services (documentation AWS CloudFormation)

Informations supplémentaires

Organigramme

L'organigramme suivant décrit le contrôle du flux et la hiérarchie des appels d'API mis en œuvre par le script personnalisé pour automatiser le déploiement des ensembles de piles.

Exemples de fichiers de configuration de déploiement

Création d'un nouvel ensemble de piles

Le fichier de configuration de déploiement suivant crée un nouvel ensemble de piles appelé `sample-stack-set` dans la région AWS `us-east-1` en trois OUs.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                          },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Déploiement d'un ensemble de piles existant sur une autre unité d'organisation

Si vous déployez la configuration illustrée dans l'exemple précédent et que vous souhaitez déployer le stack set sur une unité d'organisation supplémentaire appelée `dev-org-unit-2` dans l'environnement de développement, le fichier de configuration de déploiement peut ressembler à ce qui suit.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                             "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Déploiement d'un ensemble de piles existant dans une autre région AWS

Si vous déployez la configuration illustrée dans l'exemple précédent et que vous souhaitez déployer le stack set dans une région AWS supplémentaire (`us-east-2`) dans l'environnement de développement pour deux OUs (`dev-org-unit-1`et`dev-org-unit-2`), le fichier de configuration de déploiement peut ressembler à ce qui suit.

> **Note**
>
> Les ressources du CloudFormation modèle doivent être valides et spécifiques à la région.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                             "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                             "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Suppression d'une instance de pile d'une unité d'organisation ou d'une région AWS

Supposons que la configuration de déploiement présentée dans l'exemple précédent ait été déployée. Le fichier de configuration suivant supprime les instances de pile des deux régions de l'unité d'organisation`dev-org-unit-2`.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1", "us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                           },
     "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
     "auto_deployement": "True",
     "retain_stacks_on_account_removal": "True",
     "region_deployment_concurrency": "PARALLEL"
 }
```

Le fichier de configuration suivant supprime l'instance de pile de la région AWS `us-east-1` pour les deux OUs dans l'environnement de développement.

```
{
     "deployment_action": "deploy",
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
```

```
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                            },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
 }
```

Supprimer l'ensemble complet de piles

Le fichier de configuration de déploiement suivant supprime l'ensemble de piles et toutes les instances de pile associées.

```
{
     "deployment_action": “delete”,
     "stack_set_name": "sample-stack-set",
     "stack_set_desciption": "this is a sample stack set",
    "deployment_targets": {
                                "dev": {
                                        "org_units": ["dev-org-unit-1", "dev-org-
unit-2"],
                                        "regions": ["us-east-2"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                                "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
```

```
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
                           },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Exclure un compte du déploiement

Le fichier de configuration de déploiement suivant exclut le compte`111122223333`, qui fait partie de l'unité d'`dev-org-unit-1`organisation, du déploiement.

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                    "org_units": ["dev-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": ["111122223333"],
                                    "filter_type": "DIFFERENCE"
                                },
                            "test": {
                                    "org_units": ["test-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                },
                            "prod": {
                                    "org_units": ["prod-org-unit-1"],
                                    "regions": ["us-east-1"],
                                    "filter_accounts": [],
                                    "filter_type": ""
                                }
```

```
                        },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Déploiement de l'application sur un sous-ensemble de comptes dans une unité d'organisation

Le fichier de configuration de déploiement suivant déploie l'application sur trois comptes uniquement (111122223333,444455556666, et777788889999) de l'unité d'organisation. `dev-org-unit-1`

```
{
    "deployment_action": "deploy",
    "stack_set_name": "sample-stack-set",
    "stack_set_desciption": "this is a sample stack set",
   "deployment_targets": {
                            "dev": {
                                        "org_units": ["dev-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": ["111122223333",
"444455556666", "777788889999"],
                                        "filter_type": "INTERSECTION"
                                    },
                            "test": {
                                        "org_units": ["test-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    },
                            "prod": {
                                        "org_units": ["prod-org-unit-1"],
                                        "regions": ["us-east-1"],
                                        "filter_accounts": [],
                                        "filter_type": ""
                                    }
                        },
    "cft_capabilities": ["CAPABILITY_IAM", "CAPABILITY_NAMED_IAM"],
    "auto_deployement": "True",
    "retain_stacks_on_account_removal": "True",
    "region_deployment_concurrency": "PARALLEL"
}
```

Associez automatiquement une politique gérée par AWS pour Systems Manager aux profils d' EC2 instance à l'aide de Cloud Custodian et d'AWS CDK

Créée par Ali Asfour (AWS) et Aaron Lennon (AWS)

Récapitulatif

Vous pouvez intégrer des instances Amazon Elastic Compute Cloud (Amazon EC2) à AWS Systems Manager pour automatiser les tâches opérationnelles et améliorer la visibilité et le contrôle. Pour s'intégrer à Systems Manager, EC2 les instances doivent disposer d'un agent AWS Systems Manager (agent SSM) installé et d'une politique `AmazonSSMManagedInstanceCore` AWS Identity and Access Management (IAM) attachée à leurs profils d'instance.

Toutefois, si vous voulez vous assurer que la `AmazonSSMManagedInstanceCore` politique est attachée à tous les profils d' EC2 instance, vous pouvez avoir des difficultés à mettre à jour les nouvelles EC2 instances qui n'ont pas de profil d'instance ou les EC2 instances qui ont un profil d'instance mais qui n'ont pas cette `AmazonSSMManagedInstanceCore` politique. Il peut également être difficile d'appliquer cette politique à plusieurs comptes Amazon Web Services (AWS) et à plusieurs régions AWS.

Ce modèle permet de résoudre ces problèmes en déployant trois politiques Cloud Custodian dans vos comptes AWS :

- La première politique Cloud Custodian vérifie les EC2 instances existantes qui ont un profil d'instance mais qui n'ont pas cette `AmazonSSMManagedInstanceCore` politique. La `AmazonSSMManagedInstanceCore` politique est ensuite jointe.
- La deuxième politique Cloud Custodian vérifie les EC2 instances existantes sans profil d'instance et ajoute un profil d'instance par défaut auquel la `AmazonSSMManagedInstanceCore` politique est attachée.
- La troisième politique Cloud Custodian crée des fonctions AWS Lambda dans vos comptes afin de surveiller la création d'instances et EC2 de profils d'instance. Cela garantit que la `AmazonSSMManagedInstanceCore` politique est automatiquement attachée lors de la création d'une EC2 instance.

Ce modèle utilise les DevOps outils AWS pour réaliser un déploiement continu et à grande échelle des politiques Cloud Custodian dans un environnement multi-comptes, sans mettre en place un environnement de calcul distinct.

Conditions préalables et limitations

Prérequis

- Deux comptes AWS actifs ou plus. L'un des comptes est le compte de sécurité et les autres sont des comptes de membres.
- Autorisations permettant de fournir des ressources AWS dans le compte de sécurité. Ce modèle utilise des autorisations d'administrateur, mais vous devez accorder des autorisations conformément aux exigences et aux politiques de votre organisation.
- Possibilité d'assumer un rôle IAM, du compte de sécurité aux comptes des membres, et de créer les rôles IAM requis. Pour plus d'informations à ce sujet, consultez la section Déléguer l'accès entre les comptes AWS à l'aide de rôles IAM dans la documentation IAM.
- **Important**

  Interface de ligne de commande AWS (AWS CLI), installée et configurée. À des fins de test, vous pouvez configurer l'AWS CLI à l'aide de la `aws configure` commande ou en définissant des variables d'environnement. : Cela n'est pas recommandé pour les environnements de production et nous recommandons de n'accorder à ce compte que l'accès avec le moindre privilège. Pour plus d'informations à ce sujet, consultez la section Accorder le moindre privilège dans la documentation IAM.
- Le `devops-cdk-cloudcustodian.zip` fichier (joint), téléchargé sur votre ordinateur local.
- Connaissance de Python.
- Les outils requis (Node.js, AWS Cloud Development Kit (AWS CDK) et Git) sont installés et configurés. Vous pouvez utiliser le `install-prerequisites.sh` fichier qu'il `devops-cdk-cloudcustodian.zip` contient pour installer ces outils. Assurez-vous d'exécuter ce fichier avec les privilèges root.

Limites

- Bien que ce modèle puisse être utilisé dans un environnement de production, assurez-vous que tous les rôles et politiques IAM répondent aux exigences et aux politiques de votre organisation.

Versions du package

- Cloud Custodian version 0.9 ou ultérieure
- TypeScript version 3.9.7 ou ultérieure
- Node.js version 14.15.4 ou ultérieure
- npmversion 7.6.1 ou ultérieure
- AWS CDK version 1.96.0 ou ultérieure

Architecture

Le schéma suivant illustre le flux de travail suivant :

1. Les politiques Cloud Custodian sont transférées vers un CodeCommit référentiel AWS dans le compte de sécurité. Une règle Amazon CloudWatch Events lance automatiquement le CodePipeline pipeline AWS.
2. Le pipeline récupère le code le plus récent CodeCommit et l'envoie à la partie d'intégration continue du pipeline d'intégration continue et de livraison continue (CI/CD) géré par AWS. CodeBuild
3. CodeBuild exécute les DevSecOps actions complètes, y compris la validation de la syntaxe des politiques sur les politiques Cloud Custodian, et exécute ces politiques en `--dryrun` mode pour vérifier quelles ressources sont identifiées.
4. S'il n'y a aucune erreur, la tâche suivante invite un administrateur à examiner les modifications et à approuver le déploiement dans les comptes des membres.

Pile technologique

- AWS CDK
- CodeBuild
- CodeCommit
- CodePipeline
- IAM
- Cloud Custodian

Automatisation et mise à l'échelle

Le module AWS CDK pipelines fournit un pipeline CI/CD qui permet d' CodePipeline orchestrer la création et le test du code source CodeBuild, en plus du déploiement de ressources AWS avec AWS stacks. CloudFormation Vous pouvez utiliser ce modèle pour tous les comptes membres et toutes les régions de votre organisation. Vous pouvez également étendre la `Roles creation` pile pour déployer d'autres rôles IAM dans vos comptes membres.

Outils

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel permettant de définir l'infrastructure cloud dans le code et de la provisionner via AWS. CloudFormation
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS à l'aide de commandes dans votre shell de ligne de commande.
- AWS CodeBuild est un service de création entièrement géré dans le cloud.
- AWS CodeCommit est un service de contrôle de version que vous pouvez utiliser pour stocker et gérer des actifs de manière privée.
- AWS CodePipeline est un service de livraison continue que vous pouvez utiliser pour modéliser, visualiser et automatiser les étapes nécessaires à la publication de votre logiciel.
- AWS Identity and Access Management est un service Web qui vous permet de contrôler en toute sécurité l'accès aux ressources AWS.
- Cloud Custodian est un outil qui réunit les dizaines d'outils et de scripts que la plupart des entreprises utilisent pour gérer leurs comptes de cloud public en un seul outil open source.
- Node.js est un JavaScript environnement d'exécution basé sur le JavaScript moteur V8 de Google Chrome.

Code

Pour une liste détaillée des modules, des fonctions de compte, des fichiers et des commandes de déploiement utilisés dans ce modèle, consultez le `README` fichier dans le `devops-cdk-cloudcustodian.zip` fichier (joint).

Épopées

Configuration du pipeline avec AWS CDK

Tâche	Description	Compétences requises
Configurez le CodeCommit référentiel.	1. Décompressez le `devops-cdk-cloudcustodian.zip` fichier (joint) dans le répertoire de travail de votre ordinateur local. 2. Connectez-vous à l'AWS Management Console pour votre compte de sécurité, ouvrez la CodeCommit console, puis créez un nouveau `devops-cdk-cloudcustodian` référentiel. 3. Accédez au répertoire du projet et configurez le CodeCommit référentiel comme origine, validez les modifications, puis transférez-les vers la branche d'origine en exécutant les commandes suivantes : • `cd devops-cdk-cloudcustodian` • `git init --initial-branch=main` • `git add . git commit -m 'initial commit'`	Developer

Tâche	Description	Compétences requises
	• `git remote add origin https://git-codecommit.us-east-1.amazonaws.com/v1/devops-cdk-cloudcustodian` • `git push origin main` Pour plus d'informations à ce sujet, consultez la section Création d'un CodeCommit référentiel dans la CodeCommit documentation AWS.	
Installez les outils nécessaires.	Utilisez le `install-prerequisites.sh` fichier pour installer tous les outils requis sur Amazon Linux. Cela n'inclut pas l'AWS CLI car elle est préinstallée. Pour plus d'informations à ce sujet, consultez la section Conditions préalables de la section Getting started with the AWS CDK dans la documentation du AWS CDK.	Developer

Tâche	Description	Compétences requises
Installez les packages AWS CDK requis.	1. Configurez votre environnement virtuel en exécutant la commande suivante dans l'AWS CLI : `$ python3 -m venv .env` 2. Activez votre environnement virtuel en exécutant la commande suivante : `$ source .env/bin/activate` 3. Une fois l'environnement virtuel activé, installez les dépendances requises en exécutant la commande suivante : `$ pip install -r requirements.txt` 4. Pour ajouter des dépendances supplémentaires (par exemple, d'autres bibliothèques AWS CDK), ajoutez-les au `requirements.txt` fichier, puis exécutez la commande suivante : `pip install -r requirements.txt` Les packages suivants sont requis par AWS CDK et sont inclus dans le `requirements.txt` fichier : • `aws-cdk.aws-cloudwatch`	Developer

Tâche	Description	Compétences requises
	• `aws-cdk.aws-codebuild` • `aws-cdk.aws-codecommit` • `aws-cdk.aws-codedeploy` • `aws-cdk.aws-codepipeline` • `aws-cdk.aws-codepipeline-actions` • `aws-cdk.aws-events` • `aws-cdk.aws-events-targets` • `aws-cdk.aws-iam` • `aws-cdk.aws-logs` • `aws-cdk.aws-s3` • `aws-cdk.aws-sns` • `aws-cdk.aws-sns-subscriptions` • `aws-cdk.aws-sqs` • `aws-cdk.core`	

Configurez votre environnement

Tâche	Description	Compétences requises
Mettez à jour les variables requises.	Ouvrez le `vars.py` fichier dans le dossier racine de votre CodeCommit dépôt et mettez à jour les variables suivantes :	Developer

Tâche	Description	Compétences requises
	• Effectuez la mise à jour `var_deploy_region = ‘us-east-1’` avec la région AWS dans laquelle vous souhaitez que le pipeline soit déployé. • Effectuez la mise à jour `var_codecommit_repo_name = “cdk-cloudcustodian”` avec le nom de votre CodeCommit dépôt. • Mettre à jour `var_codecommit_branch_name = “main”` avec le nom de la CodeCommit branche. • Effectuez la mise à jour `var_adminEmail=notifyadmin@email.com’` avec l'adresse e-mail de l'administrateur qui approuve les modifications. • Mettre à jour `var_slackWebHookUrl = https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXXXXXXXXXXXXXXXX` » avec le webhook Slack utilisé pour envoyer des notifications à Cloud Custodian lorsque des modifications sont apportées.	

Tâche	Description	Compétences requises
	• Effectuez la mise à jour `var_orgId = 'o-yyyyyyyyyy'` avec l'identifiant de votre organisation. • Effectuez la mise à jour `security_account = '123456789011'` avec l'ID de compte AWS du compte sur lequel le pipeline est déployé. • Effectuez la mise à jour `member_accounts = ['111111111111','111111111112','111111111113']` avec les comptes membres sur lesquels vous souhaitez démarrer la pile AWS CDK et déployer les rôles IAM requis. • Définissez `cdk_bootstrap_member_accounts = True` cette `True` option si vous souhaitez que le pipeline démarre automatiquement le CDK AWS sur vos comptes membres. Si `True` cette option est définie, le nom d'un rôle IAM existant dans les comptes membres, qui peut être assumé à partir du compte de sécurité, est également requis. Ce rôle	

Tâche	Description	Compétences requises
	IAM doit également disposer des autorisations requises pour démarrer le AWS CDK. • **Note** Mise à jour `cdk_bootstrap_role = 'AWSControlTowerExecution'` avec le rôle IAM existant dans les comptes membres qui peut être assumé à partir du compte de sécurité. Ce rôle doit également être autorisé à démarrer le kit AWS CDK. : Cela ne s'applique que s'`cdk_bootstrap_member_accounts` il est défini sur`True`.	

Tâche	Description	Compétences requises

Mettez à jour le fichier account.yml avec les informations du compte du membre.	Pour exécuter l'outil Cloud Custodian de c7n-org sur plusieurs comptes, vous devez placer le fichier de `accounts.yml` configuration à la racine du référentiel. Voici un exemple de fichier de configuration Cloud Custodian pour AWS :
	`accounts:`
	`- account_id: '123123123123'`
	`  name: account-1`
	`  regions:`
	`  - us-east-1`
	`  - us-west-2`
	`  role: arn:aws:iam::123123123123:role/CloudCustodian`
	`  vars:`
	`  charge_code: xyz`
	`  tags:`
	`  - type:prod`
	`  - division:some division`
	`  - partition:us`
	`  - scope:pci`
		Developer

Démarrez les comptes AWS

Tâche	Description	Compétences requises
Boostrap le compte de sécurité.	Démarrez-le `deploy_account` avec l'`cloudcustodian_stack` application	Developer

Tâche	Description	Compétences requises
	en exécutant la commande suivante : `cdk bootstrap -a 'python3 cloudcustodian/cloudcustodian_stack.py`	
Option 1 - Démarrez automatiquement les comptes des membres.	Si la `cdk_bootstrap_member_accounts` variable est définie sur `True` dans le `vars.py` fichier, les comptes spécifiés dans la `member_accounts` variable sont automatiquement initialisés par le pipeline. Si nécessaire, vous pouvez effectuer une mise à jour `*cdk_bootstrap_role*` avec un rôle IAM que vous pouvez assumer depuis le compte de sécurité et qui dispose des autorisations requises pour démarrer le kit AWS CDK. Les nouveaux comptes ajoutés à la `member_accounts` variable sont automatiquement initialisés par le pipeline afin que les rôles requis puissent être déployés.	Developer

Tâche	Description	Compétences requises
Option 2 - Démarrez manuellement les comptes des membres.	Bien que nous ne recommandons pas cette approche, vous pouvez définir la valeur de `cdk_bootstrap_member_accounts` to `False` et effectuer cette étape manuellement en exécutant la commande suivante : `$ cdk bootstrap -a 'python3 cloudcustodian/member_account_roles_stack.py' \ --trust {security_account_id} \ --context assume-role-credentials:writeIamRoleName={role_name} \ --context assume-role-credentials:readIamRoleName={role_name} \ --mode=ForWriting \ --context bootstrap=true \ --cloudformation-execution-policies arn:aws:iam::aws:policy/AdministratorAccess`	Developer

Tâche	Description	Compétences requises
	Important Assurez-vous de mettre à jour les `{role_name}` valeurs `{security_account_id}` et avec le nom d'un rôle IAM que vous pouvez assumer à partir du compte de sécurité et qui dispose des autorisations requises pour démarrer le kit AWS CDK. Vous pouvez également utiliser d'autres approches pour démarrer les comptes des membres, par exemple avec AWS CloudFormation. Pour plus d'informations à ce sujet, consultez Bootstrapping dans la documentation AWS CDK.	

Déployez les piles AWS CDK

Tâche	Description	Compétences requises
Créez les rôles IAM dans les comptes des membres.	Exécutez la commande suivante pour déployer la `member_account_rol`	Developer

Tâche	Description	Compétences requises
	`es_stack` pile et créer les rôles IAM dans les comptes membres : `cdk deploy --all -a 'python3 cloudcustodian/member_account_roles_stack.py' --require-approval never`	
Déployez la pile de pipelines Cloud Custodian.	Exécutez la commande suivante pour créer le `cloudcustodian_stack.py` pipeline Cloud Custodian qui est déployé dans le compte de sécurité : `cdk deploy -a 'python3 cloudcustodian/cloudcustodian_stack.py'`	Developer

Ressources connexes

- Commencer à utiliser le kit AWS CDK

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez automatiquement des pipelines CI/CD et des clusters Amazon ECS pour les microservices à l'aide d'AWS CDK

Créée par Varsha Raju (AWS)

Récapitulatif

Ce modèle décrit comment créer automatiquement l'intégration continue et la livraison continue (CI/CD) pipelines and underlying infrastructure for building and deploying microservices on Amazon Elastic Container Service (Amazon ECS). You can use this approach if you want to set up proof-of-concept CI/CD pipelines to show your organization the benefits of CI/CD, microservices, and DevOps. You can also use this approach to create initial CI/CDpipelines) que vous pouvez ensuite personnaliser ou modifier en fonction des exigences de votre organisation.

L'approche du modèle crée un environnement de production et un environnement hors production dotés chacun d'un cloud privé virtuel (VPC) et d'un cluster Amazon ECS configurés pour s'exécuter dans deux zones de disponibilité. Ces environnements sont partagés par tous vos microservices, puis vous créez des CI/CD pipeline for each microservice. These CI/CD pipelines, vous extrayez les modifications depuis un référentiel source dans AWS CodeCommit, vous les générez automatiquement, puis vous les déployez dans vos environnements de production et hors production. Lorsqu'un pipeline termine avec succès toutes ses étapes, vous pouvez l'utiliser URLs pour accéder au microservice dans les environnements de production et hors production.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif.
- Un compartiment Amazon Simple Storage Service (Amazon S3) existant contenant `starter-code.zip` le fichier (joint).
- AWS Cloud Development Kit (AWS CDK), installé et configuré dans votre compte. Pour plus d'informations à ce sujet, consultez Getting started with the AWS CDK dans la documentation AWS CDK.
- Python 3 et`pip`, installé et configuré. Pour plus d'informations à ce sujet, consultez la documentation Python.
- Connaissance d'AWS CDK, d'AWS, d' CodePipelineAWS CodeBuild, d' CodeCommitAmazon Elastic Container Registry (Amazon ECR), d'Amazon ECS et d'AWS Fargate.
- Connaissance de Docker.

- Compréhension du CI/CD et. DevOps

Limites

- Les limites générales du compte AWS s'appliquent. Pour plus d'informations à ce sujet, consultez les quotas de service AWS dans la documentation de référence générale AWS.

Versions du produit

- Le code a été testé à l'aide de Node.js version 16.13.0 et d'AWS CDK version 1.132.0.

Architecture

Le schéma suivant illustre le flux de travail suivant :

1. Un développeur d'applications valide le code dans un CodeCommit référentiel.
2. Un pipeline est lancé.
3. CodeBuild crée et envoie l'image Docker vers un référentiel Amazon ECR
4. CodePipeline déploie une nouvelle image sur un service Fargate existant dans un cluster Amazon ECS hors production.
5. Amazon ECS extrait l'image du référentiel Amazon ECR vers un service Fargate hors production.
6. Les tests sont effectués à l'aide d'une URL hors production.
7. Le responsable de publication approuve le déploiement en production.
8. CodePipeline déploie la nouvelle image sur un service Fargate existant dans un cluster Amazon ECS de production
9. Amazon ECS extrait l'image du référentiel Amazon ECR vers le service de production Fargate.
10. Les utilisateurs de production accèdent à votre fonctionnalité à l'aide d'une URL de production.

Pile technologique

- AWS CDK
- CodeBuild
- CodeCommit

- CodePipeline
- Amazon ECR
- Amazon ECS
- Amazon VPC

Automatisation et mise à l'échelle

Vous pouvez utiliser l'approche de ce modèle pour créer des pipelines pour les microservices déployés dans une CloudFormation pile AWS partagée. L'automatisation peut créer plusieurs clusters Amazon ECS dans chaque VPC et également créer des pipelines pour les microservices déployés dans un cluster Amazon ECS partagé. Toutefois, cela nécessite que vous fournissiez de nouvelles informations sur les ressources en entrée de la pile de pipelines.

Outils

- AWS CDK — AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel permettant de définir l'infrastructure cloud dans le code et de la provisionner via AWS. CloudFormation
- AWS CodeBuild — AWS CodeBuild est un service de création entièrement géré dans le cloud. CodeBuild compile votre code source, exécute des tests unitaires et produit des artefacts prêts à être déployés.
- AWS CodeCommit — AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git dans le cloud AWS. CodeCommit vous n'avez plus à gérer votre propre système de contrôle de source ou à vous soucier de la mise à l'échelle de son infrastructure.
- AWS CodePipeline — AWS CodePipeline est un service de livraison continue que vous pouvez utiliser pour modéliser, visualiser et automatiser les étapes nécessaires à la publication de votre logiciel. Vous pouvez rapidement modéliser et configurer les différentes étapes d'un processus de publication d'un logiciel. CodePipeline automatise les étapes nécessaires à la publication continue des modifications de votre logiciel.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif utilisé pour exécuter, arrêter et gérer des conteneurs sur un cluster. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate. Pour mieux contrôler votre infrastructure, vous pouvez également exécuter vos tâches et services sur un cluster d'instances Amazon Elastic Compute Cloud (Amazon EC2) que vous gérez.

- Docker — Docker aide les développeurs à emballer, expédier et exécuter n'importe quelle application sous la forme d'un conteneur léger, portable et autonome.

Code

Le code de ce modèle est disponible dans les `starter-code.zip` fichiers `cicdstarter.zip` et (joints).

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises
Configurez le répertoire de travail pour AWS CDK.	1. Créez un répertoire nommé `cicdproject` sur votre machine locale. 2. Téléchargez le `cicdstarter.zip` fichier (joint) dans le `cicdproject` répertoire et décompressez-le. Cela crée un dossier nommé`cicdstarter` . 3. Exécutez la commande `cd <user-home>/cicdproject/cicdstarter` . 4. Configurez l'environnement virtuel Python en exécutant la `python3 -m venv .venv` commande. 5. Exécutez la commande `source ./.venv/bin/activate` . 6. Configurez votre environnement AWS en exécutant la `aws configure`	AWS DevOps, infrastructure cloud

Tâche	Description	Compétences requises
	commande ou en utilisant les variables d'environ nement suivantes : • `AWS_ACCESS_KEY_ID` • `AWS_SECRET_ACCESS_KEY` • `AWS_DEFAULT_REGION`	

Création de l'infrastructure partagée

Tâche	Description	Compétences requises
Créez l'infrastructure partagée.	1. Dans votre répertoire de travail, exécutez la `cd cicdvpcecs` commande. 2. Exécutez la `pip3 install -r requirements.txt` commande pour installer toutes les dépendances Python requises 3. Exécutez le `cdk bootstrap command` pour définir l'environnement AWS pour le CDK AWS. 4. Exécutez la commande `cdk synth --context aws_account=<aws_account_ID> --context aws_region=<aws-region> .`	AWS DevOps, infrastructure cloud

Tâche	Description	Compétences requises
	5. Exécutez la commande `cdk deploy --context aws_account=<aws_account_ID> --context aws_region=<aws-region>` .	
	6. La CloudFormation pile AWS crée l'infrastructure suivante : • Un VPC hors production nommé `cicd-vpc-ecs/cicd-vpc-nonprod` • Un VPC de production nommé `cicd-vpc-ecs/cicd-vpc-prod` • Un cluster Amazon ECS hors production nommé `cicd-ecs-nonprod` • Un cluster Amazon ECS de production nommé `cicd-ecs-prod`	

Tâche	Description	Compétences requises
Surveillez la CloudFormation pile AWS.	1. Connectez-vous à l'AWS Management Console, ouvrez la CloudForm ation console AWS, puis choisissez la `cicd-vpc-ecs` pile dans la liste. 2. Dans le volet des détails de la pile, choisissez l'onglet Événements et surveillez la progression de la création de votre pile.	AWS DevOps, infrastructure cloud

Tâche	Description	Compétences requises
Testez la CloudFormation pile AWS.	1. Une fois la CloudFormation pile `cicd-vpc-ecs` AWS créée, assurez-vous que les `cicd-vpc-ecs/cicd-vpc-nonprod` et `cicd-vpc-ecs/cicd-vpc-prod` VPCs sont créés. 2. Assurez-vous que les clusters `cicd-ecs-nonprod` et `cicd-ecs-prod` Amazon ECS sont créés. **Important** Assurez-vous d'enregistrer le IDs pour les deux groupes de sécurité VPCs et le groupe de sécurité IDs pour les groupes de sécurité par défaut dans les deux VPCs.	AWS DevOps, infrastructure cloud

Création d'un pipeline CI/CD pour un microservice

Tâche	Description	Compétences requises
Créez l'infrastructure du microservice.	1. Donnez un nom à votre microservice. Par exemple, ce modèle utilise `myservice1` comme nom du microservice.	AWS DevOps, infrastructure cloud

Tâche	Description	Compétences requises
	2. Dans votre répertoire de travail, exécutez la `cd <working-directory>/cdkpipeline` commande. 3. Exécutez la commande `pip3 install -r requirements.txt .` 4. Exécutez la `cdk synth` commande complète disponible dans la section Informations supplémentaires de ce modèle. 5. Exécutez la `cdk deploy` commande complète disponible dans la section Informations supplémentaires de ce modèle. **Note** Vous pouvez également fournir les valeurs des deux commandes en utilisant le `cdk.json` fichier du répertoire.	

Tâche	Description	Compétences requises
Surveillez la CloudFormation pile AWS.	Ouvrez la CloudFormation console AWS et surveillez la progression de la `myservice 1-cicd-stack` pile. Finalement, le statut passe à `CREATE_COMPLETE` .	AWS DevOps, infrastructure cloud

Tâche	Description	Compétences requises
Testez la CloudFormation pile AWS.	1. Sur la CodeCommit console AWS, vérifiez qu'un référentiel nommé `myservice1` existe et contient le code de démarrage. 2. Sur la CodeBuild console AWS, vérifiez qu'un projet de construction nommé `myservice1` existe. 3. Sur la console Amazon ECR, vérifiez qu'un référentiel Amazon ECR nommé `myservice1` existe. 4. Sur la console Amazon ECS, vérifiez qu'un service Fargate `myservice1` nommé existe à la fois dans un cluster Amazon ECS hors production et dans un cluster Amazon ECS de production. 5. Sur la console Amazon Elastic Compute Cloud (Amazon EC2), vérifiez que les équilibreurs de charge des applications hors production et de production sont créés. Enregistrez les noms DNS du ALBs. 6. Sur la CodePipeline console AWS, vérifiez qu'un pipeline	

Tâche	Description	Compétences requises
	nommé `myservice 1` existe. Il doit avoir `SourceBuild`,`Deploy-NonProd` , et `Deploy-Prod` étapes. Le pipeline doit également avoir un `in progress` statut. 7. Surveillez le pipeline jusqu'à ce que toutes les étapes soient terminées. 8. Approuvez-le manuellement pour la production. 9. Dans une fenêtre de navigateur, entrez les noms DNS du ALBs. 10. L'application doit s'afficher `Hello World` en mode hors production et en mode production URLs.	

Tâche	Description	Compétences requises
Utilisez le pipeline.	1. Ouvrez le CodeCommit référentiel que vous avez créé précédemment et ouvrez le `index.js` fichier. 2. Remplacez `Hello World` par `Hello CI/CD`. 3. Enregistrez et validez les modifications apportées à la branche principale. 4. Vérifiez que le pipeline démarre et que la modification passe par les `Deploy-Prod` étapes`Build`,`Deploy-NonProd` , et. 5. Approuvez manuellement la production. 6. La production et la non-production URLs devraient désormais s'afficher*`Hello CICD`*.	AWS DevOps, infrastructure cloud
Répétez cette épopée pour chaque microservice.	Répétez les tâches de cette épopée pour créer un pipeline CI/CD pour chacun de vos microservices.	AWS DevOps, infrastructure cloud

Ressources connexes

- Utilisation de Python avec AWS CDK
- Référence Python du kit AWS CDK
- Création d'un service AWS Fargate à l'aide du kit AWS CDK

Informations supplémentaires

Commande **cdk synth** de la

```
cdk synth --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production
 VPC> --context vpc_prod_id=<id_of_production_VPC> --context
 ecssg_nonprod_id=< default_security_group_id_of_non-production_VPC>
 --context ecssg_prod_id=<default_security_group_id_of_production_VPC>
 --context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

cdk deploy commande

```
cdk deploy --context aws_account=<aws_account_number> --context
 aws_region=<aws_region> --context vpc_nonprod_id=<id_of_non_production_VPC>
 --context vpc_prod_id=<id_of_production_VPC> --context ecssg_nonprod_id=<
 default_security_group_id_of_non-production_VPC> --context
 ecssg_prod_id=<default_security_group_id_of_production_VPC> --
context code_commit_s3_bucket_for_code=<S3 bucket name> --context
 code_commit_s3_object_key_for_code=<Object_key_of_starter_code> --context
 microservice_name=<name_of_microservice>
```

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez une architecture faiblement couplée avec des microservices en utilisant DevOps Practices et AWS Cloud9

Créée par Alexandre Nardi (AWS)

Récapitulatif

Remarque : n' AWS Cloud9 est plus disponible pour les nouveaux clients. Les clients existants de AWS Cloud9 peuvent continuer à utiliser le service normalement. En savoir plus

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle montre comment développer une application Web typique dans une architecture sans serveur, pour les développeurs et les responsables du développement qui commencent à tester DevOps des pratiques sur Amazon Web Services (AWS). Il crée un exemple d'application qui crée une vitrine et un backend pour parcourir et acheter des livres, et fournit un microservice qui peut être développé indépendamment. Le modèle utilise AWS Cloud9 comme environnement de développement, une base de données Amazon DynamoDB comme magasin de données et des services AWS tels qu'AWS et CodeBuild AWS pour les fonctionnalités d'intégration CodePipeline et de déploiement continus (CI/CD).

Le modèle vous guide à travers les activités de développement suivantes :

- Création d'un environnement de développement AWS Cloud9 standard
- Utilisation de CloudFormation modèles AWS pour créer une application Web et un microservice pour les livres
- Utilisation d'AWS Cloud9 pour modifier le front-end, valider les modifications et tester les modifications
- Création et test d'un pipeline CI/CD vers le microservice
- Automatisation des tests unitaires

Le code de ce modèle est fourni dans GitHub le référentiel AWS DevOps End-to-End Workshop.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

- Fichiers de l'AWS DevOps End-to-End Workshop téléchargés sur votre ordinateur

> **Important**
>
> La création de cette application de démonstration dans votre compte AWS crée et consomme des ressources AWS. Vous êtes responsable du coût des services et des ressources AWS utilisés pour créer et exécuter l'application. Une fois votre travail terminé, veillez à supprimer toutes les ressources afin d'éviter des frais récurrents. Pour les instructions de nettoyage, consultez la section Epics.

Limites

Cette procédure pas à pas est uniquement destinée à des fins de démonstration et de développement. Pour l'utiliser dans un environnement de production, consultez les meilleures pratiques en matière de sécurité dans la documentation AWS Identity and Access Management (IAM) et apportez les modifications nécessaires aux rôles IAM, à Amazon DynamoDB et aux autres services utilisés. L'application Web est dérivée de l'application de démonstration AWS Bookstore ; pour plus d'informations, consultez la section Limitations connues du fichier README.

Architecture

L'architecture de l'application de librairie est illustrée dans la section Architecture du fichier README de l'application de démonstration AWS Bookstore.

Du point de vue du déploiement, l'application de démonstration Bookstore utilise un CloudFormation modèle unique pour déployer tous les services et objets dans une seule pile. Ce modèle apporte quelques modifications pour montrer comment un développeur ou une équipe en particulier pourrait travailler sur un produit spécifique (Books) et le mettre à jour indépendamment du reste de l'application. C'est pourquoi le code de ce modèle sépare les fonctions AWS Lambda et les objets associés pour le microservice Books dans un second CloudFormation modèle, qui crée une pile Books. Cela permet de voir le microservice mis à jour en utilisant les pratiques CI/CD. Dans le schéma suivant, la bordure en pointillés identifie le microservice Books.

Outils

Outils

- Framework Jest pour les tests JavaScript
- Python 3.9

Code

Le code source et les modèles de ce modèle sont disponibles sur GitHub le référentiel AWS DevOps End-to-End Workshop. Avant de suivre les étapes de la section Epics, téléchargez tous les fichiers du référentiel sur votre ordinateur.

> **Note**
>
> La section Epics fournit les étapes de haut niveau de cette procédure pas à pas, afin de vous donner des informations générales sur le processus. Pour terminer chaque étape, consultez le fichier README dans le référentiel AWS DevOps End-to-End Workshop pour obtenir des instructions détaillées.

Le référentiel AWS DevOps End-to-End Workshop étend le référentiel des applications de démonstration AWS Bookstore et utilise une version modifiée du code d'amorçage AWS Cloud9 pour créer l'IDE AWS Cloud9.

Bonnes pratiques

L'utilisation de l'application Bookstore est simple. Voici quelques bonnes pratiques recommandées :

- Lorsque vous installez l'application, vous pouvez utiliser le nom du projet de votre choix ou utiliser le nom par défaut (`demobookstore`) pour plus de commodité.
- Une fois que l'application est opérationnelle, il est recommandé d'arrêter la base de données Amazon Neptune si vous souhaitez poursuivre les tests pendant un jour de plus, car l'instance de base de données peut entraîner des frais supplémentaires. Sachez toutefois que la base de données sera automatiquement démarrée au bout de sept jours.
- Pour plus de détails sur le code, consultez la documentation du référentiel d'applications de démonstration AWS Bookstore. Il décrit chaque microservice et chaque table.
- Pour d'autres bonnes pratiques, consultez la section Quelques défis si vous avez le temps... section du fichier README dans le référentiel AWS DevOps End-to-End Workshop. Nous vous recommandons de consulter les informations pour approfondir les fonctionnalités supplémentaires de sécurité et pour pratiquer le découplage des services.

Épopées

Téléchargez le code source

Tâche	Description	Compétences requises
Téléchargez le code source depuis GitHub.	Le code source et les modèles de ce modèle sont disponibles dans GitHub le référentiel AWS DevOps End-to-End Workshop. Avant de suivre les étapes suivantes de la section Epics, téléchargez tous les fichiers du référentiel sur votre ordinateur. **Note** La section Epics fournit les étapes de haut niveau de cette procédure pas à pas, afin de vous donner des informations générales sur le processus. Pour terminer chaque étape, consultez le fichier README dans le référentiel AWS DevOps End-to-End Workshop pour obtenir des instructions détaillées.	Développeur d'applications

Tâche	Description	Compétences requises
	Le référentiel AWS DevOps End-to-End Workshop étend le référentiel des applications de démonstration AWS Bookstore et utilise une version modifiée du code d'amorçage AWS Cloud9 pour créer l'IDE AWS Cloud9.	

Créez l'application Web Bookstore et le microservice Books

Tâche	Description	Compétences requises
Créez les fonctions frontales et Lambda pour l'application Bookstore.	1. Connectez-vous à la CloudFormation console et déployez le `DemoBookstoreMainTemplate.yml` modèle pour créer la DemoBookStoreStack pile. Cela crée les fonctions frontales et Lambda qui ne font pas partie du microservice Books. 2. Dans l'onglet Sorties de la pile, notez l'URL du site Web sous l'WebApplicationétiquette.	Developer
Créez le microservice Books.	Sur la CloudFormation console, déployez le `DemoBookstoreBooksServiceTemplate.yml` modèle pour créer la DemoBooksServiceStack pile.	Developer

Tâche	Description	Compétences requises
Testez votre application.	Utilisez l'URL du site Web figurant dans la DemoBookStoreStack pile pour accéder à l'application Bookstore.	Developer

Utilisez l'environnement Cloud9 pour gérer votre application

Tâche	Description	Compétences requises
Créez un IDE AWS Cloud9.	Sur la CloudFormation console, déployez le `C9EnvironmentTemplate.yml` modèle pour créer un environnement AWS Cloud9.	Développeur, responsable du développement
Créez des CodeCommit référentiels.	1. Connectez-vous à la CodeCommit console AWS et vérifiez que vous disposez d'un `demobookstore-WebAssets` référentiel contenant le code de l'application frontale. 2. Créez un référentiel pour le microservice Books appelé`demobookstore-BooksService` . 3. Clonez les deux référentiels dans AWS Cloud9 `demobookstore-WebAssets` (`demobookstore-Book`	Developer

Tâche	Description	Compétences requises
	`sService` et) à l'aide `git clone` de la commande.	
Modifiez le code dans le frontend et vérifiez le pipeline.	1. Utilisez AWS Cloud9 pour apporter des modificat ions au code d'une page Web. Cela mettra à jour le `demobookstore-WebA ssets` référentiel. 2. Sur la CodePipeline console AWS, vérifiez que DemoBookStore-Asse ts-Pipeline est en cours d'exécution. 3. Testez votre application Web en l'actualisant depuis le navigateur (Ctrl+F5 sur Firefox).	Developer

Implémenter un pipeline CI/CD pour le microservice Books

Tâche	Description	Compétences requises
Ajoutez les fichiers YAML pour la compilation et la mise à jour du service.	1. Dans AWS Cloud9, chargez les fichiers `buildspec .yml` et`DemoBooks toreBooksServiceUp dateTemplate.yml` . • `buildspec .yml` contient des instructions de montage et inclut également des instructions de test pour les tests automatisés.	Developer

Tâche	Description	Compétences requises
	Ils sont commentés à ce stade et seront utilisés ultérieurement. • `DemoBookstoreBooksServiceUpdateTemplate.yml` est une version mise à jour de`DemoBookstoreBooksServiceTemplate.yml`, à utiliser lors de la phase de déploiement du pipeline. 2. Validez et publiez les fichiers.	
Créez un compartiment S3 pour le pipeline de construction.	Pour créer un compartiment S3, suivez les instructions de la documentation Amazon S3. • Le nom du bucket doit être unique au monde ; par exemple,`demobookstore-books-service-pipeline-bucket-<YYYYMMDDHHMM>`. • Décochez la case Bloquer tout accès public, puis cochez la case J'accuse réception...	Developer

Tâche	Description	Compétences requises
Utilisez IAM pour créer un rôle à CloudFormation déployer.	Créez un `demobookstore-CloudFormation-role` rôle et associez la `AdministratorAccess` politique. Dans la prochaine épopée, vous pourrez reconfigurer ce rôle pour obtenir des autorisations minimales.	Developer
Créez un nouveau pipeline pour automatiser la création et le déploiement du microservice Books.	Créez un pipeline (par exemple, demobookstore-BooksService -Pipeline) avec les étapes Commit, Build et Deploy, comme décrit dans le fichier README.	Developer
Testez votre microservice dans AWS Cloud9.	Modifiez la ListBooksfonction et observez le pipeline fonctionner.	Developer
Automatisez le test unitaire pour la fonction ListBooks Lambda.	Dans l'IDE AWS Cloud9, activez la version pour exécuter des tests unitaires et vérifiez les résultats des tests. Pour obtenir des instructions, consultez le fichier README.	Developer

(Facultatif) Implémenter des fonctionnalités supplémentaires

Tâche	Description	Compétences requises
Sécurisez votre solution.	Configurez `demobookstore-CloudFormation-role` pour disposer d'autorisations minimales et	Developer

Tâche	Description	Compétences requises
	vérifiez également les autres rôles utilisés.	
Éliminez les dépendances dans les CloudFormation modèles.	La méthode d'échange d'informations entre le `DemoBookstoreMainTemplate.yml` modèle et le `DemoBookstoreBooksServiceTemplate.yml` modèle est basée sur les sorties et les importations. Le transfert de valeurs entre ces deux modèles ajoute des dépendances. Pour éliminer les dépendances, pensez à utiliser AWS Systems Manager Parameter Store.	Developer
Créez un microservice Cart.	Utilisez le microservice Books comme exemple pour supprimer les fonctions liées au panier d'achat du `DemoBookstoreMainTemplate.yml` modèle et créer un microservice Cart.	Developer

Nettoyage

Tâche	Description	Compétences requises
Supprimez les compartiments S3.	Sur la console Amazon S3, supprimez les compartiments suivants associés à l'exemple d'application Web :	Developer

Tâche	Description	Compétences requises
	• Deux compartiments créés pour l'application de démonstration AWS Bookstore. Les noms des compartiments commencent par le nom de pile que vous avez fourni à AWS CloudFormation lorsque vous avez créé le frontend ; par exemple,. DemoBookStoreStack • <YYYYMMDDHHMM>Un compartiment pour le pipeline de construction ; par exemple, demobookstore-books-service-pipeline-bucket-.	

Tâche	Description	Compétences requises
Supprimez les piles.	Sur la CloudFormation console, supprimez les piles associées à l'exemple d'application Web : • DemoBooksServiceStack • DemoBookStoreStack Le retrait peut prendre plus de 90 minutes. Si la suppression échoue, supprimez-les à nouveau et supprimez également toutes les ressources manuelles (par exemple, le VPC ou les interfaces réseau) en fonction des notifications.	Developer
Supprimez les rôles IAM.	Sur la console IAM, supprimez les rôles suivants : • `demobookstore-Cloudformation-role` • `demobookstore-BooksService-BuildProject-service-role` Pour step-by-step obtenir des instructions, consultez la documentation IAM.	Developer

Ressources connexes

- Application de démonstration AWS Bookstore

- Exemple de bootstrapping d'AWS Cloud9
- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Création d'un compartiment (documentation Amazon S3)

Informations supplémentaires

Pour obtenir des step-by-step instructions détaillées, consultez le fichier README dans le GitHub référentiel AWS DevOps End-to-End Workshop.

À propos de la mise à jour de mai 2023 : ce modèle a été mis à jour pour utiliser les nouvelles versions de Node et Python. Nous avons mis à jour de nombreux packages du code source et supprimé Glyphicon car il n'est plus gratuit. Nous avons également supprimé toutes les dépendances du référentiel de l'application de démonstration AWS Bookstore, de sorte que les deux référentiels peuvent désormais évoluer indépendamment.

Créez et envoyez des images Docker vers Amazon ECR à l'aide d' GitHub Actions et de Terraform

Créée par Ruchika Modi (AWS)

Récapitulatif

Ce modèle explique comment créer des GitHub flux de travail réutilisables pour créer votre Dockerfile et transférer l'image résultante vers Amazon Elastic Container Registry (Amazon ECR). Le modèle automatise le processus de création de vos Dockerfiles à l'aide de Terraform et d'Actions. GitHub Cela minimise le risque d'erreur humaine et réduit considérablement le temps de déploiement.

Une action GitHub push sur la branche principale de votre GitHub dépôt déclenche le déploiement des ressources. Le flux de travail crée un référentiel Amazon ECR unique basé sur la combinaison de l' GitHub organisation et du nom du référentiel. Il envoie ensuite l'image Dockerfile vers le référentiel Amazon ECR.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un GitHub compte actif.
- Un GitHub référentiel.
- Terraform version 1 ou ultérieure installée et configurée.
- Un bucket Amazon Simple Storage Service (Amazon S3) pour le backend Terraform.
- Une table Amazon DynamoDB pour le verrouillage de l'état et la cohérence de Terraform. La table doit avoir une clé de partition nommée `LockID` avec un type de`String`. Si cela n'est pas configuré, le verrouillage d'état sera désactivé.
- Rôle AWS Identity and Access Management (IAM) autorisé à configurer le backend Amazon S3 pour Terraform. Pour les instructions de configuration, consultez la documentation Terraform.

Limites

Ce code réutilisable a été testé uniquement avec des GitHub actions.

Architecture

Pile technologique cible

- Référentiel Amazon ECR
- GitHub Les actions
- Terraform

Architecture cible

Le diagramme illustre les éléments suivants :

1. Un utilisateur ajoute un Dockerfile et des modèles Terraform au référentiel. GitHub

2. Ces ajouts initient un flux de travail GitHub Actions.

3. Le flux de travail vérifie l'existence d'un référentiel Amazon ECR. Dans le cas contraire, il crée le référentiel en fonction de l' GitHub organisation et du nom du référentiel.

4. Le flux de travail crée le Dockerfile et envoie l'image vers le référentiel Amazon ECR.

Outils

Services Amazon

- Amazon Elastic Container Registry (Amazon ECR) est un service de registre de conteneurs géré sécurisé, évolutif et fiable.

Autres outils

- GitHub Actions est intégré à la GitHub plateforme pour vous aider à créer, partager et exécuter des flux de travail au sein de vos GitHub référentiels. Vous pouvez utiliser GitHub les actions pour automatiser des tâches telles que la création, le test et le déploiement de votre code.
- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer une infrastructure cloud et sur site.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Docker ECR Actions Workflow.

- Lorsque vous créez des GitHub actions, les fichiers de flux de travail Docker sont enregistrés dans le `/.github/workflows/` dossier de ce référentiel. Le flux de travail de cette solution se trouve dans le fichier workflow.yaml.
- Le `e2e-test` dossier fournit un exemple de Dockerfile à des fins de référence et de test.

Bonnes pratiques

- Pour connaître les meilleures pratiques en matière d'écriture de Dockerfiles, consultez la documentation Docker.
- Utilisez un point de terminaison VPC pour Amazon ECR. Les points de terminaison VPC sont alimentés par AWS PrivateLink, une technologie qui vous permet d'accéder en privé à Amazon ECR APIs via des adresses IP privées. Pour les tâches Amazon ECS qui utilisent le type de lancement Fargate, le point de terminaison VPC permet à la tâche d'extraire des images privées d'Amazon ECR sans attribuer d'adresse IP publique à la tâche.

Épopées

Configuration du fournisseur et GitHub du référentiel OIDC

Tâche	Description	Compétences requises
Configurez OpenID Connect.	Créez un fournisseur OpenID Connect (OIDC). Vous utiliserez le fournisseur dans la politique de confiance pour le rôle IAM utilisé dans cette action. Pour obtenir des instructions, consultez la section Configuration d'OpenID Connect dans Amazon Web Services dans la GitHub documentation.	Administrateur AWS, AWS DevOps, AWS général
Clonez le GitHub dépôt.	Clonez le référentiel GitHub Docker ECR Actions Workflow dans votre dossier local :	DevOps ingénieur

Tâche	Description	Compétences requises
	`$git clone https://github.com/aws-samples/docker-ecr-actions-workflow`	

Personnalisez le flux de travail GitHub réutilisable et déployez l'image Docker

Tâche	Description	Compétences requises
Personnalisez l'événement qui lance le flux de travail Docker.	Le flux de travail de cette solution se trouve dans workflow.yaml. Ce script est actuellement configuré pour déployer des ressources lorsqu'il reçoit l'`workflow_dispatch` événement. Vous pouvez personnaliser cette configuration en remplaçant l'événement par un autre flux de travail parent `workflow_call` et en appelant le flux de travail à partir d'un autre flux de travail parent.	DevOps ingénieur
Personnalisez le flux de travail.	Le fichier workflow.yaml est configuré pour créer un flux de travail dynamique et réutilisable. GitHub Vous pouvez modifier ce fichier pour personnaliser la configuration par défaut, ou vous pouvez transmettre les valeurs d'entrée depuis la console GitHub Actions si	DevOps ingénieur

Tâche	Description	Compétences requises

	vous utilisez l'`workflow_dispatch` événement pour lancer le déploiement manuellement.
	• Assurez-vous de spécifier l'ID de compte AWS et la région cible corrects.
	• Créez une politique de cycle de vie Amazon ECR (voir exemple de politique) et mettez à jour le chemin par défaut (`e2e-test/policy.json`) en conséquence.
	• Le fichier de flux de travail nécessite deux rôles IAM en entrée :
	  • Rôle IAM autorisé à configurer le backend Amazon S3 pour Terraform (voir la section Conditions préalables). Vous pouvez mettre à jour le nom de rôle par défaut `workload-assumable-role` dans le. `yaml`classer en conséquence.
	  • Rôle IAM autorisé à accéder GitHub. Ce rôle est également utilisé dans la politique Amazon ECR pour restreindre les	

Tâche	Description	Compétences requises
	opérations Amazon ECR. Pour plus d'informations, consultez le fichier data.tf.	
Déployez les modèles Terraform.	Le flux de travail déploie automatiquement les modèles Terraform qui créent le référentiel Amazon ECR, en fonction de l' GitHub événement que vous avez configuré. Ces modèles sont disponibles sous forme de `.tf` fichiers à la racine du référentiel Github.	AWS DevOps, DevOps ingénieur

Résolution des problèmes

Problème	Solution
Problèmes ou erreurs lorsque vous configurez Amazon S3 et DynamoDB en tant que backend distant Terraform.	Suivez les instructions de la documentation Terraform pour configurer les autorisations requises sur les ressources Amazon S3 et DynamoDB pour la configuration du backend distant.
Impossible d'exécuter ou de démarrer le flux de travail avec l'`workflow_dispatch` événement.	Le flux de travail configuré pour être déployé à partir de l'`workflow_dispatch` événement ne fonctionnera que s'il est également configuré sur la branche principale.

Ressources connexes

- Réutilisation des flux de travail (GitHub documentation)
- Déclenchement d'un flux de travail (GitHub documentation)

Créez et testez des applications iOS avec AWS CodeCommit CodePipeline, AWS et AWS Device Farm

Créée par Abdullahi Olaoye (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle décrit les étapes de création d'un pipeline d'intégration et de livraison continues (CI/CD) qui utilise AWS CodePipeline pour créer et tester des applications iOS sur des appareils réels sur AWS. Le modèle utilise AWS CodeCommit pour stocker le code de l'application, l'outil open source Jenkins pour créer l'application iOS et AWS Device Farm pour tester l'application créée sur de vrais appareils. Ces trois phases sont orchestrées ensemble dans un pipeline à l'aide d'AWS CodePipeline.

Ce modèle est basé sur l'article Création et test d'applications iOS et iPadOS avec AWS DevOps et les services mobiles publié sur le DevOps blog AWS. Pour des instructions détaillées, consultez le billet de blog.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un compte de développeur Apple
- Serveur de compilation (macOS)
- Xcode version 11.3 (installé et configuré sur le serveur de compilation)
- Interface de ligne de commande AWS (AWS CLI) (AWS CLI) installée et configurée sur le poste de travail
- Connaissances de base de Git

Limites

- Le serveur de génération d'applications doit exécuter macOS.
- Le serveur de build doit avoir une adresse IP publique afin de CodePipeline pouvoir s'y connecter à distance pour lancer des builds.

Architecture

Pile technologique source

- Processus de création d'applications iOS sur site qui implique l'utilisation d'un simulateur ou un test manuel sur des appareils physiques

Pile technologique cible

- Un CodeCommit référentiel AWS pour le stockage du code source de l'application
- Un serveur Jenkins pour les builds d'applications à l'aide de Xcode
- Un pool d'appareils AWS Device Farm pour tester des applications sur de vrais appareils

Architecture cible

Lorsqu'un utilisateur apporte des modifications au référentiel source, le pipeline (AWS CodePipeline) extrait le code du référentiel source, lance une compilation Jenkins et transmet le code de l'application à Jenkins. Après le build, le pipeline récupère l'artefact de build et lance une tâche AWS Device Farm pour tester l'application par rapport à un pool d'appareils.

Outils

- AWS CodePipeline est un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. CodePipeline automatise les phases de création, de test et de déploiement de votre processus de publication chaque fois qu'un changement de code est effectué, en fonction du modèle de version que vous définissez.
- AWS CodeCommit est un service de contrôle de source entièrement géré qui héberge des référentiels sécurisés basés sur Git. Il permet aux équipes de collaborer facilement sur le code dans un écosystème sécurisé et hautement évolutif. CodeCommit élimine le besoin d'exploiter votre propre système de contrôle de source ou de vous soucier de la mise à l'échelle de son infrastructure.
- AWS Device Farm est un service de test d'applications qui vous permet d'améliorer la qualité de vos applications Web et mobiles en les testant sur une large gamme de navigateurs de bureau et de véritables appareils mobiles, sans avoir à fournir ni à gérer d'infrastructure de test.

- Jenkins est un serveur d'automatisation open source qui permet aux développeurs de créer, de tester et de déployer leurs logiciels.

Épopées

Configuration de l'environnement de construction

Tâche	Description	Compétences requises
Installez Jenkins sur le serveur de compilation qui exécute macOS.	Jenkins sera utilisé pour créer l'application, vous devez donc d'abord l'installer sur le serveur de compilation. Pour obtenir des instructions détaillées concernant cette tâche et les tâches suivantes , consultez le billet de blog AWS sur la création et le test d'applications iOS et iPadOS avec AWS DevOps , les services mobiles et d'autres ressources dans la section Ressources connexes à la fin de ce modèle.	DevOps
Configurez Jenkins.	Suivez les instructions affichées à l'écran pour configurer Jenkins.	DevOps
Installez le CodePipeline plugin AWS pour Jenkins.	Ce plugin doit être installé sur le serveur Jenkins pour que Jenkins puisse interagir avec le service AWS CodePipeline .	DevOps
Créez un projet Jenkins Freestyle.	Dans Jenkins, créez un projet de freestyle. Configurez le projet pour spécifier les déclencheurs et les autres	DevOps

Tâche	Description	Compétences requises
	options de configuration de construction.	

Configuration d'AWS Device Farm

Tâche	Description	Compétences requises
Créez un projet Device Farm.	Ouvrez la console AWS Device Farm. Créez un projet et un pool d'appareils à tester. Pour obtenir des instructions, consultez le billet de blog.	Developer

Configuration du référentiel source

Tâche	Description	Compétences requises
Créez un CodeCommit référentiel.	Créez un référentiel dans lequel le code source sera stocké.	DevOps
Enregistrez le code de votre application dans le référentiel.	Connectez-vous au CodeCommit référentiel que vous avez créé. Transférez le code de votre machine locale vers le référentiel.	DevOps

Configuration du pipeline

Tâche	Description	Compétences requises
Créez un pipeline dans AWS CodePipeline.	Ouvrez la CodePipeline console AWS et créez	DevOps

Tâche	Description	Compétences requises
	un pipeline. Le pipeline orchestre toutes les phases du processus CI/CD. Pour obtenir des instructions, consultez le billet de blog AWS intitulé Création et test d'applications iOS et iPadOS avec AWS DevOps et les services mobiles.	
Ajoutez une phase de test au pipeline.	Pour ajouter une phase de test et l'intégrer à AWS Device Farm, modifiez le pipeline.	DevOps
Lancez le pipeline.	Pour démarrer le pipeline et le processus CI/CD, choisissez Release change.	DevOps

Afficher les résultats des tests d'applications

Tâche	Description	Compétences requises
Passez en revue les résultats des tests.	Dans la console AWS Device Farm, sélectionnez le projet que vous avez créé et passez en revue les résultats des tests. La console affichera les détails de chaque test.	Developer

Ressources connexes

Step-by-step instructions pour ce modèle

- Création et test d'applications iOS et iPadOS avec AWS DevOps et les services mobiles (article de DevOps blog AWS)

Configuration d'AWS Device Farm

- Console AWS Device Farm

Configuration du référentiel source

- Création d'un CodeCommit référentiel AWS
- Connectez-vous à un CodeCommit référentiel AWS

Configuration du pipeline

- CodePipeline Console AWS

Ressources supplémentaires

- CodePipeline Documentation AWS
- CodeCommit Documentation AWS
- Documentation d'AWS Device Farm
- Documentation de Jenkins
- Installation de Jenkins sur macOS
- CodePipeline Plug-in AWS pour Jenkins
- Installation de Xcode
- Installation et configuration de la CLI AWS
- Documentation Git

Consultez les applications ou les CloudFormation modèles AWS CDK pour connaître les meilleures pratiques à l'aide des packs de règles cdk-nag

Créée par Arun Donti

Récapitulatif

Ce modèle explique comment utiliser l'utilitaire cdk-nag pour vérifier les bonnes pratiques des applications AWS Cloud Development Kit (AWS CDK) en utilisant une combinaison de packs de règles. cdk-nag est un projet open source inspiré par cfn_nag. Il met en œuvre des règles dans des packs d'évaluation tels que AWS Solutions Library, Health Insurance Portability and Accountability Act (HIPAA) et National Institute of Standards and Technology (NIST) 800-53 en utilisant AWS CDK Aspects. Vous pouvez vérifier les bonnes pratiques de vos applications AWS CDK en utilisant les règles de ces packs, détecter et corriger le code en fonction des meilleures pratiques, et supprimer les règles que vous ne souhaitez pas utiliser dans vos évaluations.

Vous pouvez également utiliser cdk-nag pour vérifier vos CloudFormation modèles AWS à l'aide du module cloudformation-include.

Pour plus d'informations sur tous les packs disponibles, consultez la section Règles du référentiel cdk-nag. Des packs d'évaluation sont disponibles pour :

- Bibliothèque de solutions AWS
- Sécurité HIPAA
- NIST 800-53 version 4
- NIST 800-53 version 5
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) 3.2.1

Conditions préalables et limitations

Prérequis

- Une application qui utilise le kit AWS CDK

Outils

- AWS CDK — Cloud Development Kit (AWS CDK) est un framework de développement logiciel permettant de définir l'infrastructure cloud dans le code et de la provisionner via AWS. CloudFormation
- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, et vous pouvez les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.

Épopées

Intégrez cdk-nag à votre application AWS CDK

Tâche	Description	Compétences requises
En savoir plus sur cdk-nag.	Accédez au GitHub référentiel cdk-nag et lisez la documentation.	Développeur d’applications
Installez le package cdk-nag dans votre application AWS CDK.	Pour utiliser cdk-nag dans votre application AWS CDK, vous devez d'abord l'installer. cdk-nag est disponible en téléchargement depuis PyPI, npm et Apache Maven. NuGet Pour obtenir les dernières informations sur les versions disponibles et les emplacements de téléchargement, consultez le fichier Readme dans le référentiel.	Développeur d’applications
Choisissez votre NagPacks.	cdk-nag possède différents packs de règles appelés.	Développeur d’applications

Tâche	Description	Compétences requises
	NagPacks Chacune NagPack contient des règles conformes à une norme spécifique. Par exemple, les solutions AWS NagPack contiennent les meilleures pratiques générales , et le NIST 800-53 rev 5 NagPack peut contribuer à la conformité. Vous pouvez en appliquer plusieurs NagPacks à votre application, et vous pouvez ajouter et supprimer des packs si nécessaire. Pour obtenir la liste des packs disponibles, consultez le fichier Readme dans le GitHub référentiel. Pour plus d'informations sur les règles individuelles de chaque pack, consultez la section Règles du GitHub référentiel.	

Tâche	Description	Compétences requises

Intégrez cdk-nag dans votre application AWS CDK.	Vous pouvez intégrer cdk-nag dans votre application à l'échelle de l'application, ou l'intégrer dans des étapes ou des piles individuelles de votre application. Par exemple, pour intégrer les solutions AWS et la sécurité HIPAA NagPacks dans une application AWS CDK v2 à l'échelle de TypeScript l'application, vous pouvez utiliser le code suivant :
	
	`import { App, Aspects } from 'aws-cdk-lib';`
	`import { CdkTestStack } from '../lib/cdk-test-stack';`
	`import { AwsSolutionsChecks, HIPAASecurityChecks } from 'cdk-nag';`
	
	`const app = new App();`
	`new CdkTestStack(app, 'CdkNagDemo');`
	`// Simple rule informational messages`
	`Aspects.of(app).add(new AwsSolutionsChecks());`
	`// Additional explanations on the purpose of triggered rules`
	`Aspects.of(app).add(new HIPAASecurityChecks({ verbose: true }));`
		Développeur d'applications

Ressources connexes

- dépôt de code cdk-nag
- cdk-nag dans Construct Hub

Configurer l'authentification TLS mutuelle pour les applications exécutées sur Amazon EKS

Créée par Mahendra Siddappa (AWS)

Récapitulatif

La sécurité mutuelle de couche de transport (TLS) basée sur des certificats est un composant TLS optionnel qui fournit une authentification réciproque entre les serveurs et les clients. Avec le protocole TLS mutuel, les clients doivent fournir un certificat X.509 pendant le processus de négociation de session. Le serveur utilise ce certificat pour identifier et authentifier le client.

Le protocole TLS mutuel est une exigence courante pour les applications de l'Internet des objets (IoT) et peut être utilisé pour business-to-business des applications ou des normes telles que l'Open Banking.

Ce modèle décrit comment configurer le protocole TLS mutuel pour les applications exécutées sur un cluster Amazon Elastic Kubernetes Service (Amazon EKS) à l'aide d'un contrôleur d'entrée NGINX. Vous pouvez activer les fonctionnalités TLS mutuelles intégrées pour le contrôleur d'entrée NGINX en annotant la ressource d'entrée. Pour plus d'informations sur les annotations TLS mutuelles sur les contrôleurs NGINX, consultez la section Authentification par certificat client dans la documentation de Kubernetes.

> **Important**
>
> Ce modèle utilise des certificats auto-signés. Nous vous recommandons d'utiliser ce modèle uniquement avec les clusters de test, et non dans les environnements de production. Si vous souhaitez utiliser ce modèle dans un environnement de production, vous pouvez utiliser AWS Private Certificate Authority (AWS Private CA) ou votre norme d'infrastructure à clé publique (PKI) existante pour émettre des certificats privés.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif.
- Un cluster Amazon EKS existant.

- Interface de ligne de commande AWS (AWS CLI) version 1.7 ou ultérieure, installée et configurée sur macOS, Linux ou Windows.
- L'utilitaire de ligne de commande kubectl, installé et configuré pour accéder au cluster Amazon EKS. Pour plus d'informations à ce sujet, consultez la section Installation de kubectl dans la documentation Amazon EKS.
- Nom DNS (Domain Name System) existant pour tester l'application.

Limites

- Ce modèle utilise des certificats auto-signés. Nous vous recommandons d'utiliser ce modèle uniquement avec les clusters de test, et non dans les environnements de production.

Architecture

Pile technologique

- Amazon EKS
- Amazon Route 53
- Kubectl

Outils

- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.
- Kubectl est un utilitaire de ligne de commande que vous utilisez pour interagir avec un cluster Amazon EKS.

Épopées

Générez les certificats auto-signés

Tâche	Description	Compétences requises
Générez la clé et le certificat CA.	Générez la clé et le certificat de l'autorité de certification (CA) en exécutant la commande suivante. `openssl req -x509 -sha256 -newkey rsa:4096 -keyout ca.key -out ca.crt -days 356 -nodes -subj '/CN=Test Cert Authority'`	DevOps ingénieur
Générez la clé du serveur et le certificat, puis signez avec le certificat CA.	Générez la clé du serveur et le certificat, puis signez avec le certificat CA en exécutant la commande suivante. `openssl req -new -newkey rsa:4096 -keyout server.key -out server.csr -nodes -subj '/CN= <your_domain_name> ' && openssl x509 -req -sha256 -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt` **Important** Assurez-vous de le remplacer <your_dom	DevOps ingénieur

Tâche	Description	Compétences requises
	`ain_name>` par votre nom de domaine existant.	
Générez la clé client et le certificat, puis signez avec le certificat CA.	Générez la clé client et le certificat, puis signez avec le certificat CA en exécutant la commande suivante. `openssl req -new -newkey rsa:4096 -keyout client.key -out client.csr -nodes -subj '/CN=Test' && openssl x509 -req -sha256 -days 365 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -out client.crt`	DevOps ingénieur

Déployez le contrôleur d'entrée NGINX

Tâche	Description	Compétences requises
Déployez le contrôleur d'entrée NGINX dans votre cluster Amazon EKS.	Déployez le contrôleur d'entrée NGINX à l'aide de la commande suivante. `kubectl apply -f https://raw.githubusercontent.com/kubernetes/ingress-nginx/controller-v1.7.0/deploy/static/provider/aws/deploy.yaml`	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez que le service du contrôleur d'entrée NGINX est en cours d'exécution.	Vérifiez que le service du contrôleur d'entrée NGINX est en cours d'exécution à l'aide de la commande suivante. `kubectl get svc -n ingress-nginx` **Important** Assurez-vous que l'adresse du champ de service contient le nom de domaine du Network Load Balancer.	DevOps ingénieur

Créez un espace de noms dans le cluster Amazon EKS pour tester le protocole TLS mutuel

Tâche	Description	Compétences requises
Créez un espace de noms dans le cluster Amazon EKS.	Créez un espace de noms appelé `mtls` dans votre cluster Amazon EKS en exécutant la commande suivante. `kubectl create ns mtls` Cela déploie l'exemple d'application pour tester le protocole TLS mutuel.	DevOps ingénieur

Création du déploiement et du service pour l'exemple d'application

Tâche	Description	Compétences requises

Créez le déploiement et le service Kubernetes dans l'espace de noms MTLS.	Créez un fichier nommé `mtls.yaml` . Collez le code suivant dans le fichier.
	
	`kind: Deployment`
	`apiVersion: apps/v1`
	`metadata:`
	`  name: mtls-app`
	`  labels:`
	`  app: mtls`
	`spec:`
	`  replicas: 1`
	`  selector:`
	`  matchLabels:`
	`  app: mtls`
	`  template:`
	`  metadata:`
	`  labels:`
	`  app: mtls`
	`  spec:`
	`  containers:`
	`  - name: mtls-app`
	`  image: hashicorp/http-echo`
	`  args:`
	`  - "-text=mTLS is working"`
	
	`---`
	
	`kind: Service`
	`apiVersion: v1`
	`metadata:`
	`  name: mtls-service`
	`spec:`
	`  selector:`
	`  app: mtls`
		DevOps ingénieur

Tâche	Description	Compétences requises

	`ports:`
	`- port: 5678 #`
	`Default port for image`
	
	Créez le déploiement et le service Kubernetes dans l'espace de `mtls` noms en exécutant la commande suivante.
	
	`kubectl create -f mtls.yaml -n mtls`	

Vérifiez que le déploiement de Kubernetes est créé.	Exécutez la commande suivante pour vérifier que le déploiement est créé et qu'un pod est disponible. `kubectl get deploy -n mtls`	DevOps ingénieur
Vérifiez que le service Kubernetes est créé.	Vérifiez que le service Kubernetes est créé en exécutant la commande suivante. `kubectl get service -n mtls`	DevOps ingénieur

Création d'un secret dans l'espace de noms MTLS

Tâche	Description	Compétences requises
Créez un secret pour la ressource d'entrée.	Exécutez la commande suivante pour créer un secret	DevOps ingénieur

Tâche	Description	Compétences requises
	pour le contrôleur d'entrée NGINX en utilisant les certificats que vous avez créés précédemment. `kubectl create secret generic mtls-certs --from-file=tls.crt=server.crt --from-file=tls.key=server.key --from-file=ca.crt=ca.crt -n mtls` Votre secret contient un certificat de serveur permettant au client d'identifier le serveur et un certificat CA permettant au serveur de vérifier les certificats du client.	

Créez la ressource d'entrée dans l'espace de noms mtls

Tâche	Description	Compétences requises

Créez la ressource d'entrée dans l'espace de noms MTLS.	Créez un fichier nommé `ingress.yaml` . Collez le code suivant dans le fichier (remplacez-le `<your_domain_name>` par votre nom de domaine existant).
	
	`apiVersion: networking.k8s.io/v1`
	`kind: Ingress`
	`metadata:`
	`  annotations:`
		DevOps ingénieur

Tâche	Description	Compétences requises

	<pre> nginx.ingress.kube
	rnetes.io/auth-tls-
	verify-client: "on"
	    nginx.ingress.kube
	rnetes.io/auth-tls-
	secret: mtls/mtls-certs
	  name: mtls-ingress
	spec:
	  ingressClassName:
	 nginx
	  rules:
	  - host: "*.<your_
	domain_name>"
	    http:
	      paths:
	      - path: /
	        pathType: Prefix
	        backend:
	          service:
	            name: mtls-
	service
	            port:
	              number:
	 5678
	  tls:
	  - hosts:
	    - "*.<your_
	domain_name>"
	    secretName: mtls-
	certs</pre>
	Créez la ressource d'entrée dans l'espace de `mtls` noms en exécutant la commande suivante.
	<pre>kubectl create -f
	 ingress.yaml -n mtls</pre>	

Tâche	Description	Compétences requises
	Cela signifie que le contrôleur d'entrée NGINX peut acheminer le trafic vers votre exemple d'application.	
Vérifiez que la ressource d'entrée est créée.	Vérifiez que la ressource d'entrée est créée en exécutant la commande suivante. `kubectl get ing -n mtls` **Important** Assurez-vous que l'adresse de la ressource d'entrée indique l'équilibreur de charge créé pour le contrôleur d'entrée NGINX.	DevOps ingénieur

Configurer le DNS pour qu'il pointe le nom d'hôte vers l'équilibreur de charge

Tâche	Description	Compétences requises
Créez un enregistrement CNAME qui pointe vers l'équilibreur de charge du contrôleur d'entrée NGINX.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon Route 53 et créez un enregistrement Canonical Name (CNAME) qui pointe `mtls.<your_domain_name>` vers	DevOps ingénieur

Tâche	Description	Compétences requises
	l'équilibreur de charge du contrôleur d'entrée NGINX. Pour plus d'informations, consultez la section Création d'enregistrements à l'aide de la console Route 53 dans la documentation Route 53.	

Tester l'application

Tâche	Description	Compétences requises
Testez la configuration mutuelle du protocole TLS sans certificats.	Exécutez la commande suivante. `curl -k https://mtls.<your_domain_name>` Vous devriez recevoir le message d'erreur « 400 Aucun certificat SSL requis n'a été envoyé ».	DevOps ingénieur
Testez la configuration mutuelle du protocole TLS avec des certificats.	Exécutez la commande suivante. `curl -k https://mtls.<your_domain_name> --cert client.crt --key client.key` Vous devriez recevoir la réponse « mTLS fonctionne ».	DevOps ingénieur

Ressources connexes

- Création d'enregistrements à l'aide de la console Amazon Route 53
- Utilisation d'un Network Load Balancer avec le contrôleur d'entrée NGINX sur Amazon EKS
- Authentification par certificat client

Automatisez la création de ressources AppStream 2.0 à l'aide d'AWS CloudFormation

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Ce modèle fournit des exemples de code et des étapes pour automatiser la création de ressources Amazon AppStream 2.0 dans le cloud Amazon Web Services (AWS) à l'aide d'un CloudFormation modèle AWS. Le modèle vous montre comment utiliser une CloudFormation pile AWS pour automatiser la création de vos ressources d'application AppStream 2.0, notamment un générateur d'images, une image, une instance de flotte et une pile. Vous pouvez diffuser votre application AppStream 2.0 aux utilisateurs finaux sur un navigateur HTML5 compatible en utilisant le mode de livraison de bureau ou d'application.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une acceptation des termes et conditions de la AppStream version 2.0
- Connaissance de base des AppStream ressources, telles que les piles, lesflottes et les générateurs d'images

Limites

- Vous ne pouvez pas modifier le rôle AWS Identity and Access Management (IAM) associé à une instance AppStream 2.0 une fois celle-ci créée.
- Vous ne pouvez pas modifier les propriétés (telles que le sous-réseau ou le groupe de sécurité) sur l'instance du générateur d'images AppStream 2.0 une fois ce générateur d'images créé.

Architecture

Le schéma suivant montre comment automatiser la création de ressources AppStream 2.0 à l'aide d'un CloudFormation modèle AWS.

Le schéma suivant illustre le flux de travail suivant :

1. Vous créez un CloudFormation modèle AWS basé sur le code YAML dans la section Informations supplémentaires de ce modèle.
2. Le CloudFormation modèle AWS crée une pile de CloudFormation tests AWS.
   a. (Facultatif) Vous créez une instance de générateur d'images à l'aide de la AppStream version 2.0.
   b. (Facultatif) Vous créez une image Windows à l'aide de votre logiciel personnalisé.
3. La CloudFormation pile AWS crée une instance et une pile de flotte AppStream 2.0.
4. Vous déployez vos ressources AppStream 2.0 auprès des utilisateurs finaux sur un navigateur HTML5 compatible.

Pile technologique

- Amazon AppStream 2.0
- AWS CloudFormation

Outils

- Amazon AppStream 2.0 est un service de streaming d'applications entièrement géré qui vous permet d'accéder instantanément à vos applications de bureau où que vous soyez. AppStream La version 2.0 gère les ressources AWS requises pour héberger et exécuter vos applications, évolue automatiquement et fournit un accès à vos utilisateurs à la demande.
- AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.

Épopées

(Facultatif) Créez une image AppStream 2.0

Tâche	Description	Compétences requises
Installez un logiciel personnalisé et créez une image.	1. Installez l'application AppStream 2.0 que vous	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
	prévoyez de déployer auprès de vos utilisateurs. 2. Utilisez l'agent de création d'image Photon ou un PowerShell script pour créer une nouvelle image Windows pour votre logiciel personnalisé. **Note** Envisagez d'utiliser la AppLocker fonctionn alité Windows pour verrouiller davantage l'image.	

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Mettez à jour le CloudForm ation modèle AWS.	1. Enregistrez le code dans la section Informations supplémentaires de ce modèle sous forme de fichier YAML. 2. Mettez à jour le fichier YAML avec les valeurs requises pour les paramètre s de votre environnement.	Administrateur système AWS, administrateur cloud, architect e cloud, AWS général, administrateur AWS

Tâche	Description	Compétences requises
Créez une CloudFormation pile AWS à l'aide du modèle.	1. Connectez-vous à la console de gestion AWS et ouvrez la CloudFormation console AWS. 2. Dans le volet de navigation, choisissez Stacks. 3. Choisissez Créer une pile, puis choisissez Avec de nouvelles ressources (standard). 4. Dans la section Prérequis — Préparer le modèle, sélectionnez Le modèle est prêt. 5. Dans la section Spécifier le modèle, choisissez Télécharger un fichier modèle. 6. Choisissez Choisir un fichier, puis choisissez votre CloudFormation modèle AWS mis à jour. 7. Effectuez le reste des étapes de l'assistant pour créer votre pile.	Propriétaire de l'application, administrateur système AWS, ingénieur Windows

Ressources connexes

Références

- Commencez avec Amazon AppStream 2.0 : configuration à l'aide d'exemples d'applications
- Créez une flotte et une pile AppStream 2.0

Tutoriels et vidéos

- Flux de travail utilisateur Amazon AppStream 2.0
- Comment migrer une ancienne application Windows Forms vers Amazon AppStream 2.0
- AWS re:Invent 2018 : déployez des applications de bureau en toute sécurité avec Amazon AppStream 2.0 (01) BAP2

Informations supplémentaires

Le code suivant est un exemple de CloudFormation modèle AWS qui vous permet de créer automatiquement des ressources AppStream 2.0.

```
AWSTemplateFormatVersion: 2010-09-09
Parameters:
  SubnetIds:
    Type: 'List<AWS::EC2::Subnet::Id>'
  testSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup::Id'
  ImageName:
    Type: String
Resources:

  AppStreamFleet:
    Type: 'AWS::AppStream::Fleet'
    Properties:
      ComputeCapacity:
        DesiredInstances: 5
      InstanceType: stream.standard.medium
      Name: appstream-test-fleet
      DisconnectTimeoutInSeconds: 1200
      FleetType: ON_DEMAND
      IdleDisconnectTimeoutInSeconds: 1200
      ImageName: !Ref ImageName
      MaxUserDurationInSeconds: 345600
      VpcConfig:
        SecurityGroupIds:
          - !Ref testSecurityGroup
        SubnetIds: !Ref SubnetIds
  AppStreamStack:
    Type: 'AWS::AppStream::Stack'
    Properties:
```

```
      Description: AppStream stack for test
      DisplayName: AppStream test Stack
      Name: appstream-test-stack
      StorageConnectors:
        - ConnectorType: HOMEFOLDERS
      UserSettings:
        - Action: CLIPBOARD_COPY_FROM_LOCAL_DEVICE
          Permission: ENABLED
        - Action: CLIPBOARD_COPY_TO_LOCAL_DEVICE
          Permission: ENABLED
        - Action: FILE_DOWNLOAD
          Permission: ENABLED
        - Action: PRINTING_TO_LOCAL_DEVICE
          Permission: ENABLED
  AppStreamFleetAssociation:
    Type: 'AWS::AppStream::StackFleetAssociation'
    Properties:
      FleetName: appstream-test-fleet
      StackName: appstream-test-stack
    DependsOn:
      - AppStreamFleet
      - AppStreamStack
```

Créez un analyseur de journaux personnalisé pour Amazon ECS à l'aide d'un routeur de journaux Firelens

Créée par Varun Sharma (AWS)

Récapitulatif

Firelens est un routeur de journaux pour Amazon Elastic Container Service (Amazon ECS) et AWS Fargate. Vous pouvez utiliser Firelens pour acheminer les journaux de conteneurs d'Amazon ECS vers Amazon CloudWatch et d'autres destinations (par exemple, Splunk ou Sumo Logic). Firelens fonctionne avec Fluentd ou Fluent Bit comme agent de journalisation, ce qui signifie que vous pouvez utiliser les paramètres de définition des tâches Amazon ECS pour acheminer les journaux.

En choisissant d'analyser les journaux au niveau de la source, vous pouvez analyser vos données de journalisation et effectuer des requêtes afin de répondre de manière plus efficace aux problèmes opérationnels. Étant donné que les différentes applications ont des modèles de journalisation différents, vous devez utiliser un analyseur personnalisé qui structure les journaux et facilite les recherches à destination finale.

Ce modèle utilise un routeur de journaux Firelens avec un analyseur personnalisé pour transférer les journaux CloudWatch depuis un exemple d'application Spring Boot s'exécutant sur Amazon ECS. Vous pouvez ensuite utiliser Amazon CloudWatch Logs Insights pour filtrer les journaux en fonction des champs personnalisés générés par l'analyseur personnalisé.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée sur votre machine locale.
- Docker, installé et configuré sur votre machine locale.
- Une application conteneurisée basée sur Spring Boot existante sur Amazon Elastic Container Registry (Amazon ECR).

Architecture

Pile technologique

- CloudWatch
- Amazon ECR
- Amazon ECS
- Fargate
- Docker
- Fluent Bit

Outils

- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs géré par AWS qui est sécurisé, évolutif et fiable.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif qui facilite l'exécution, l'arrêt et la gestion des conteneurs sur un cluster.
- AWS Identity and Access Management (IAM) — IAM est un service Web permettant de contrôler en toute sécurité l'accès aux services AWS.
- AWS CLI — AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS à l'aide de commandes dans votre shell de ligne de commande.
- Docker — Docker est une plateforme ouverte pour le développement, l'expédition et l'exécution d'applications.

Code

Les fichiers suivants sont joints à ce modèle :

- `customFluentBit.zip`— Contient les fichiers permettant d'ajouter l'analyse et les configurations personnalisées.
- `firelens_policy.json`— Contient le document de stratégie permettant de créer une politique IAM.
- `Task.json`— Contient un exemple de définition de tâche pour Amazon ECS.

Épopées

Création d'une image Fluent Bit personnalisée

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon ECR et créez un référentiel appelé`fluentbit_custom` . Pour plus d'informations à ce sujet, consultez la section Création d'un référentiel dans la documentation Amazon ECR.	Administrateur système, Développeur
Décompressez le package customFluentBit .zip.	1. Téléchargez le `customFluentBit.zip` package (joint) sur votre ordinateur local. 2. Décompressez le fichier `customFluentBit` dans le répertoire en exécutant la commande suivante : `unzip -d customFluentBit.zip` 3. Le répertoire contient les fichiers suivants qui sont nécessaires pour ajouter l'analyse et les configurations personnalisées : • `parsers/springboot_parser.conf` —	

Tâche	Description	Compétences requises
	Contient la directive de l'analyseur et définit le modèle d'expression régulière (regex) pour l'analyseur personnalisé. Vous pouvez ajouter le modèle regex pour votre analyseur spécifique. • `conf/parse_springboot.conf` — Contient le filtre et la directive de service. • Le Dockerfile	

Tâche	Description	Compétences requises
Créez l'image Docker personnalisée.	1. Remplacez le répertoire par `customFluentBit` . 2. Ouvrez la console Amazon ECR, choisissez le `fluentbit_custom` référentiel, puis sélectionnez Afficher les commandes push. 3. Téléchargez votre projet. 4. Une fois le téléchargement terminé, copiez l'URL du build. Cette URL est obligatoire lorsque vous créez un conteneur dans Amazon ECS Pour plus d'informations à ce sujet, consultez la section Pushing a Docker image dans la documentation Amazon ECR.	Administrateur système, Développeur

Configuration du cluster Amazon ECS

Tâche	Description	Compétences requises
Créez un nouveau cluster Amazon ECS.	Créez un cluster Amazon ECS en suivant les instructions de la section Modèle de mise en réseau uniquement de la section Création d'un cluster de la documentation Amazon ECS.	Administrateur système, Développeur

Tâche	Description	Compétences requises
	Note Assurez-vous de choisir Create VPC pour créer un nouveau cloud privé virtuel (VPC) pour votre cluster Amazon ECS.	

Configuration de la tâche Amazon ECS

Tâche	Description	Compétences requises
Configurez le rôle IAM d'exécution de tâches Amazon ECS.	Créez un rôle IAM d'exécution de tâches Amazon ECS à l'aide de la politique `AmazonECSTaskExecutionRolePolicy` gérée. Pour plus d'informations à ce sujet, consultez le rôle IAM d'exécution de tâches Amazon ECS dans la documentation Amazon ECS. **Note** Assurez-vous d'enregistrer le nom de ressource Amazon (ARN) du rôle IAM.	Administrateur système, Développeur
Associez la politique IAM au rôle IAM d'exécution des tâches Amazon ECS.	1. Créez une politique IAM à l'aide du document de stratégie `firelens_`	Administrateur système, Développeur

Tâche	Description	Compétences requises
	`policy.json` (joint). Pour plus d'informations à ce sujet, consultez la section Création de politiques dans l'onglet JSON de la documentation IAM. 2. Associez cette politique au rôle IAM d'exécution de tâches Amazon ECS que vous avez créé précédemment. Pour plus d'informations à ce sujet, consultez la section Ajout de politiques IAM (CLI AWS) dans la documentation IAM.	

Tâche	Description	Compétences requises
Configurez la définition de tâche Amazon ECS.	1. Mettez à jour les sections suivantes dans l'`Task.json` exemple de définition de tâche (ci-joint) : • Mettre à jour le `executionRoleArn` et `taskRoleArn` avec l'ARN du rôle IAM d'exécution de la tâche • Mettez à jour l'image `containerDefinitions` avec l'image Fluent Bit Docker personnalisée que vous avez créée précédemment • Mettez à jour l'image `containerDefinitions` avec le nom de l'image de votre application 2. Ouvrez la console Amazon ECS, choisissez Définitions de tâches, choisissez Créer une nouvelle définition de tâche, puis choisissez Fargate sur la page de sélection des compatibilités. 3. Choisissez Configurer via Json, collez le `Task.json` fichier mis à jour dans la zone de texte, puis sélectionnez Enregistrer.	Administrateur système, Développeur

Tâche	Description	Compétences requises
	4. Créez la définition de tâche. Pour plus d'informations à ce sujet, consultez la section Création d'une définition de tâche dans la documentation Amazon ECS.	

Exécuter la tâche Amazon ECS

Tâche	Description	Compétences requises
Exécutez la tâche Amazon ECS.	Sur la console Amazon ECS, choisissez Clusters, choisissez le cluster que vous avez créé précédemment, puis exécutez la tâche autonome. Pour plus d'informations à ce sujet, consultez la section Exécuter une tâche autonome dans la documentation Amazon ECS.	Administrateur système, Développeur

Vérifiez les CloudWatch journaux

Tâche	Description	Compétences requises
Vérifiez les journaux.	1. Ouvrez la CloudWatch console, choisissez Log groups, puis choisissez `/aws/ecs/containerinsights/{{cluster`	Administrateur système, Développeur

Tâche	Description	Compétences requises
	`_ARN}}/firelens/application` . 2. Vérifiez les journaux, en particulier les champs personnalisés ajoutés par l'analyseur personnalisé. 3. CloudWatch À utiliser pour filtrer les journaux en fonction des champs personnalisés.	

Ressources connexes

- Notions de base sur Docker pour Amazon ECS
- Amazon ECS sur AWS Fargate
- Configuration des paramètres de service de base

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Création d'un pipeline et d'une AMI à l'aide de CodePipeline and HashiCorp Packer

Créée par Akash Kumar (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle fournit des exemples de code et des étapes pour créer à la fois un pipeline dans le cloud Amazon Web Services (AWS) à l'aide d'AWS CodePipeline et une image machine Amazon (AMI) à l'aide de HashiCorp Packer. Le modèle est basé sur la pratique de l'intégration continue, qui automatise la création et le test du code avec un système de contrôle de version basé sur Git. Dans ce modèle, vous créez et clonez un référentiel de code à l'aide d'AWS CodeCommit. Créez ensuite un projet et configurez votre code source à l'aide d'AWS CodeBuild. Enfin, créez une AMI qui sera validée dans votre référentiel.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une AMI Amazon Linux pour le lancement d'instances Amazon Elastic Compute Cloud (Amazon EC2)
- HashiCorp Packer 0.12.3 ou version ultérieure
- Amazon CloudWatch Events (facultatif)
- Amazon CloudWatch Logs (facultatif)

Architecture

Le schéma suivant montre un exemple de code d'application qui automatise la création d'une AMI en utilisant l'architecture de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Le développeur valide les modifications de code dans un dépôt CodeCommit Git privé. CodePipeline Utilisez-le ensuite CodeBuild pour lancer la génération et ajouter de nouveaux

artefacts prêts à être déployés dans le compartiment Amazon Simple Storage Service (Amazon S3).

2. CodeBuild utilise Packer pour regrouper et empaqueter l'AMI en fonction d'un modèle JSON. Si cette option est activée, CloudWatch Events peut démarrer automatiquement le pipeline lorsqu'une modification survient dans le code source.

Pile technologique

- CodeBuild
- CodeCommit
- CodePipeline
- CloudWatch Événements (facultatif)

Outils

- AWS CodeBuild — AWS CodeBuild est un service de création entièrement géré dans le cloud. CodeBuild compile votre code source, exécute des tests unitaires et produit des artefacts prêts à être déployés.
- AWS CodeCommit — AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git dans le cloud AWS. CodeCommit vous n'avez plus à gérer votre propre système de contrôle de source ou à vous soucier de la mise à l'échelle de son infrastructure.
- AWS CodePipeline — AWS CodePipeline est un service de livraison continue que vous pouvez utiliser pour modéliser, visualiser et automatiser les étapes nécessaires à la publication de votre logiciel.
- HashiCorp Packer — HashiCorp Packer est un outil open source permettant d'automatiser la création d'images de machine identiques à partir d'une configuration source unique. Packer est léger, fonctionne sur tous les principaux systèmes d'exploitation et crée des images de machine pour plusieurs plateformes en parallèle.

Code

Ce modèle inclut les pièces jointes suivantes :

- `buildspec.yml`— Ce fichier est utilisé CodeBuild pour créer et créer un artefact à déployer.

- `amazon-linux_packer-template.json`— Ce fichier utilise Packer pour créer une AMI Amazon Linux.

Épopées

Configuration du référentiel de code

Tâche	Description	Compétences requises
Créez le référentiel.	Créez un CodeCommit référentiel.	Administrateur système AWS
Pour cloner le référentiel.	Connectez-vous au CodeCommit référentiel en le clonant.	Développeur d'applications
Transférez le code source vers le dépôt distant.	1. Créez un commit pour ajouter les `amazon-linux_packer-template.json` fichiers `buildspec.yml` et à votre dépôt local. 2. Transférez le commit de votre dépôt local vers le CodeCommit référentiel distant.	Développeur d'applications

Création d'un CodeBuild projet pour l'application

Tâche	Description	Compétences requises
Créez un projet de génération.	1. Connectez-vous à la console de gestion AWS, ouvrez la CodeBuild console AWS, puis	Développeur d'applications, administrateur système AWS

Tâche	Description	Compétences requises
	choisissez Create build project. 2. Dans le champ Nom du projet, entrez le nom de votre projet. 3. Dans le champ Source provider, choisissez AWS CodeCommit. 4. Pour Repository, choisissez le référentiel dans lequel vous souhaitez créer le pipeline de code. 5. Pour Image d'environnement, choisissez Image gérée ou Image personnalisée. 6. Pour Système d'exploitation, choisissez Ubuntu. 7. Pour RunTime(s), choisissez Standard. 8. Pour Image, choisissez aws/codebuild/standard : 4.0. 9. Pour la version image, choisissez Toujours utiliser la dernière image pour cette version d'exécution. 10. Dans Environnement, choisissez Linux. 11. Cochez la case Privileged. 12. Pour Rôle de service, choisissez Nouveau rôle de	

Tâche	Description	Compétences requises
	service ou Rôle de service existant. 13. Pour les spécifications de construction, choisissez Utiliser un fichier de spécification de construction ou Insérer des commandes de construction. 14. (Facultatif) Dans le champ Type dans la section Artefacts, sélectionnez Aucun artefact. 15. (Recommandé) Pour télécharger les journaux de sortie de build dans CloudWatch Logs, sélectionnez CloudWatch logs. 16. (Facultatif) Pour télécharger les journaux de sortie de build sur Amazon S3, cochez la case Journaux S3. 17. Choisissez Créer un projet de génération.	

Configuration du pipeline

Tâche	Description	Compétences requises
Nom du pipeline	1. Connectez-vous à la console de gestion AWS, ouvrez la CodePipel	Développeur d'applications, administrateur système AWS

Tâche	Description	Compétences requises
	ine console AWS, puis choisissez Create pipeline. 2. Dans Nom du pipeline, entrez un nom pour le pipeline. 3. Pour Rôle de service, choisissez Nouveau rôle de service ou Rôle de service existant. 4. Dans le champ Role name (Nom de rôle), saisissez un nom pour votre rôle. 5. Dans la section Paramètres avancés, pour le magasin d'artifacts, choisissez Emplacement par défaut si vous souhaitez qu'Amazon S3 crée un compartiment et y stocke les artefacts. Pour utiliser un compartiment S3 existant, choisissez Emplacement personnalisé. Choisissez Suivant. 6. Dans le champ Source provider, choisissez AWS CodeCommit. 7. Dans Nom du référentiel, choisissez le référentiel que vous avez cloné précédemment. Dans Nom de la branche, choisissez votre branche de code source.	

Tâche	Description	Compétences requises
	8. Pour les options de détection des modifications, choisissez Amazon CloudWatch Events (recommandé) pour démarrer le pipeline ou AWS CodePipeline pour vérifier régulièrement les modifications. Choisissez Suivant. 9. Dans le champ Build provider, choisissez AWS CodeBuild. 10. Dans Nom du projet, choisissez le projet de construction que vous avez créé dans l'épopée Créer un CodeBuild projet pour l'application. 11. Choisissez vos options de compilation, puis cliquez sur Suivant. 12. Choisissez Ignorer l'étape de déploiement. 13. Choisissez Créer un pipeline.	

Ressources connexes

- Utilisation de référentiels dans AWS CodeCommit
- Utilisation des projets de génération
- Travailler avec des pipelines dans CodePipeline

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez un pipeline et déployez des mises à jour d'artefacts sur des instances locales à l'aide de EC2 CodePipeline

Créée par Akash Kumar (AWS) et Sandeep Reddy Jogammagari (AWS)

Récapitulatif

Ce modèle fournit des exemples de code et des étapes pour créer un pipeline dans le cloud Amazon Web Services (AWS) et déployer des artefacts mis à jour sur des instances Amazon Elastic Compute Cloud (Amazon EC2) sur site dans AWS CodePipeline. Le modèle est basé sur la pratique de l'intégration continue. Cette pratique automatise la création et le test du code à l'aide d'un système de contrôle de version basé sur Git. Dans ce modèle, vous créez et clonez un référentiel de code à l'aide d'AWS CodeCommit. Ensuite, vous créez un projet et configurez votre code source à l'aide d'AWS CodeBuild. Enfin, vous créez votre application et configurez son environnement cible pour les EC2 instances sur site à l'aide d'AWS CodeDeploy.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Balises définies par l'utilisateur pour identifier les EC2 instances lors du déploiement
- CodeDeploy agent, installé sur les EC2 instances
- Le logiciel d'exécution requis, installé sur les EC2 instances
- Amazon Corretto 8 pour le kit de développement Java
- Serveur Web Apache Tomcat, installé
- Amazon CloudWatch Events (facultatif)
- Une paire de clés pour se connecter au serveur Web (facultatif)
- Un projet d'application Apache Maven pour une application Web

Architecture

Le schéma suivant montre un exemple d'application Web Java déployée sur des EC2 instances locales à l'aide de l'architecture de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Le développeur valide les modifications de code dans un dépôt CodeCommit Git privé.
2. CodePipeline utilise CodeBuild pour lancer la construction et ajouter de nouveaux artefacts prêts à être déployés dans le compartiment Amazon Simple Storage Service (Amazon S3).
3. CodePipeline utilise l' CodeDeploy agent pour préinstaller toutes les dépendances requises pour les modifications des artefacts de déploiement.
4. CodePipeline utilise l' CodeDeploy agent pour déployer les artefacts du compartiment S3 vers les EC2 instances cibles. Si cette option est activée, CloudWatch Events peut démarrer automatiquement le pipeline lorsqu'une modification se produit dans le code source.

Pile technologique

- CodeBuild
- CodeCommit
- CodeDeploy
- CodePipeline
- CloudWatch Événements (facultatif)

Outils

- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés. CodeBuild compile votre code source, exécute des tests unitaires et produit des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS CodeDeploy automatise les déploiements vers Amazon Elastic Compute Cloud EC2 (Amazon) ou des instances sur site, les fonctions AWS Lambda ou les services Amazon Elastic Container Service (Amazon ECS).
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.

Code

Ce modèle inclut les pièces jointes suivantes :

- `buildspec.yml`— Ce fichier spécifie les actions qui CodeBuild nécessitent de créer et de créer un artefact pour le déploiement.
- `appspec.yml`— Ce fichier spécifie les actions CodeDeploy requises pour créer une application et configurer un environnement cible pour les EC2 instances locales.
- `install_dependencies.sh`— Ce fichier installe les dépendances du serveur Web Apache Tomcat.
- `start_server.sh`— Ce fichier démarre le serveur Web Apache Tomcat.
- `stop_server.sh`— Ce fichier arrête le serveur Web Apache Tomcat.

Épopées

Configuration du référentiel de code

Tâche	Description	Compétences requises
Créez le référentiel.	Créez un CodeCommit référentiel.	Administrateur système AWS
Pour cloner le référentiel.	Connectez-vous au CodeCommit référentiel en le clonant.	Développeur d'applications
Transférez le code source vers le dépôt distant.	1. Créez un commit pour ajouter les `appspec.yml` fichiers `buildspec.yml` et à votre dépôt local. 2. Transférez le commit de votre dépôt local vers le CodeCommit référentiel distant.	Développeur d'applications

Création d'un CodeBuild projet pour l'application

Tâche	Description	Compétences requises
Créez un projet de génération.	1. Connectez-vous à l'AWS Management Console, ouvrez la CodeBuild console AWS, puis choisissez Create build project. 2. Dans Nom du projet, entrez le nom de votre projet. 3. Dans le champ Source provider, choisissez AWS CodeCommit. 4. Pour Repository, choisissez le référentiel dans lequel vous souhaitez créer le pipeline de code. 5. Pour Image d'environnement, choisissez Image gérée ou Image personnalisée. 6. Pour Operating system (Système d'exploitation), choisissez Amazon Linux 2. **Note** Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez	Administrateur AWS, développeur d'applications

Tâche	Description	Compétences requises
	Amazon Linux 2 FAQs. 7. Pour RunTime(s), choisissez Standard. 8. Pour Image, choisissez aws/codebuild/amazonlinux2-aarch64-standard:2.0. 9. Pour la version image, choisissez Toujours utiliser la dernière image pour cette version d'exécution. 10. Pour Rôle de service, choisissez Nouveau rôle de service ou Rôle de service existant. 11. Pour les spécifications de construction, choisissez Utiliser un fichier de spécification de construction ou Insérer des commandes de construction. 12. (Facultatif) Choisissez Ajouter un artefact pour configurer les artefacts. 13. (Facultatif) Pour télécharger les journaux de sortie de build sur Amazon CloudWatch, sélectionnez CloudWatch logs.	

Tâche	Description	Compétences requises
	14. Choisissez Créer un projet de génération.	

Configuration du déploiement d'artefacts pour les instances sur site EC2

Tâche	Description	Compétences requises
Créez l'application.	1. Connectez-vous à l'AWS Management Console, ouvrez la CodeDeploy console AWS, puis choisissez Create application. 2. Dans Nom de l'application, entrez le nom de votre application. 3. Pour la plateforme de calcul, choisissez EC2/On-premises. 4. Choisissez Créer une application, puis Créer un groupe de déploiement. 5. Pour Nom du groupe de déploiement, entrez un nom. 6. **Note** Créez un rôle de service pour CodeDeploy. : le rôle de service doit disposer des autorisat	Administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
	ions nécessair es pour autoriser CodeDeploy l'accès à votre environne ment cible. 7. Pour Rôle de service, choisissez le rôle de service que vous avez créé à l'étape 6. 8. Pour le type de déploieme nt, choisissez sur place ou bleu/vert en fonction des besoins de votre entreprise. 9. Pour la configuration de l'environnement, choisisse z les options qui répondent aux exigences de votre entreprise. 10. (Facultatif) Créez un groupe cible pour votre équilibre ur de charge séparémen t dans la EC2 console Amazon, puis revenez à la page Créer un groupe de déploiement de la CodeDeploy console AWS pour choisir votre équilibre ur de charge et votre groupe cible. 11. Choisissez Créer un groupe de déploiement.	

Configuration du pipeline

Tâche	Description	Compétences requises
Créez le pipeline.	1. Connectez-vous à l'AWS Management Console, ouvrez la CodePipeline console AWS, puis choisissez Create pipeline. 2. Dans Nom du pipeline, entrez un nom pour le pipeline. 3. Pour Rôle de service, choisissez Nouveau rôle de service ou Rôle de service existant. 4. Dans le champ Role name (Nom de rôle), saisissez un nom pour votre rôle. 5. Dans la section Paramètres avancés, pour Artifact store, choisissez Default location si vous souhaitez qu'Amazon S3 crée un bucket et stocke les artefacts dans le bucket. Pour utiliser un compartiment S3 existant, choisissez Emplacement personnalisé. Choisissez Suivant. 6. Dans le champ Source provider, choisissez AWS CodeCommit. 7. Dans Nom du référentiel, choisissez le référenti	Administrateur système AWS, développeur d'applications

Tâche	Description	Compétences requises
	el que vous avez cloné précédemment. Dans Nom de la branche, choisisse z votre branche de code source. 8. Pour les options de détection des modificat ions, choisissez Amazon CloudWatch Events (recommandé) ou AWS CodePipeline. Choisissez Suivant. 9. Dans le champ Build provider, choisissez AWS CodeBuild. 10. Pour Nom du projet, choisissez le projet de construction que vous avez créé dans la section Créer un CodeBuild projet pour l'application de ce modèle. 11. Choisissez vos options de compilation, puis cliquez sur Suivant. 12. Dans le champ Deploy provider, choisissez AWS CodeDeploy. 13. Choisissez un nom d'application et un groupe de déploiement, puis choisissez Next. 14. Choisissez Créer un pipeline.	

Ressources connexes

- Utilisation de référentiels dans AWS CodeCommit
- Utilisation des projets de génération
- Utilisation d'applications dans CodeDeploy
- Travailler avec des pipelines dans CodePipeline

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez automatiquement des pipelines CI dynamiques pour les projets Java et Python

Créée par Aromal Raj Jayarajan (AWS), Amarnath Reddy (AWS), MAHESH RAGHUNANDANAN (AWS) et Vijesh Vijayakumaran Nair (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle montre comment créer automatiquement des pipelines d'intégration continue (CI) dynamiques pour les projets Java et Python à l'aide des outils de développement AWS.

À mesure que les technologies se diversifient et que les activités de développement augmentent, il peut devenir difficile de créer et de maintenir des pipelines de CI cohérents au sein d'une organisation. En automatisant le processus dans AWS Step Functions, vous pouvez vous assurer que l'utilisation et l'approche de vos pipelines CI sont cohérentes.

Pour automatiser la création de pipelines CI dynamiques, ce modèle utilise les entrées variables suivantes :

- Langage de programmation (Java ou Python uniquement)
- Nom du pipeline
- Étapes de pipeline requises

> **Note**
>
> Step Functions orchestre la création de pipelines en utilisant plusieurs services AWS. Pour plus d'informations sur les services AWS utilisés dans cette solution, consultez la section Outils de ce modèle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

- Un compartiment Amazon S3 dans la même région AWS où cette solution est déployée
- Un responsable d'AWS Identity and Access Management (IAM) disposant des CloudFormation autorisations AWS requises pour créer les ressources nécessaires à cette solution

Limites

- Ce modèle ne prend en charge que les projets Java et Python.
- Les rôles IAM fournis selon ce modèle suivent le principe du moindre privilège. Les autorisations des rôles IAM doivent être mises à jour en fonction des ressources spécifiques que votre pipeline CI doit créer.

Architecture

Pile technologique cible

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Systems Manager
- AWS Step Functions
- AWS Lambda
- Amazon DynamoDB

Architecture cible

Le schéma suivant montre un exemple de flux de travail permettant de créer automatiquement des pipelines de CI dynamiques pour des projets Java et Python à l'aide des outils de développement AWS.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur AWS fournit les paramètres d'entrée pour la création d'un pipeline CI au format JSON. Cette entrée lance un flux de travail Step Functions (machine à états) qui crée un pipeline CI à l'aide des outils de développement AWS.
2. Une fonction Lambda lit un dossier nommé input-reference, qui est stocké dans un compartiment Amazon S3, puis génère un fichier buildspec.yml. Ce fichier généré définit les étapes du pipeline CI et est stocké dans le même compartiment Amazon S3 qui stocke les références de paramètres.
3. Step Functions vérifie les dépendances du flux de création du pipeline CI pour détecter toute modification et met à jour la pile de dépendances selon les besoins.
4. Step Functions crée les ressources du pipeline CI dans une CloudFormation pile, y compris un CodeCommit référentiel, un CodeBuild projet et un CodePipeline pipeline.
5. La CloudFormation pile copie l'exemple de code source pour la pile technologique sélectionnée (Java ou Python) et le fichier buildspec.yml dans le référentiel. CodeCommit
6. Les détails d'exécution du pipeline CI sont stockés dans une table DynamoDB.

Automatisation et mise à l'échelle

- Ce modèle est destiné à être utilisé dans un seul environnement de développement uniquement. Des modifications de configuration sont nécessaires pour une utilisation dans plusieurs environnements de développement.
- Pour ajouter la prise en charge de plusieurs CloudFormation piles, vous pouvez créer des CloudFormation modèles supplémentaires. Pour plus d'informations, consultez Getting started with AWS CloudFormation dans la CloudFormation documentation.

Outils

Outils

- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Code

Le code de ce modèle est disponible dans le GitHub automated-ci-pipeline-creationréférentiel. Le référentiel contient les CloudFormation modèles requis pour créer l'architecture cible décrite dans ce modèle.

Bonnes pratiques

- N'entrez pas d'informations d'identification (secrets) telles que des jetons ou des mots de passe directement dans les CloudFormation modèles ou les configurations d'actions Step Functions. Dans ce cas, les informations seront affichées dans les journaux DynamoDB. Utilisez plutôt AWS Secrets Manager pour configurer et stocker des secrets. Référencez ensuite les secrets stockés dans Secrets Manager dans les CloudFormation modèles et les configurations d'action Step Functions selon vos besoins. Pour plus d'informations, consultez la section Qu'est-ce qu'AWS Secrets Manager dans la documentation de Secrets Manager.

- Configurez le chiffrement côté serveur pour les CodePipeline artefacts stockés dans Amazon S3. Pour plus d'informations, consultez Configurer le chiffrement côté serveur pour les artefacts stockés dans Amazon S3 ou CodePipeline dans la CodePipeline documentation.
- Appliquez les autorisations du moindre privilège lors de la configuration des rôles IAM. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.
- Assurez-vous que votre compartiment Amazon S3 n'est pas accessible au public. Pour plus d'informations, consultez la section Configuration du paramètre de blocage de l'accès public pour vos compartiments S3 dans la documentation Amazon S3.
- Assurez-vous d'activer la gestion des versions pour votre compartiment Amazon S3. Pour plus d'informations, consultez la section Utilisation du versionnement dans les compartiments S3 dans la documentation Amazon S3.
- Utilisez IAM Access Analyzer lors de la configuration des politiques IAM. L'outil fournit des recommandations pratiques pour vous aider à créer des politiques IAM sécurisées et fonctionnelles. Pour plus d'informations, consultez la section Utilisation d'AWS Identity and Access Management Access Analyzer dans la documentation IAM.
- Dans la mesure du possible, définissez des conditions d'accès spécifiques lors de la configuration des politiques IAM.
- Activez la CloudWatch journalisation Amazon à des fins de surveillance et d'audit. Pour plus d'informations, consultez Qu'est-ce qu'Amazon CloudWatch Logs ? dans la CloudWatch documentation.

Épopées

Configuration des prérequis

Tâche	Description	Compétences requises
Créez un compartiment Amazon S3.	Créez un compartiment Amazon S3 (ou utilisez un compartiment existant) pour stocker les CloudFormation modèles, le code source et les fichiers d'entrée requis pour la solution.	AWS DevOps

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez Étape 1 : Création de votre premier compartiment S3 dans la documentation Amazon S3. **Note** Le compartiment Amazon S3 doit se trouver dans la même région AWS que celle dans laquelle vous déployez la solution.	
Clonez le GitHub dépôt.	Clonez le GitHub automated-ci-pipeline-creationdépôt en exécutant la commande suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/automated-ci-pipeline-creation.git` Pour plus d'informations, consultez la section Clonage d'un dépôt dans la GitHub documentation.	AWS DevOps

Tâche	Description	Compétences requises
Téléchargez le dossier Solutions Templates depuis le GitHub référentiel cloné vers votre compartiment Amazon S3.	Copiez le contenu du dossier Solution-Templates cloné et chargez-le dans le compartiment Amazon S3 que vous avez créé. Pour plus d'informations, consultez la section Chargement d'objets dans la documentation Amazon S3. **Note** Assurez-vous de télécharger uniquement le contenu du dossier Solution-Templates. Vous pouvez charger les fichiers uniquement au niveau racine du compartiment Amazon S3.	AWS DevOps

Déployez la solution

Tâche	Description	Compétences requises
Créez une CloudFormation pile pour déployer la solution en utilisant le fichier template.yml dans le référentiel cloné. GitHub	1. Connectez-vous à la console de gestion AWS, puis ouvrez la CloudFormation console AWS.	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	2. Sélectionnez Créer la pile. Une liste déroulante apparaît. 3. Dans la liste déroulant e, sélectionnez Avec de nouvelles ressources (standard). La page Créer une pile s'ouvre. 4. Dans la section Spécifier le modèle, cochez la case à côté de Télécharger un fichier modèle. 5. Sélectionnez Choose file (Choisir un fichier). Accédez ensuite au dossier racine du GitHub dépôt cloné et sélectionnez le fichier template.yml. Choisissez ensuite Ouvrir. 6. Choisissez Suivant. La page Spécifier les détails de la pile s'ouvre. 7. Dans la section Paramètre s, spécifiez les paramètres suivants : • Pour S3 TemplateB ucketName, entrez le nom du compartiment Amazon S3 que vous avez créé précédemm ent, qui contient le code source et les référence s de cette solution. Assurez-vous que le	

Tâche	Description	Compétences requises
	paramètre du nom du compartiment est en minuscules. • Pour Dynamo DBTable, entrez le nom de la table DynamoDB créée par la pile. CloudFormation • Pour StateMachineName, entrez un nom pour la machine d'état Step Functions créée par la CloudFormation pile. 8. Choisissez Suivant. La page Configurer les options de pile s'ouvre. 9. Sur la page Configurer les options de pile, choisisse z Suivant. Ne modifiez aucune des valeurs par défaut. La page de révision s'ouvre. 10. Vérifiez les paramètres de création de piles. Choisisse z ensuite Create stack pour lancer votre stack. **Note** Lors de la création de votre pile, elle est répertoriée sur la page Stacks avec le statut CREATE_IN	

Tâche	Description	Compétences requises
	_PROGRESS. Assurez-vous d'attendre que le statut de la pile passe à CREATE_COMPLETE avant de terminer les étapes restantes de ce modèle.	

Tester la configuration

Tâche	Description	Compétences requises
Exécutez la fonction step que vous avez créée.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la console Step Functions. 2. Ouvrez la fonction d'étape que vous avez créée. 3. Choisissez Start execution (Démarrer l'exécution). Entrez ensuite vos valeurs d'entrée pour le flux de travail au format JSON (voir les exemples de saisie suivants). 4. Choisissez Start execution (Démarrer l'exécution). Formatage JSON `{ "details": {`	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	<pre>"tech_stack": "Name of the Tech Stack (python/java)", "project_name": "Name of the Project that you want to create with", "pre_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "post_build": "Choose the step if it required in the buildspec.yml file i.e., yes/no", "reports": "Choose the step if it required in the buildspec.yml file i.e., yes/no", } }</pre> Exemple de saisie Java JSON <pre>{ "details": { "tech_stack": "java", "project_name": "pipeline-java-pjt", "pre_build": "yes", "build": "yes", "post_build": "yes", "reports": "yes"</pre>	

Tâche	Description	Compétences requises

	<pre> }
	}</pre>
	Exemple de saisie JSON en Python
	<pre>{
	  "details": {
	    "tech_stack":
	 "python",
	    "project_name":
	 "pipeline-python-p
	jt",
	    "pre_build": "yes",
	    "build": "yes",
	    "post_build":
	 "yes",
	    "reports": "yes"
	  }
	}</pre>	

Tâche	Description	Compétences requises
Vérifiez que le CodeCommit référentiel pour le pipeline CI a été créé.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la CodeCommit console. 2. Sur la page Référentiels, vérifiez que le nom du CodeCommit référentiel que vous avez créé apparaît dans la liste des référenti els. Le nom du dépôt est ajouté avec ce qui suit : pipeline-java-pjt -Repo 3. Ouvrez le CodeCommi t référentiel et vérifiez que l'exemple de code source ainsi que les fichiers buildspec.yml sont transféré s vers la branche principale.	AWS DevOps

Tâche	Description	Compétences requises
Vérifiez les ressources CodeBuild du projet.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la CodeBuild console. 2. Sur la page Créer des projets, vérifiez que le nom du CodeBuild projet que vous avez créé apparaît dans la liste des projets. Le nom du projet est ajouté avec ce qui suit : pipeline-java-pjt -Build 3. Sélectionnez le nom de votre CodeBuild projet pour l'ouvrir. Passez ensuite en revue et validez les configurations suivantes : • Configuration du projet • Source • Environnement • Spécifications de construction • Configuration par lots • Artefacts	AWS DevOps

Tâche	Description	Compétences requises
Validez les CodePipeline étapes.	1. Connectez-vous à l'AWS Management Console, puis ouvrez la CodePipeline console. 2. Sur la page Pipelines, vérifiez que le nom du pipeline que vous avez créé apparaît dans la liste des pipelines. Le nom du pipeline est ajouté avec ce qui suit : pipeline-java-pjt - Pipeline 3. Sélectionnez le nom de votre pipeline pour l'ouvrir. Passez ensuite en revue et validez chaque étape du pipeline, y compris la validation et le déploiement.	AWS DevOps
Vérifiez que le pipeline CI s'est correctement exécuté.	1. Dans la CodePipeline console, sur la page Pipelines, sélectionnez le nom de votre pipeline pour afficher son statut. 2. Vérifiez que chaque étape du pipeline possède le statut Succeeded.	AWS DevOps

Nettoyage de vos ressources

Tâche	Description	Compétences requises
Supprimez les ressources empilées CloudFormation.	Supprimez la pile de ressources du pipeline CI CloudFormation. Pour plus d'informations, consultez la section Suppression d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation. **Note** Assurez-vous de supprimer la pile nommée - stack<project_name>.	AWS DevOps
Supprimez les dépendances du pipeline CI dans Amazon S3 et CloudFormation.	1. Videz le compartiment Amazon S3 nommé DeploymentArtifactBucket. Pour plus d'informations, consultez la section Vidage d'un compartiment dans la documentation Amazon S3. 2. Supprimez la pile de dépendances du pipeline CI CloudFormation. Pour plus d'informations, consultez la section Suppression d'une pile sur la CloudFormation console AWS dans la	AWS DevOps

Tâche	Description	Compétences requises
	CloudFormation documentation. **Note** Assurez-vous de supprimer la pile nommée pipeline-creation-dependencies-stack.	
Supprimez le bucket de modèles Amazon S3.	Supprimez le compartiment Amazon s3 que vous avez créé dans la section Configurer les prérequis de ce modèle, qui stocke les modèles de cette solution. Pour plus d'informations, consultez Supprimer un compartiment dans la documentation Amazon S3.	AWS DevOps

Ressources connexes

- Création d'une machine d'état Step Functions utilisant Lambda (documentation AWS Step Functions)
- AWS Step Functions WorkFlow Studio (documentation AWS Step Functions)
- DevOps et AWS
- Comment CloudFormation fonctionne AWS ? (CloudFormation documentation AWS)
- CI/CD complet avec AWS, CodeCommit AWS CodeDeploy, CodeBuild AWS et AWS (article de blog CodePipeline AWS)

- Quotas IAM et AWS STS, exigences relatives aux noms et limites de caractères (documentation IAM)

Déployez des CloudWatch canaris Synthetics à l'aide de Terraform

Créée par Dhrubajyoti Mukherjee (AWS) et Jean-Francois Landreau (AWS)

Récapitulatif

Il est important de valider l'état d'un système du point de vue du client et de confirmer que les clients sont en mesure de se connecter. Cela est plus difficile lorsque les clients n'appellent pas constamment le terminal. Amazon CloudWatch Synthetics prend en charge la création de canaris, qui peuvent tester des points de terminaison publics et privés. En utilisant des canaris, vous pouvez connaître l'état d'un système même s'il n'est pas utilisé. Ces canaris sont soit des scripts Node.js Puppeteer, soit des scripts Python Selenium.

Ce modèle décrit comment utiliser HashiCorp Terraform pour déployer des canaris qui testent des points de terminaison privés. Il intègre un script Puppeteer qui teste si une URL est renvoyée. `200-OK` Le script Terraform peut ensuite être intégré au script qui déploie le point de terminaison privé. Vous pouvez également modifier la solution pour surveiller les points de terminaison publics.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif avec un cloud privé virtuel (VPC) et des sous-réseaux privés
- URL du point de terminaison accessible depuis les sous-réseaux privés
- Terraform installé dans l'environnement de déploiement

Limites

La solution actuelle fonctionne pour les versions d'exécution de CloudWatch Synthetics suivantes :

- syn-nodejs-puppeteer-3,4
- syn-nodejs-puppeteer-3,5
- syn-nodejs-puppeteer-3,6
- syn-nodejs-puppeteer-3,7

À mesure que de nouvelles versions d'exécution sont publiées, vous devrez peut-être mettre à jour la solution actuelle. Vous devrez également modifier la solution pour suivre les mises à jour de sécurité.

Versions du produit

- Terraform 1.3.0

Architecture

Amazon CloudWatch Synthetics est basé sur CloudWatch Lambda et Amazon Simple Storage Service (Amazon S3). Amazon CloudWatch propose un assistant pour créer les canaris et un tableau de bord qui affiche l'état des canaris. La fonction Lambda exécute le script. Amazon S3 stocke les journaux et les captures d'écran des Canary Runs.

Ce modèle simule un point de terminaison privé via une instance Amazon Elastic Compute Cloud (Amazon EC2) déployée dans les sous-réseaux ciblés. La fonction Lambda nécessite des interfaces réseau élastiques dans le VPC où le point de terminaison privé est déployé.

Le diagramme décrit les éléments suivants :

1. Le Synthetics Canary lance la fonction Lambda Canary.
2. La fonction Lambda Canary se connecte à l'interface Elastic Network.
3. La fonction Canary Lambda surveille l'état du terminal.
4. Le Synthetics Canary envoie les données d'exécution vers le compartiment S3 et les métriques. CloudWatch
5. Une CloudWatch alarme est déclenchée sur la base des métriques.
6. L' CloudWatch alarme lance la rubrique Amazon Simple Notification Service (Amazon SNS).

Outils

Services AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS. Ce modèle utilise des points de terminaison VPC et des interfaces réseau élastiques.

Autres services

- HashiCorp Terraform est un outil open source d'infrastructure sous forme de code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources cloud. Ce modèle utilise Terraform pour déployer l'infrastructure.
- Puppeteer est une bibliothèque Node.js. Le runtime CloudWatch Synthetics utilise le framework Puppeteer.

Code

La solution est disponible dans le watch-synthetics-canary-terraform référentiel GitHub cloud. Pour plus d'informations, consultez la section Informations supplémentaires.

Épopées

Implémenter la solution de surveillance d'une URL privée

Tâche	Description	Compétences requises
Rassemblez les exigences relatives à la surveillance de l'URL privée.	Rassemblez la définition complète de l'URL : domaine, paramètres et en-têtes. Pour communiquer en privé avec Amazon S3 et Amazon CloudWatch, utilisez des points de terminaison VPC. Notez comment le VPC et les	Architecte cloud, administr ateur réseau

Tâche	Description	Compétences requises
	sous-réseaux sont accessibl es au point de terminaison. Tenez compte de la fréquence des courses de canaris.	

Tâche	Description	Compétences requises
Modifiez la solution existante pour surveiller l'URL privée.	Modifiez le `terraform .tfvars` fichier : • `name`— Le nom de votre canari. • `runtime_version` — La version d'exécution du Canary. Nous vous recommandons d'utiliser syn-nodejs-puppeteer -3.7. • `take_screenshot` — Si une capture d'écran doit être prise. • `api_hostname` — Le nom d'hôte du point de terminaison surveillé. • `api_path`— Le chemin du point de terminaison surveillé. • `vpc_id`— L'ID VPC utilisé par la fonction Lambda Canary. • `subnet_ids` — Le sous-réseau IDs utilisé par la fonction Lambda Canary. • `frequency` — La fréquence de course du canari en minutes. • `alert_sns_topic` — Rubrique SNS à laquelle la notification CloudWatch d'alarme est envoyée.	Architecte du cloud

Tâche	Description	Compétences requises

Déployez et exploitez la solution.	Pour déployer la solution, procédez comme suit :
	1. Depuis le `cloudwatch-synthetics-canary-terraform` répertoire de votre environnement de développement, initialisez Terraform.
	`terraform init`
	2. Planifiez et passez en revue les modifications.
	`terraform plan`
	3. Déployez la solution.
	`terraform apply`
		Architecte cloud, DevOps ingénieur

Résolution des problèmes

Problème	Solution
La suppression des ressources provisionnées est bloquée.	Supprimez manuellement la fonction Lambda Canary, l'interface Elastic Network correspon dante et le groupe de sécurité, dans cet ordre.

Ressources connexes

- Utilisation de la surveillance synthétique
- Surveillez les points de terminaison API Gateway avec Amazon CloudWatch Synthetics (article de blog)

Informations supplémentaires

Artefacts du référentiel

Les artefacts du référentiel se présentent dans la structure suivante.

```
.
### README.md
### main.tf
### modules
#   ### canary
#   ### canary-infra
### terraform.tfvars
### tf.plan
### variable.tf
```

Le `main.tf` fichier contient le module principal et déploie deux sous-modules :

- `canary-infra`déploie l'infrastructure requise pour les canaris.
- `canary`déploie les canaris.

Les paramètres d'entrée de la solution se trouvent dans le `terraform.tfvars` fichier. Vous pouvez utiliser l'exemple de code suivant pour créer un canari.

```
module "canary" {
    source = "./modules/canary"
    name   = var.name
    runtime_version = var.runtime_version
    take_screenshot = var.take_screenshot
    api_hostname = var.api_hostname
    api_path = var.api_path
    reports-bucket = module.canary_infra.reports-bucket
    role = module.canary_infra.role
    security_group_id = module.canary_infra.security_group_id
    subnet_ids = var.subnet_ids
    frequency = var.frequency
    alert_sns_topic = var.alert_sns_topic
}
```

Le fichier .var correspondant suit.

```
name   = "my-canary"
runtime_version = "syn-nodejs-puppeteer-3.7"
take_screenshot = false
api_hostname = "mydomain.internal"
api_path = "/path?param=value"
vpc_id = "vpc_id"
subnet_ids = ["subnet_id1"]
frequency = 5
alert_sns_topic = "arn:aws:sns:eu-central-1:111111111111:yyyyy"
```

Nettoyage de la solution

Si vous testez cela dans un environnement de développement, vous pouvez nettoyer la solution pour éviter des coûts supplémentaires.

1. Sur la console de gestion AWS, accédez à la console Amazon S3. Videz le compartiment Amazon S3 créé par la solution. Assurez-vous de faire une sauvegarde des données, si nécessaire.
2. Dans votre environnement de développement, depuis le `cloudwatch-synthetics-canary-terraform` répertoire, exécutez la `destroy` commande.

   ```
   terraform destroy
   ```

Déployer un pipeline CI/CD pour les microservices Java sur Amazon ECS

Créée par Vijay Thompson (AWS) et Sankar Sangubotla (AWS)

Récapitulatif

Ce modèle vous guide à travers les étapes du déploiement d'une intégration continue et d'une livraison continue (le CI/CD) pipeline for Java microservices on an existing Amazon Elastic Container Service (Amazon ECS) cluster by using AWS CodeBuild. When the developer commits the changes, the CI/CD pipeline est lancé et le processus de création démarre) CodeBuild. Lorsque le build est terminé, l'artefact est transféré vers Amazon Elastic Container Registry (Amazon ECR) et le dernier build d'Amazon ECR est récupéré et transmis au service Amazon ECS.

Conditions préalables et limitations

Prérequis

- Une application de microservices Java existante exécutée sur Amazon ECS
- Connaissance d'AWS CodeBuild et d'AWS CodePipeline

Architecture

Pile technologique source

- Microservices Java exécutés sur Amazon ECS
- Référentiel de code dans Amazon ECR
- AWS Fargate

Architecture source

Pile technologique cible

- Amazon ECR
- Amazon ECS
- AWS Fargate
- AWS CodePipeline

- AWS CodeBuild

Architecture cible

Automatisation et évolutivité

Fichier CodeBuild `buildspec.yml` :

```
version: 0.2

phases:
  pre_build:
    commands:
      - echo Logging in to Amazon ECR...
      - aws --version
      - $(aws ecr get-login --region $AWS_DEFAULT_REGION --no-include-email)
      - REPOSITORY_URI=$AWS_ACCOUNT_ID.dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/
$IMAGE_REPO
      - COMMIT_HASH=$(echo $CODEBUILD_RESOLVED_SOURCE_VERSION | cut -c 1-7)
      - IMAGE_TAG=build-$(echo $CODEBUILD_BUILD_ID | awk -F":" '{print $2}')
  build:
    commands:
      - echo Build started on `date`
      - echo building the Jar file
      - mvn clean install
      - echo Building the Docker image...
      - docker build -t $REPOSITORY_URI:$BUILD_TAG .
      - docker tag $REPOSITORY_URI:$BUILD_TAG $REPOSITORY_URI:$IMAGE_TAG
  post_build:
    commands:
      - echo Build completed on `date`
      - echo Pushing the Docker images...
      - docker push $REPOSITORY_URI:$BUILD_TAG
      - docker push $REPOSITORY_URI:$IMAGE_TAG
      - echo Writing image definitions file...
      - printf '[{"name":"%s","imageUri":"%s"}]' $DOCKER_CONTAINER_NAME
 $REPOSITORY_URI:$IMAGE_TAG > imagedefinitions.json
      - cat imagedefinitions.json
artifacts:
    files:
     - imagedefinitions.json
```

```
    - target/DockerDemo.jar
```

Outils

Services AWS

- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés. AWS CodeBuild évolue en permanence et traite plusieurs versions simultanément, afin que vos versions ne soient pas laissées dans la file d'attente.
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles. Vous pouvez intégrer AWS CodePipeline à des services tiers tels que GitHub, ou utiliser un service AWS tel qu'Amazon ECR.
- Amazon Elastic Container Registry (Amazon ECR) est un registre entièrement géré qui permet aux développeurs de stocker, de gérer et de déployer facilement des images de conteneurs Docker. Amazon ECR est intégré à Amazon ECS pour simplifier votre development-to-production flux de travail. Amazon ECR héberge vos images dans une architecture hautement disponible et évolutive afin que vous puissiez déployer des conteneurs pour vos applications de manière fiable. L'intégration à AWS Identity and Access Management (IAM) permet de contrôler chaque référentiel au niveau des ressources.
- Amazon Elastic Container Service (Amazon ECS) est un service d'orchestration de conteneurs hautement évolutif et performant qui prend en charge les conteneurs Docker et vous permet d'exécuter et de dimensionner facilement des applications conteneurisées sur AWS. Amazon ECS vous évite d'avoir à installer et à exploiter votre propre logiciel d'orchestration de conteneurs, à gérer et à dimensionner un cluster de machines virtuelles ou à planifier des conteneurs sur ces machines virtuelles.
- AWS Fargate est un moteur de calcul pour Amazon ECS qui vous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou de clusters. Avec AWS Fargate, vous n'avez plus besoin de provisionner, de configurer et de dimensionner des clusters de machines virtuelles pour exécuter des conteneurs. Vous n'avez plus à choisir de types de serveurs, décider quand mettre à l'échelle vos clusters ni optimiser les packs de clusters.

Autres outils

- Docker est une plate-forme qui vous permet de créer, de tester et de fournir des applications dans des packages appelés conteneurs.
- Git est un système de contrôle de version distribué permettant de suivre les modifications du code source pendant le développement de logiciels. Il est conçu pour coordonner le travail entre les programmeurs, mais il peut être utilisé pour suivre les modifications apportées à n'importe quel ensemble de fichiers. Ses objectifs incluent la rapidité, l'intégrité des données et la prise en charge de flux de travail distribués et non linéaires.

Épopées

Configuration du projet de génération dans AWS CodeBuild

Tâche	Description	Compétences requises
Créez un projet CodeBuild de construction.	Dans la CodeBuild console AWS, créez un projet de génération et spécifiez son nom.	Développeur d'applications, administrateur système AWS
Sélectionnez la source.	Ce modèle utilise Git pour le dépôt de code. GitHub Choisissez donc dans la liste des options disponibles. Choisissez un dépôt public ou depuis votre GitHub compte.	Développeur d'applications, administrateur système AWS
Sélectionnez un référentiel.	Sélectionnez le référentiel à partir duquel vous souhaitez générer le code.	Développeur d'applications, administrateur système AWS
Sélectionnez l'environnement.	Vous pouvez sélectionner une image dans une liste d'images gérées ou opter pour une image personnalisée à l'aide de Docker. Ce modèle utilise l'image gérée suivante :	Développeur d'applications, administrateur système AWS

Tâche	Description	Compétences requises
	• **Note** Amazon Linux 2 (: Amazon Linux 2 touche à sa fin de support. Pour plus d'informations, consultez Amazon Linux 2 FAQs.) • Durée d'exécution : Standard • Version de l'image 1.0	
Choisissez un rôle de service.	Vous pouvez créer un rôle de service ou le sélectionner dans une liste de rôles existants.	Développeur d'applications, administrateur système AWS

Tâche	Description	Compétences requises
Ajoutez des variables d'environnement.	Dans la section Configuration supplémentaire, configurez les variables d'environnement suivantes : • AWS_DEFAULT_REGION pour la région AWS par défaut • AWS_ACCOUNT_ID pour le numéro de compte utilisateur • IMAGE_REPO pour le référentiel privé Amazon ECR • BUILD_TAG pour la version du build (le dernier build est la valeur de cette variable) • DOCKER_CONTAINER_NAME pour le nom du conteneur dans la tâche Ces variables sont des espaces réservés dans le `buildspec.yml` fichier et seront remplacées par leurs valeurs respectives.	Développeur d'applications, administrateur système AWS

Tâche	Description	Compétences requises
Créez un fichier buildspec.	Vous pouvez créer un `buildspec.yml` fichier au même emplacement `pom.xml` et ajouter la configuration fournie dans ce modèle, ou utiliser l'éditeur buildspec en ligne et ajouter la configura tion. Configurez les variables environnementales avec les valeurs appropriées en suivant les étapes indiquées.	Développeur d'applications, administrateur système AWS
Configurez le projet pour les artefacts.	(Facultatif) Configurez le projet de construction pour les artefacts, si nécessaire.	Développeur d'applications, administrateur système AWS
Configurez Amazon CloudWatch Logs.	(Facultatif) Configurez Amazon CloudWatch Logs pour le projet de génération, si nécessaire. Cette étape est facultative mais recommand ée.	Développeur d'applications, administrateur système AWS
Configurez les journaux Amazon S3.	(Facultatif) Configurez les journaux Amazon Simple Storage Service (Amazon S3) pour le projet de génération, si vous souhaitez stocker les journaux.	Développeur d'applications, administrateur système AWS

Configuration du pipeline dans AWS CodePipeline

Tâche	Description	Compétences requises
Créez un pipeline.	Sur la CodePipeline console AWS, créez un pipeline et spécifiez son nom. Pour plus d'informations sur la création d'un pipeline, consultez la CodePipeline documentation AWS.	Développeur d'applications, administrateur système AWS
Sélectionnez un rôle de service.	Créez un rôle de service ou sélectionnez-le dans la liste des rôles de service existants . Si vous créez un rôle de service, attribuez un nom au rôle et sélectionnez l'option permettant CodePipeline de créer le rôle.	Développeur d'applications, administrateur système AWS
Choisissez un magasin d'artefacts.	Dans les paramètres avancés, si vous souhaitez qu'Amazon S3 crée un compartiment et y stocke les artefacts, utilisez l'emplacement par défaut du magasin d'artefac ts. Vous pouvez également sélectionner un emplaceme nt personnalisé et spécifier un compartiment existant. Vous pouvez également choisir de chiffrer l'artefact à l'aide d'une clé de chiffrement.	Développeur d'applications, administrateur système AWS

Tâche	Description	Compétences requises
Spécifiez le fournisseur source.	Dans le champ Source provider, choisissez GitHub (Version 2).	Développeur d'applications, administrateur système AWS
Sélectionnez le référentiel et la branche du code.	Si vous n'êtes pas connecté, fournissez les informations de connexion auxquelles vous souhaitez vous connecter GitHub, puis sélectionnez le nom du référentiel et le nom de la branche.	Développeur d'applications, administrateur système AWS
Modifiez les options de détection.	Choisissez Démarrer le pipeline lors de la modification du code source et passez à la page suivante.	Développeur d'applications, administrateur système AWS
Sélectionnez un fournisseur de build.	Dans le champ Build provider CodeBuild, choisissez AWS, puis fournissez la région AWS et les détails du nom du projet de build. Pour Type de construction, choisissez Construction unique.	Développeur d'applications, administrateur système AWS
Choisissez un fournisseur de déploiement.	Pour le fournisseur de déploiement, choisissez Amazon ECS. Choisissez le nom du cluster, le nom du service, le fichier de définitio ns d'image, le cas échéant, et une valeur de délai de déploiement, si nécessaire. Choisissez Créer un pipeline.	Développeur d'applications, administrateur système AWS

Ressources connexes

- Documentation AWS ECS
- Documentation AWS ECR
- CodeBuild Documentation AWS
- CodePipeline Documentation AWS
- Créez un pipeline de livraison continue pour vos images de conteneurs avec Amazon ECR comme source (article de blog)

Déployez une ChatOps solution pour gérer les résultats du scan SAST en utilisant Amazon Q Developer dans les applications de chat, les actions personnalisées et AWS CloudFormation

Créée par Anand Bukkapatnam Tirumala (AWS)

Récapitulatif

Ce modèle présente une solution complète qui utilise Amazon Q Developer dans les applications de chat afin de rationaliser la gestion des défaillances d'analyse des tests de sécurité des applications statiques (SAST) signalées par le biais SonarQube de ce modèle. Cette approche innovante intègre des actions et des notifications personnalisées dans une interface conversationnelle, permettant une collaboration efficace et des processus décisionnels au sein des équipes de développement.

Dans l'environnement de développement logiciel en évolution rapide d'aujourd'hui, la gestion efficace des résultats du scan SAST est essentielle pour maintenir la qualité et la sécurité du code. Cependant, de nombreuses organisations sont confrontées aux défis importants suivants :

- Prise de conscience différée des vulnérabilités critiques en raison de l'inefficacité des systèmes de notification
- Processus de prise de décision lents causés par des flux de travail d'approbation déconnectés
- Absence de réponses immédiates et exploitables en cas d'échec du scan SAST
- Communication et collaboration fragmentées autour des résultats de sécurité
- Configuration manuelle de l'infrastructure fastidieuse et sujette aux erreurs pour les outils de sécurité

Ces problèmes augmentent souvent les risques de sécurité, retardent les publications et réduisent la productivité des équipes. Pour relever efficacement ces défis, il faut une solution capable de rationaliser la gestion des résultats du SAST, d'améliorer la collaboration des équipes et d'automatiser le provisionnement de l'infrastructure.

Les principales fonctionnalités de la solution sont les suivantes :

- Notifications personnalisées — Les alertes et notifications en temps réel sont transmises directement aux canaux de discussion de l'équipe, ce qui permet de détecter et d'agir rapidement en cas de vulnérabilité ou d'échec du scan SAST.

- Approbations conversationnelles — Les parties prenantes peuvent initier et terminer des flux de travail d'approbation pour les résultats du scan SAST de manière fluide via l'interface de chat, accélérant ainsi les processus de prise de décision.
- Actions personnalisées — Les équipes peuvent définir et exécuter des actions personnalisées en fonction des résultats du scan SAST, telles que le déclenchement automatique d'e-mails en cas de défaillance du contrôle qualité ou l'amélioration de la réactivité face aux problèmes de sécurité.
- Collaboration centralisée — Toutes les discussions, décisions et actions liées au scan SAST sont conservées dans un environnement de discussion unifié, ce qui favorise une meilleure collaboration et un partage des connaissances entre les membres de l'équipe.
- Infrastructure sous forme de code (IaC) : l'ensemble de la solution est enveloppé de AWS CloudFormation modèles, ce qui permet un provisionnement plus rapide et plus fiable de l'infrastructure tout en réduisant les erreurs de configuration manuelle.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Rôle AWS Identity and Access Management (IAM) autorisé à créer et à gérer les ressources associées aux ressources Services AWS répertoriées dans Outils.
- Un espace de travail Slack.
- Amazon Q Developer dans les applications de chat a été ajouté à l'espace de travail Slack requis en tant que plug-in. Pour plus d'informations, consultez la section Ajouter des applications à votre espace de travail Slack dans la documentation Slack. Notez l'identifiant de l'espace de travail Slack tel qu'indiqué sur le une AWS Management Console fois l'enregistrement réussi.
- Un client Amazon Q Developer configuré dans des applications de chat, avec l'ID de l'espace de travail facilement disponible pour la saisie dans la AWS CloudFormation console. Pour obtenir des instructions, consultez la section Configurer un client Slack dans le Guide de l'administrateur des applications de chat Amazon Q pour les développeurs.
- Un compte e-mail source créé et vérifié dans Amazon Simple Email Service (Amazon SES) pour envoyer des e-mails d'approbation. Pour les instructions de configuration, consultez la section Création et vérification des identités e-mail dans le manuel Amazon Simple Email Service Developer Guide.
- Adresse e-mail de destination pour recevoir les notifications d'approbation. Cette adresse peut être une boîte de réception partagée ou une liste de distribution spécifique à une équipe.

- Une SonarQube instance opérationnelle accessible depuis votre Compte AWS. Pour plus d'informations, consultez les instructions SonarQube d'installation.
- Un jeton SonarQube utilisateur autorisé à déclencher et à créer des projets via le pipeline.

Limites

- La création de boutons d'action personnalisés est un processus manuel dans cette solution.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Le schéma montre le flux de travail automatisé d'assurance qualité du code :

1. Préparation et téléchargement du code :
   - Le développeur compresse la base de code dans un fichier .zip.
   - Le développeur télécharge manuellement le fichier .zip dans un compartiment Amazon Simple Storage Service (Amazon S3) désigné.
2. Déclenchement et AWS Step Functions orchestration d'événements Amazon S3 :
   - L'événement de téléchargement Amazon S3 déclenche un flux de travail Step Functions.
   - Step Functions orchestre un scan SAST à l'aide de. SonarQube
   - Le flux de travail surveille l'état de la AWS CodeBuild tâche pour déterminer les prochaines actions. En cas de CodeBuild succès (contrôle qualité), le flux de travail s'arrête. En cas d' CodeBuild échec, une AWS Lambda fonction est invoquée à des fins de diagnostic. Pour plus de détails, consultez AWS Step Functions la section logique plus loin dans cette section.
3. AWS CodeBuild exécution :
   - La CodeBuild tâche exécute une SonarQube analyse de la base de code téléchargée.
   - Les artefacts de scan sont stockés dans un compartiment Amazon S3 distinct à des fins d'audit et d'analyse.
4. Analyse des défaillances (fonction Lambda) :

- En CodeBuild cas d'échec, la fonction `CheckBuildStatus` Lambda est déclenchée.
- En cas de CodeBuild succès, le processus est arrêté et aucune autre action n'est nécessaire.

5. La fonction Lambda analyse la cause de la défaillance (défaillance du contrôle qualité ou autres problèmes)
   - La `CheckBuildStatus` fonction crée une charge utile personnalisée avec des informations détaillées sur les défaillances.
   - La `CheckBuildStatus` fonction publie la charge utile personnalisée dans une rubrique Amazon Simple Notification Service (Amazon SNS).
6. Système de notification :
   - Amazon SNS transmet la charge utile à Amazon Q Developer dans des applications de chat pour l'intégration à Slack.
7. Intégration à Slack :
   - Dans les applications de chat, Amazon Q Developer publie une notification sur le canal Slack désigné.
8. Processus d'approbation :
   - Les approbateurs examinent les détails de l'échec dans la notification Slack.
   - Les approbateurs peuvent initier l'approbation à l'aide du bouton Approuver dans Slack.
9. Gestionnaire d'approbation :
   - Une fonction Lambda d'approbation traite l'action d'approbation depuis Slack.
   - La fonction d'approbation publie le message personnalisé sur Amazon SES.
10. Message généré :
    - La fonction d'approbation génère un message personnalisé pour les notifications destinées aux développeurs.
11. Notification aux développeurs :
    - Amazon SES envoie un e-mail au développeur avec les prochaines étapes ou les actions requises.

Ce flux de travail associe le téléchargement manuel du code à des contrôles de qualité automatisés, fournit un feedback immédiat via Slack et permet une intervention humaine si nécessaire, garantissant ainsi un processus de révision du code robuste et flexible.

AWS Step Functions logique

Comme indiqué dans le schéma d'architecture précédent, si le transfert du contrôle qualité SonarQube échoue, le flux de travail passe à la fonction `CheckBuildStatus` Lambda. La `CheckBuildStatus` fonction déclenche une notification sur le canal Slack. Chaque notification inclut des informations avec les prochaines étapes suggérées. Les types de notifications sont les suivants :

- L'application a échoué lors de l'analyse de sécurité du code : l'utilisateur reçoit cette notification lorsque le code téléchargé n'a pas réussi le scan SonarQube de sécurité. L'utilisateur peut choisir APPROVE pour accepter le build. Cependant, la notification conseille à l'utilisateur de se méfier de la mauvaise qualité du code et des risques de sécurité potentiels. La notification inclut les informations suivantes :
  - Prochaines étapes : Erreur : État du contrôle de qualité : ÉCHEC — Afficher les détails à l'URL fournie.
  - Triez les vulnérabilités comme indiqué dans le document à l'adresse URL fournie.
  - CodeBuild les détails sont disponibles sur place à l'adresse URL fournie.
- Le pipeline d'analyse des applications a échoué pour une autre raison : l'utilisateur reçoit cette notification lorsque le pipeline échoue pour une raison autre que l'échec de l'analyse de sécurité du code. La notification inclut les informations suivantes :
  - Pour les étapes suivantes, cliquez sur le lien fourni pour un dépannage plus approfondi.

Pour voir des captures d'écran des notifications telles qu'elles apparaissent sur une chaîne Slack, rendez-vous dans le dossier des ressources du référentiel GitHub chatops-slack.

Le schéma suivant montre un exemple du statut de l'étape Step Functions après l'échec du contrôle qualité.

Outils

Services AWS

- Amazon Q Developer dans les applications de chat vous permet d'utiliser les canaux de discussion Amazon Chime, Microsoft Teams et Slack pour surveiller les événements opérationnels de vos applications et y répondre. AWS Avis de fin de support : le 20 février 2026, le support du service Amazon Chime AWS prendra fin. Après le 20 février 2026, vous ne pourrez plus accéder à la console Amazon Chime ni aux ressources de l'application Amazon Chime. Pour plus

d'informations, consultez le billet de blog. Cela n'a aucune incidence sur la disponibilité du service Amazon Chime SDK.

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Simple Email Service (Amazon SES) vous permet d'envoyer et de recevoir des e-mails en utilisant vos propres adresses e-mail et domaines.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.

Autres outils

- Slack, une offre de Salesforce, est une plateforme conversationnelle basée sur l'IA qui permet la collaboration par chat et vidéo, automatise les processus sans code et prend en charge le partage d'informations.
- SonarQubeest un outil d'analyse sur site conçu pour détecter les problèmes de codage dans plus de 30 langages, frameworks et plateformes IaC.

Référentiel de code

Le code de ce modèle est disponible dans le dépôt GitHub chatops-slack.

Bonnes pratiques

- CloudFormation gestion des piles : si vous rencontrez des défaillances lors de l'exécution de la CloudFormation pile, nous vous recommandons de supprimer la pile défaillante. Recréez-le ensuite avec les valeurs de paramètres correctes. Cette approche permet un déploiement propre et permet d'éviter les conflits potentiels ou les implémentations partielles.
- Configuration des e-mails dans une boîte de réception partagée : lorsque vous configurez le `SharedInboxEmail` paramètre, utilisez une liste de distribution commune accessible à tous les développeurs concernés. Cette approche favorise la transparence et permet aux notifications importantes de parvenir aux membres de l'équipe concernés.
- Flux de travail d'approbation de production : pour les environnements de production, limitez l'accès au canal Slack utilisé pour les approbations de construction. Seuls les approbateurs désignés doivent être membres de cette chaîne. Cette pratique permet de maintenir une chaîne de responsabilité claire et d'améliorer la sécurité en limitant le nombre de personnes habilitées à approuver les modifications critiques.
- Autorisations IAM — Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Effectuer la configuration initiale

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Pour cloner le dépôt chatops-slack pour ce modèle, utilisez la commande suivante. `git clone “git@github.com:aws-samples/chatops-slack.git“`	AWS DevOps, responsable du développement, DevOps ingénieur, administrateur du cloud

Tâche	Description	Compétences requises

Créez les fichiers .zip contenant le code Lambda.	Créez les fichiers .zip pour le code de AWS Lambda fonction de la `ApprovalEmail` fonctionnalité `CheckBuildStatus` et. Pour créer `notification.zip` et`approval.zip` , utilisez les commandes suivantes.
	`cd chatops-slack/src`
	`chmod -R 775 *`
	`zip -r approval.zip approval`
	`zip -r notification.zip notification`
		AWS DevOps, responsable du développement, DevOps ingénieur, administrateur du cloud

Déployez le fichier de pile pre-requisite.yml

Tâche	Description	Compétences requises
Exécutez le fichier de `pre-requisite.yml` pile.	Le fichier de `pre-requisite.yml` CloudFormation pile déploie les ressources initiales requises avant que vous n'exécutiez le fichier de `app-security.yml` pile. Pour exécuter le `pre-requisite.yml` fichier, procédez comme suit :	Administrateur AWS, AWS DevOps, responsable du développement, DevOps ingénieur

Tâche	Description	Compétences requises
	1. Connectez-vous à la AWS Management ConsoleAWS CloudFormationconsole et ouvrez-la. Choisissez Créer une pile, puis choisisse z Avec de nouvelles ressources (standard) dans la liste déroulante. 2. Sur la page Créer une pile, choisissez Choisir un modèle existant et Charger un fichier modèle. Choisissez ensuite Choisir un fichier et sélectionnez pre-requisite.yml. Choisisse z Suivant. 3. Sur la page Spécifier les détails de la pile, entrez les valeurs des paramètre s comme décrit dans Informations supplémen taires. Ensuite, choisissez Suivant. 4. Sur la page Configurer les options de pile, choisissez le rôle IAM pour créer les ressources, comme décrit dans Conditions préalables. Ensuite, choisissez Suivant. 5. Sur la page Réviser et créer, choisissez Soumettre . 6. Sur la page de détails de la pile, choisissez les onglets	

Tâche	Description	Compétences requises
	Ressources et Sorties. Notez les valeurs des `CKMSKeyId` paramètres `S3LambdaCKMSKeyArn`, et qui sont utilisées dans les étapes suivantes.	
Téléchargez les fichiers .zip dans le compartiment Amazon S3.	Chargez les `approval.zip` fichiers `notification.zip` et que vous avez créés précédemment dans le compartiment Amazon S3 nommé`S3LambdaBucket`. Le fichier de `app-security.yml` CloudFormation pile est utilisé `S3LambdaBucket` pour provisionner la fonction Lambda.	AWS DevOps, responsable du développement, DevOps ingénieur, administrateur système AWS

Exécutez le fichier de pile app-security.yml

Tâche	Description	Compétences requises
Exécutez le fichier de `app-security.yml` pile.	Les fichiers de `app-security.yml` pile déploient l'infrastructure restante pour le système de notification et d'approbation. Pour exécuter le `app-security.yml` fichier, procédez comme suit : 1. Connectez-vous à la AWS Management ConsoleAWS CloudFormationconsole et ouvrez-la. Choisissez Créer	AWS DevOps, administrateur système AWS, DevOps ingénieur, responsable du développement

Tâche	Description	Compétences requises
	une pile, puis choisisse z Avec de nouvelles ressources (standard) dans la liste déroulante. 2. Sur la page Créer une pile, choisissez Choisir un modèle existant et Charger un fichier modèle. Choisisse z ensuite Choisir un fichier et sélectionnez app-secur ity.yml. Choisissez Suivant. 3. Sur la page Spécifier les détails de la pile, entrez les valeurs des paramètre s comme décrit dans Informations supplémen taires. Ensuite, choisissez Suivant. 4. Sur la page Configurer les options de pile, choisissez le rôle IAM pour créer les ressources, comme décrit dans Conditions préalables. Ensuite, choisissez Suivant. 5. Sur la page Réviser et créer, choisissez Soumettre .	

Tâche	Description	Compétences requises
Testez la configuration des notifications.	Pour tester la configuration des notifications, procédez comme suit : 1. Ouvrez la console Amazon SNS. Dans le panneau de navigation de gauche, choisissez Rubriques. 2. Sélectionnez le nom du sujet qui se termine par LambdaToAWSSlackChatbot. 3. Sur la page de détails du sujet, choisissez Publier le message. 4. Sur la page Publier le message dans le sujet, pour le corps du message à envoyer au point de terminaison, entrez ce qui suit : `{ "version": "1.0", "source": "custom", "content": { "description": ":warning: This is a test notification" } }` 5. Choisissez Publier le message.	AWS DevOps, administrateur système AWS, DevOps ingénieur, responsable du développement

Tâche	Description	Compétences requises
	Une fois le message de test envoyé avec succès, vous devriez voir une notification sur le canal Slack. Pour plus d'informations, consultez la section Tester les notifications envoyées Services AWS à Slack dans le guide de l'administrateur des applications de chat Amazon Q pour les développeurs.	

Configurer le flux d'approbation

Tâche	Description	Compétences requises
Configurez une action Lambda personnalisée.	Pour configurer l' AWS Lambda action personnalisée, procédez comme suit : 1. Cliquez sur le bouton représentant des points de suspension verticaux en bas de la notification de livraison dans votre chaîne Slack. 2. Dans Gérer les actions, choisissez Créer. 3. Entrez un nom d'action personnalisé, par exemple Approuver. Ce nom est un identifiant unique pour votre action personnalisée.	Administrateur AWS DevOps, responsable du développement, DevOps ingénieur, administrateur Slack

Tâche	Description	Compétences requises
	4. Entrez un nom pour votre bouton d'action personnalisé, par exemple, Approuver. Ce nom apparaît sur un bouton de votre notification. Ce nom doit comporter 20 caractères ou moins et peut intégrer des emojis. 5. Pour Type d'action personnalisé, sélectionnez Action Lambda. 6. Choisissez Suivant. 7. Sélectionnez l'action Compte AWS et l' Région AWS endroit où vous souhaitez déployer cette action. 8. Choisissez Load Lambdas. 9. Dans Définir une fonction Lambda, sélectionnez une fonction Lambda qui se termine par. ApprovalEmailLambdaEnsuite, choisissez Suivant. 10. Pour créer le bouton Approuver, choisissez Enregistrer sur la page des critères d'affichage.	

Tâche	Description	Compétences requises
Validez le flux d'approbation.	Pour vérifier que le flux d'approbation fonctionne comme prévu, cliquez sur le bouton Approuver dans Slack. Slackbot doit envoyer une notification sur le fil de discussion avec la chaîne de confirmation « L'e-mail d'approbation a été envoyé avec succès ».	Administrateur AWS, DevOps ingénieur AWS DevOps, administrateur Slack

Résolution des problèmes

Problème	Solution
Mauvaises configurations de Slack	Pour plus d'informations sur la résolution des problèmes liés aux mauvaises configurations de Slack, consultez la section Résolution des problèmes liés aux développeurs Amazon Q Developer dans le Guide de l'administrateur d'Amazon Q Developer in Chat applications.
Le scan a échoué pour une autre raison	Cette erreur signifie que la tâche de génération du code a échoué. Pour résoudre le problème, cliquez sur le lien figurant dans le message. L'échec de la tâche de génération du code peut avoir les causes suivantes : • L'application n'est pas correctement empaquetée. La `sonar-scanner` commande ne trouve pas le `sonar.project.env.properties` fichier.

Problème	Solution
	• Les valeurs des `SonarToken` paramètres `SonarFileName` `SonarFileDirectory` , ou sont incorrectes. Vérifiez les valeurs, puis exécutez à nouveau les fichiers de pile. • L'hôte Sonar n'est pas joignable. • Autres problèmes que vous pouvez résoudre à l'aide des journaux.

Ressources connexes

AWS documentation

- Configuration d'un client Slack
- Création d'une action personnalisée
- Création d'une procédure d'identification par adresse e-mail
- Tutoriel : Commencez à utiliser Slack

Autres ressources

- Ajouter des applications à votre espace de travail Slack (documentation Slack)
- Génération et utilisation de jetons (SonarQube documentation)
- Présentation de l'installation du serveur (SonarQube documentation)

Informations supplémentaires

Cette solution met l'accent sur les actions personnalisées d'Amazon Q Developer dans les applications de chat à des fins de gestion des versions. Cependant, vous pouvez réutiliser la solution en modifiant le code Lambda en fonction de votre cas d'utilisation spécifique et en le complétant.

Paramètres des fichiers de CloudFormation pile

Le tableau suivant présente les paramètres et leurs descriptions pour le fichier de CloudFormation pile`pre-requisite.yml`.

Clé	Description
`StackName`	Nom de la CloudFormation pile.
`S3LambdaBucket`	Le nom du compartiment Amazon S3 dans lequel vous chargez le code Lambda. Le nom doit être globalement unique.
`SonarToken`	Le jeton SonarQube utilisateur tel que décrit dans la section Conditions préalables.

Le tableau suivant présente les paramètres et leurs descriptions pour le fichier de CloudFormation pile`app-security.yml`.

Clé	Description
`CKMSKeyArn`	Le nom de ressource AWS KMS key Amazon (ARN) utilisé dans les rôles IAM et les fonctions Lambda créés dans cette pile.
`CKMSKeyId`	L' AWS KMS key ID utilisé dans la rubrique Amazon SNS créée dans cette pile.
`EnvironmentType`	Nom de l'environnement client pour le déploiement du pipeline d'analyse des applicati ons. Sélectionnez le nom de l'environnement dans la liste déroulante des valeurs autorisées.
`S3LambdaBucket`	Le nom du compartiment Amazon S3 qui contient les `notification.zip` fichiers `approval.zip` et.
`SESEmail`	Le nom de l'identité e-mail enregistrée dans Amazon SES, tel que décrit dans la section Conditions préalables. Cette identité est l'adresse e-mail source.

`SharedInboxMail`	Adresse e-mail de destination à laquelle les notifications de numérisation sont envoyées.
`SlackChannelId`	L'identifiant de la chaîne Slack sur laquelle vous souhaitez que les notifications soient envoyées. Pour trouver l'identifiant de la chaîne, cliquez avec le bouton droit sur le nom de la chaîne dans Détails de la chaîne dans l'application Slack. L'identifiant de la chaîne se trouve en bas.
`SlackWorkspaceId`	L'identifiant de l'espace de travail Slack tel que décrit dans la section Conditions préalables. Pour trouver l'identifiant de l'espace de travail Slack, connectez-vous à la AWS Managemen t Console console Amazon Q Developer dans les applications de chat, puis choisissez Clients configurés, Slack, WorkspaceID.
`StackName`	Nom de la CloudFormation pile.
`SonarFileDirectory`	Le répertoire qui contient le `sonar.pro ject.<env>.properties` fichier.
`SonarFileName`	Le nom du `sonar.project.<env >properties` fichier.
`SourceCodeZip`	Nom du fichier .zip qui contient le `sonar.pro ject.<env>properties` fichier et le code source.

Déployez un pare-feu à l'aide d'AWS Network Firewall et d'AWS Transit Gateway

Créée par Shrikant Patil (AWS)

Récapitulatif

Ce modèle vous montre comment déployer un pare-feu à l'aide d'AWS Network Firewall et d'AWS Transit Gateway. Les ressources Network Firewall sont déployées à l'aide d'un CloudFormation modèle AWS. Network Firewall s'adapte automatiquement à votre trafic réseau et peut prendre en charge des centaines de milliers de connexions, de sorte que vous n'avez pas à vous soucier de créer et de maintenir votre propre infrastructure de sécurité réseau. Une passerelle de transit est un hub de transit réseau que vous pouvez utiliser pour interconnecter vos clouds privés virtuels (VPCs) et vos réseaux sur site.

Dans ce modèle, vous apprenez également à inclure un VPC d'inspection dans votre architecture réseau. Enfin, ce modèle explique comment utiliser Amazon CloudWatch pour surveiller l'activité en temps réel de votre pare-feu.

> **Tip**
>
> Il est recommandé d'éviter d'utiliser un sous-réseau Network Firewall pour déployer d'autres services AWS. Cela est dû au fait que Network Firewall ne peut pas inspecter le trafic provenant de sources ou de destinations au sein du sous-réseau d'un pare-feu.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorisations relatives au rôle et à la politique d'AWS Identity and Access Management (IAM)
- CloudFormation autorisations du modèle

Limites

Il se peut que vous rencontriez des problèmes avec le filtrage des domaines et qu'un autre type de configuration soit nécessaire. Pour plus d'informations, consultez les groupes de règles de liste de domaines Stateful dans AWS Network Firewall dans la documentation Network Firewall.

Architecture

Pile technologique

- Amazon CloudWatch Logs
- Amazon VPC
- AWS Network Firewall
- AWS Transit Gateway

Architecture cible

Le schéma suivant montre comment utiliser Network Firewall et Transit Gateway pour inspecter votre trafic :

L'architecture inclut les composants suivants :

- Votre application est hébergée dans les deux rayons VPCs. Ils VPCs sont surveillés par Network Firewall.
- Le VPC de sortie a un accès direct à la passerelle Internet mais n'est pas protégé par Network Firewall.
- Le VPC d'inspection est l'endroit où Network Firewall est déployé.

Automatisation et mise à l'échelle

Vous pouvez l'utiliser CloudFormationpour créer ce modèle en utilisant l'infrastructure comme code.

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que

vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

- AWS Network Firewall est un pare-feu réseau dynamique et géré, ainsi qu'un service de détection et de prévention des intrusions VPCs destiné au cloud AWS.
- AWS Transit Gateway est un hub central qui connecte VPCs les réseaux sur site.

Code

Le code de ce modèle est disponible dans le référentiel de déploiement d' GitHub AWS Network Firewall avec Transit Gateway. Vous pouvez utiliser le CloudFormation modèle de ce référentiel pour déployer un VPC d'inspection unique qui utilise Network Firewall.

Épopées

Création du VPC à rayons et du VPC d'inspection

Tâche	Description	Compétences requises
Préparez et déployez le CloudFormation modèle.	1. Téléchargez le `cloudformation/aws_nw_fw.yml` modèle depuis le GitHub référentiel. 2. Mettez à jour le modèle avec vos valeurs. 3. Déployez le modèle.	AWS DevOps

Création de la passerelle et des itinéraires de transit

Tâche	Description	Compétences requises
Créez une passerelle de transit.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC.	AWS DevOps

Tâche	Description	Compétences requises
	2. Dans le volet de navigation, choisissez Transit gateways. 3. Choisissez Create transit gateway (Créer une passerelle de transit). 4. Dans le champ Name tag, entrez le nom de la passerelle de transit. 5. Dans Description, entrez une description pour la passerelle de transit. 6. Pour le numéro de système autonome (ASN) côté Amazon, laissez la valeur ASN par défaut. 7. Sélectionnez l'option de support DNS. 8. Sélectionnez l'option de support VPN ECMP. 9. Sélectionnez l'option d'association de table de routage par défaut. Cette option associe automatiquement les pièces jointes de la passerelle de transit à la table de routage par défaut de la passerelle de transit. 10. Sélectionnez l'option de propagation de la table de routage par défaut. Cette option propage automatiq	

Tâche	Description	Compétences requises
	uement les pièces jointes de la passerelle de transit vers la table de routage par défaut de la passerelle de transit. 11. Choisissez Create transit gateway (Créer une passerelle de transit).	
Créez des pièces jointes pour les passerelles de transit.	Créez une pièce jointe à une passerelle de transit pour les éléments suivants : • Une pièce jointe d'inspect ion dans le VPC d'inspect ion et le sous-réseau Transit Gateway • Une pièce jointe SpokeVPCA dans le VPCA en étoile et le sous-réseau privé • Une pièce jointe SpokeVPCB dans le VPCB en étoile et le sous-réseau privé • Une pièce jointe de sortie dans le VPC de sortie et le sous-réseau privé	AWS DevOps

Tâche	Description	Compétences requises
Créez une table de routage pour passerelle de transit.	1. Créez une table de routage de passerelle de transit pour le VPC Spoke. Cette table de routage doit être associée à tous les éléments VPCs autres que le VPC d'inspection. 2. Créez une table de routage de passerelle de transit pour le pare-feu. Cette table de routage doit être associée au VPC d'inspect ion uniquement. 3. Ajoutez un itinéraire à la table de routage de la passerelle de transit pour le pare-feu : • Pour`0.0.0/0`, utilisez la pièce jointe EgressVPC. • Pour le bloc d'adresse CIDR SpokeVPCA, utilisez la pièce jointe Spoke. VPC1 • Pour le bloc CIDR SpokeVPCB, utilisez la pièce jointe Spoke. VPC2 4. Ajoutez un itinéraire à la table de routage de la passerelle de transit pour le VPC Spoke. Pour`0.0.0/0`, utilisez l'accessoire VPC d'inspection.	AWS DevOps

Création du pare-feu et des itinéraires

Tâche	Description	Compétences requises
Créez un pare-feu dans le VPC d'inspection.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, sous Network Firewall, sélectionnez Firewalls. 3. Choisissez Créer un pare-feu. 4. Dans Nom, entrez le nom que vous souhaitez utiliser pour identifier ce pare-feu. Vous ne pouvez pas modifier le nom d'un pare-feu après l'avoir créé. 5. Pour le VPC, sélectionnez votre VPC d'inspection. 6. Pour Zone de disponibilité et sous-réseau, sélectionnez la zone et le sous-réseau de pare-feu que vous avez identifiés. 7. Dans la section Stratégie de pare-feu associée, choisissez Associer une politique de pare-feu existante, puis sélectionnez la stratégie de pare-feu que vous avez créée précédemment.	AWS DevOps

Tâche	Description	Compétences requises
	8. Choisissez Créer un pare-feu.	

Tâche	Description	Compétences requises
Créez une politique de pare-feu.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, sous Network Firewall, sélectionnez Firewall policies. 3. Sur la page Décrire la politique de pare-feu, choisissez Créer une politique de pare-feu. 4. Dans Nom, entrez le nom que vous souhaitez utiliser pour la politique de pare-feu. Vous utiliserez le nom pour identifier la politique lorsque vous l'associerez à votre pare-feu ultérieurement dans ce modèle. Vous ne pouvez pas modifier le nom d'une politique de pare-feu après l'avoir créée. 5. Choisissez Suivant. 6. Sur la page Ajouter des groupes de règles, dans la section Groupe de règles apatrides, choisissez Ajouter des groupes de règles apatrides. 7. Dans la boîte de dialogue Ajouter à partir de groupes	AWS DevOps

Tâche	Description	Compétences requises
	de règles existants, cochez la case correspondant au groupe de règles apatrides que vous avez créé précédemment. Choisissez Ajouter des groupes de règles. Remarque : Au bas de la page, le compteur de capacité de la politique de pare-feu indique la capacité consommée en ajoutant ce groupe de règles à côté de la capacité maximale autorisée pour une politique de pare-feu. 8. Définissez l'action par défaut apatride sur Transférer vers les règles avec état. 9. Dans la section Groupe de règles dynamiques, choisissez Ajouter des groupes de règles dynamiques, puis cochez la case correspondant au groupe de règles dynamiques que vous avez créé précédemment. Choisissez Ajouter des groupes de règles. 10. Choisissez Suivant pour parcourir le reste de l'assistant de configuration,	

Tâche	Description	Compétences requises
	puis choisissez Créer une politique de pare-feu.	

Tâche	Description	Compétences requises
Mettez à jour vos tables de routage VPC.	Tables de routage VPC d'inspection 1. Dans la table de routage du ANF sous-réseau (`Inspection-ANFRT`), ajoutez `0.0.0/0` l'ID Transit Gateway. 2. Dans la table de routage du sous-réseau Transit Gateway (**`Inspection-TGWRT`**), ajoutez **`0.0.0/0`** au SegressVPC. Table de routage SpokeVPCA Dans le tableau des itinéraires privés, ajoutez `0.0.0.0/0` à l'ID Transit Gateway. Table de routage VPCB à rayons Dans le tableau des itinéraires privés, ajoutez `0.0.0.0/0` à l'ID Transit Gateway. Tables de routage VPC de sortie Dans la table de routage publique de sortie, ajoutez le bloc d'adresse CIDR SpokeVPCA et Spoke VPCB à l'identifiant Transit Gateway.	AWS DevOps

Tâche	Description	Compétences requises
	Répétez la même étape pour le sous-réseau privé.	

Configuration CloudWatch pour effectuer une inspection du réseau en temps réel

Tâche	Description	Compétences requises
Mettez à jour la configuration de journalisation du pare-feu.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, sous Network Firewall, sélectionnez Firewalls. 3. Sur la page Pare-feu, choisissez le nom du pare-feu que vous souhaitez modifier. 4. Choisissez l'onglet Détails du pare-feu. Dans la section Journalisation, choisissez Modifier. 5. Ajustez les sélections de type de journal selon vos besoins. Vous pouvez configurer la journalisation pour les journaux d'alertes et de flux. • Alerte : envoie des journaux pour le trafic correspondant à n'importe quelle règle dynamique dont l'action	AWS DevOps

Tâche	Description	Compétences requises
	est définie sur Alert ou Drop. Pour plus d'informations sur les règles dynamiques et les groupes de règles, consultez la section Groupes de règles dans AWS Network Firewall. • Flow — Envoie des journaux pour tout le trafic réseau que le moteur sans état transmet au moteur de règles dynamiques. 6. Pour chaque type de journal sélectionné, choisissez le type de destination, puis fournissez les informations relatives à la destination de journalisation. Pour plus d'informations, consultez les destinations de journalisation d'AWS Network Firewall dans la documentation de Network Firewall. 7. Choisissez Enregistrer.	

Vérifiez la configuration

Tâche	Description	Compétences requises
Lancez une EC2 instance pour tester la configuration.	Lancez deux instances Amazon Elastic Compute Cloud (Amazon EC2) dans	AWS DevOps

Tâche	Description	Compétences requises
	le VPC en étoile : une pour Jumpbox et une pour tester la connectivité.	
Vérifiez les indicateurs.	Les métriques sont regroupées d'abord en fonction de l'espace de noms du service, puis en fonction des différentes combinaisons de dimensions au sein de chaque espace de noms. L' CloudWatch espace de noms de Network Firewall est `AWS/NetworkFirewall` . 1. Connectez-vous à AWS Management Console et ouvrez la console CloudWatch . 2. Dans le panneau de navigation, sélectionnez Métriques. 3. Dans l'onglet Toutes les mesures, choisissez la région, puis choisissez AWS/ NetworkFirewall.	AWS DevOps

Ressources connexes

- Architecture à zone unique simple avec passerelle Internet
- Architecture multizone avec passerelle Internet
- Architecture avec passerelle Internet et passerelle NAT

Déployer une tâche AWS Glue avec un pipeline AWS CodePipeline CI/CD

Créée par Bruno Klein (AWS) et Luis Henrique Massao Yamada (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle montre comment intégrer AWS CodeCommit et AWS CodePipeline à AWS Glue, et comment utiliser AWS Lambda pour lancer des tâches dès qu'un développeur envoie ses modifications dans un référentiel AWS distant. CodeCommit

Lorsqu'un développeur soumet une modification à un référentiel d'extraction, de transformation et de chargement (ETL) et transmet les modifications à AWS CodeCommit, un nouveau pipeline est invoqué. Le pipeline lance une fonction Lambda qui lance une tâche AWS Glue avec ces modifications. La tâche AWS Glue exécute la tâche ETL.

Cette solution est utile dans les situations où les entreprises, les développeurs et les ingénieurs de données souhaitent lancer des tâches dès que les modifications sont validées et transférées vers les référentiels cibles. Cela permet d'atteindre un niveau supérieur d'automatisation et de reproductibilité, évitant ainsi les erreurs lors du lancement des tâches et du cycle de vie.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Git installé sur la machine locale
- Amazon Cloud Development Kit (Amazon CDK) installé sur la machine locale
- Python installé sur la machine locale
- Le code de la section Pièces jointes

Limites

- Le pipeline est terminé dès que la tâche AWS Glue est lancée avec succès. Il n'attend pas la fin du travail.
- Le code fourni dans la pièce jointe est destiné à des fins de démonstration uniquement.

Architecture

Pile technologique cible

- AWS Glue
- AWS Lambda
- AWS CodePipeline
- AWS CodeCommit

Architecture cible

Le processus comprend les étapes suivantes :

1. Le développeur ou l'ingénieur de données apporte une modification au code ETL, valide et transmet la modification à AWS CodeCommit.
2. Le push initie le pipeline.
3. Le pipeline lance une fonction Lambda, qui `codecommit:GetFile` appelle le référentiel et télécharge le fichier vers Amazon Simple Storage Service (Amazon S3).
4. La fonction Lambda lance une nouvelle tâche AWS Glue avec le code ETL.
5. La fonction Lambda termine le pipeline.

Automatisation et mise à l'échelle

L'exemple de pièce jointe montre comment intégrer AWS Glue à AWS CodePipeline. Il fournit un exemple de référence que vous pouvez personnaliser ou étendre pour votre propre usage. Pour plus de détails, consultez la section Epics.

Outils

- AWS CodePipeline — AWS CodePipeline est un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure.
- AWS CodeCommit — AWS CodeCommit est un service de contrôle de source entièrement géré qui héberge des référentiels sécurisés basés sur Git.

- AWS Lambda — AWS Lambda est un service de calcul sans serveur qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs.
- AWS Glue — AWS Glue est un service d'intégration de données sans serveur qui facilite la découverte, la préparation et la combinaison de données à des fins d'analyse, d'apprentissage automatique et de développement d'applications.
- Client Git : Git fournit des outils d'interface graphique. Vous pouvez également utiliser la ligne de commande ou un outil de bureau pour récupérer les artefacts requis GitHub.
- AWS CDK — L'AWS CDK est un framework de développement de logiciels open source qui vous aide à définir les ressources de vos applications cloud à l'aide de langages de programmation familiers.

Épopées

Déployez l'exemple de code

Tâche	Description	Compétences requises
Configuration de l'AWS CLI.	Configurez l'interface de ligne de commande AWS (AWS CLI) pour cibler et authentifier votre compte AWS actuel. Pour obtenir des instructions, consultez la documentation de l'AWS CLI.	Développeur, DevOps ingénieur
Extrayez les exemples de fichiers de projet.	Extrayez les fichiers de la pièce jointe pour créer un dossier contenant les exemples de fichiers de projet.	Développeur, DevOps ingénieur
Déployez l'exemple de code.	Après avoir extrait les fichiers, exécutez les commandes suivantes depuis l'emplacement d'extraction pour créer un exemple de référence : `cdk bootstrap`	Développeur, DevOps ingénieur

Tâche	Description	Compétences requises

	`cdk deploy`
	`git init`
	`git remote add origin`
	`<code-commit-repos`
	`itory-url>`
	`git stage .`
	`git commit -m "adds`
	`sample code"`
	`git push --set-upstream`
	`origin main`
	
	Après la dernière commande, vous pouvez surveiller l'état du pipeline et de la tâche AWS Glue.	

Personnalisez le code.	Personnalisez le code du fichier etl.py en fonction des besoins de votre entreprise. Vous pouvez réviser le code ETL, modifier les étapes du pipeline ou étendre la solution.	Ingénieur de données

Ressources connexes

- Commencer à utiliser le kit AWS CDK
- Ajouter des tâches dans AWS Glue
- Intégrations d'actions source dans CodePipeline
- Invoquez une fonction AWS Lambda dans un pipeline dans CodePipeline
- Programmation avec AWS Glue
- CodeCommit GetFile API AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Déployez un cluster Amazon EKS depuis AWS Cloud9 à l'aide d'un profil d'instance EC2

Créée par Sagar Panigrahi (AWS)

Récapitulatif

Remarque : n' AWS Cloud9 est plus disponible pour les nouveaux clients. Les clients existants de AWS Cloud9 peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle décrit comment utiliser AWS Cloud9 et AWS CloudFormation pour créer un cluster Amazon Elastic Kubernetes Service (Amazon EKS) qui peut être exploité sans autoriser l'accès programmatique aux utilisateurs de votre compte Amazon Web Services (AWS).

AWS Cloud9 est un environnement de développement intégré (IDE) basé sur le cloud qui vous permet d'écrire, d'exécuter et de déboguer votre code à l'aide d'un navigateur. AWS Cloud9 est utilisé comme centre de contrôle qui approvisionne un cluster Amazon EKS à l'aide de profils d'instance Amazon Elastic Compute Cloud EC2 (Amazon) et de modèles AWS CloudFormation .

Vous pouvez utiliser ce modèle si vous ne souhaitez pas créer d'utilisateurs AWS Identity and Access Management (IAM) et que vous souhaitez plutôt utiliser des rôles IAM. Le contrôle d'accès basé sur les rôles (RBAC) régule l'accès aux ressources en fonction des rôles des utilisateurs individuels. Ce modèle montre comment mettre à jour le RBAC au sein d'un cluster Amazon EKS pour autoriser l'accès à un rôle IAM spécifique.

La configuration du modèle permet également à votre DevOps équipe d'utiliser les fonctionnalités d'AWS Cloud9 pour gérer et développer des ressources d'infrastructure sous forme de code (IaC) afin de créer une infrastructure Amazon EKS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Autorisations permettant de créer des rôles et des politiques IAM pour le compte. Le rôle IAM de l'utilisateur doit inclure la `AWSCloud9Administrator` politique. Les `eksNodeRoles` rôles `AWSServiceRoleForAmazonEKS` et doivent également être créés car ils sont nécessaires pour créer un cluster Amazon EKS.
- Connaissance des concepts de Kubernetes.

Limites

- Ce modèle décrit comment créer un cluster Amazon EKS de base. Pour les clusters de production, vous devez mettre à jour le CloudFormation modèle AWS.
- Le modèle ne déploie pas de composants Kubernetes supplémentaires (par exemple, Fluentd, contrôleurs d'entrée ou contrôleurs de stockage).

Architecture

Pile technologique

- AWS Cloud9
- AWS CloudFormation
- Amazon EKS
- IAM

Automatisation et mise à l'échelle

Vous pouvez étendre ce modèle et l'intégrer dans des pipelines d'intégration continue et de déploiement continu (CI/CD) afin d'automatiser le provisionnement complet d'Amazon EKS.

Outils

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications.
- AWS Cloud9 — AWS Cloud9 offre une riche expérience d'édition de code avec la prise en charge de plusieurs langages de programmation et de débogueurs d'exécution, ainsi qu'un terminal intégré.
- AWS CLI — AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS à l'aide de commandes dans votre shell de ligne de commande.

- Kubectl — `kubectl` est un utilitaire de ligne de commande que vous pouvez utiliser pour interagir avec un cluster Amazon EKS.

Épopées

Création des rôles IAM pour le profil d' EC2 instance

Tâche	Description	Compétences requises
Créez la politique IAM.	Connectez-vous à l'AWS Management Console, ouvrez la console IAM, choisissez Policies, puis Create policy. Choisissez l'onglet JSON et collez le contenu du fichier policy-role-eks-instance - profile-for-cloud 9.json (joint). Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés lors de la validation de la politique, puis choisisse z Revoir la politique. Dans le champ Nom, entrez le nom de votre stratégie. Nous vous recommandons de l'utilise r `eks-instance-profi le-for-cloud9` pour le nom de la politique. Vérifiez le récapitulatif de politique pour voir les autorisat ions accordées par votre politique. Sélectionnez ensuite Créer une politique.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un rôle IAM à l'aide de la politique.	Sur la console IAM, choisissez Rôles, puis Create role. Choisissez AWS Service, puis EC2choisissez-le dans la liste. Choisissez Next : Permissions et recherchez la politique IAM que vous avez créée précédemment. Choisissez les balises adaptées à vos besoins. Dans la section Révision, entrez le nom du rôle. Nous vous recommandons de l'utiliser `role-eks-instance-profile-for-cloud9` pour le nom du rôle. Puis choisissez Create role (Créer un rôle).	Administrateur du cloud

Création d'une politique et d'un rôle IAM pour le RBAC Amazon EKS

Tâche	Description	Compétences requises
Créez la politique IAM.	Sur la console IAM, choisissez Policies, puis Create policy. Choisissez l'onglet JSON et collez le contenu du fichier policy-for-eks-rbac .json (joint). Résolvez les avertissements de sécurité, les erreurs ou les avertissements généraux générés lors de la validation	Administrateur du cloud

Tâche	Description	Compétences requises
	de la politique, puis choisisse z Revoir la politique. Dans le champ Nom, entrez le nom de votre stratégie. Nous vous recommandons de l'utiliser `policy-for-eks-rbac` pour le nom de la politique . Vérifiez le récapitulatif de politique pour voir les autorisat ions accordées par votre politique. Sélectionnez ensuite Créer une politique.	
Créez un rôle IAM à l'aide de la politique.	Sur la console IAM, choisisse z Rôles, puis Create role. Choisissez AWS Service, puis EC2choisissez-le dans la liste. Choisissez Next : Permissio ns et recherchez la politique IAM que vous avez créée précédemment. Choisissez les balises adaptées à vos besoins. Dans la section Révision, entrez le nom du rôle. Nous vous recommandons de l'utiliser `role-eks-admin-for-rbac` pour le nom du rôle. Puis choisissez Create role (Créer un rôle).	Administrateur du cloud

Création de l'environnement AWS Cloud9

Tâche	Description	Compétences requises
Créez l'environnement AWS Cloud9.	Ouvrez la console AWS Cloud9 et choisissez Create environment. Sur la page Nom de l'environnement, entrez le nom de votre environnement. Nous vous recommandons de l'utiliser `eks-management-env` pour le nom de l'environnement. Configurez les autres paramètres en fonction de vos besoins, puis choisissez Étape suivante. Dans la page Vérifier, choisissez Créer un environnement. Patientez pendant qu'AWS Cloud9 crée votre environnement. Cela peut prendre plusieurs minutes. Pour plus d'informations sur les options de configuration disponibles, consultez la section Création d'un EC2 environnement dans la documentation AWS Cloud9.	Administrateur du cloud
Supprimez les informations d'identification IAM temporaires pour AWS Cloud9.	Une fois votre environnement AWS Cloud9 configuré, sélectionnez Paramètres dans l'icône représentant une roue dentée. Sous Préférences, choisissez les paramètre	Administrateur du cloud

Tâche	Description	Compétences requises
	s AWS, puis sélectionnez Credentials. Désactivez les informations d'identification temporaires gérées par AWS et fermez l'onglet.	
Attachez le profil d' EC2 instance à l' EC2 instance sous-jacente.	Ouvrez la EC2 console Amazon et choisissez l' EC2 instance qui correspond à votre environnement dans AWS Cloud9. Si vous avez utilisé le nom que nous avons recommandé, l' EC2 instance est appeléeaws-cloud9-eks-management-env . Choisissez l' EC2 instance, sélectionnez Actions, puis sélectionnez Paramètres de l'instance. Choisissez Attacher/remplacer le rôle IAM. Recherchez role-eks-instance-profile-for-cloud9 ou le nom du rôle IAM que vous avez créé précédemment, puis choisissez Appliquer.	Administrateur du cloud

Création du cluster Amazon EKS

Tâche	Description	Compétences requises
Créez le cluster Amazon EKS.	Téléchargez et ouvrez le modèle eks-cfn.yaml (joint) pour AWS. CloudFormation Modifiez le modèle en fonction de vos besoins. Ouvrez l'environnement AWS Cloud9 et sélectionnez Nouveau fichier. Collez le CloudFormation modèle AWS que vous avez créé précédemment dans le champ. Nous vous recommandons d'utiliser eks-cfn.yaml comme nom du modèle. Dans le terminal AWS Cloud9, exécutez la commande suivante pour créer le cluster Amazon EKS : `aws cloudformation create-stack --stack-name eks-cluster --template-body file://eks-cfn.yaml --region <your_AWS_Region>` Si l' CloudFormation appel AWS aboutit, vous recevez le nom de ressource Amazon (ARN) de la CloudForm	Administrateur du cloud

Tâche	Description	Compétences requises
	ation pile AWS dans votre sortie. La création de la pile peut prendre entre 10 et 20 minutes.	
Vérifiez l'état du cluster Amazon EKS.	Sur la CloudFormation console AWS, ouvrez la page Stacks, puis choisissez le nom de la pile. La pile est créée lorsque le code d'état de la pile s'affiche `CREATE_COMPLETE` . Pour plus d'informations, consultez la section Affichage des données et des ressources du CloudFormation stack AWS dans la CloudFormation documentation AWS.	Administrateur du cloud

Accédez aux ressources Kubernetes dans le cluster Amazon EKS

Tâche	Description	Compétences requises
Installez kubectl dans l'environnement AWS Cloud9.	Effectuez `kubectl` l'installation dans votre environnement AWS Cloud9 en suivant les instructions de la section Installation de kubectl dans la documentation Amazon EKS.	Administrateur du cloud
Mettez à jour la nouvelle configuration Amazon EKS dans AWS Cloud9.	Exécutez la commande suivante dans le terminal AWS Cloud9 pour mettre à jour le `kubeconfig` cluster	Administrateur du cloud

Tâche	Description	Compétences requises
	Amazon EKS vers l'environnement AWS Cloud9 : `aws eks update-kubeconfig --name EKS-DEV2 --region <your_AWS_Region>` **⚠ Important** `EKS-DEV2`est le nom du cluster Amazon EKS dans le CloudFormation modèle AWS que vous avez utilisé pour créer le cluster. Exécutez la `kubectl get all -A` commande pour afficher toutes les ressources Kubernetes.	

Tâche	Description	Compétences requises

Ajoutez le rôle d'administrateur IAM au RBAC Kubernetes.	Exécutez la commande suivante sur votre terminal AWS Cloud9 pour ouvrir la carte de configuration RBAC pour Amazon EKS en mode édition :
	
	`kubectl edit cm/aws-auth -n kube-system`
	
	Ajoutez les lignes suivantes sous la `mapRoles` section :
	
	`- groups:`
	`- system:masters`
	`rolearn: <ARN_of_IAM_role _from_second_epic>`
	`username: eksadmin`
	
	Lint le fichier au format YAML pour éviter les erreurs de syntaxe. Enregistrez le fichier à l'aide des `vi` commandes, puis quittez-le.
	
	Note
	En ajoutant cette section, vous informez le RBAC Kubernetes qui doit bénéficier d'`<ARN_of_IAM_role _from_second_epic>` un
		Administrateur du cloud

Tâche	Description	Compétences requises
	accès administrateur complet sur le cluster Amazon EKS. Cela signifie que le rôle IAM identifié peut effectuer des actions administratives sur le cluster Kubernetes. AWS ajoute la section existante ci-dessou s `mapRoles` lors du provisionnement du cluster Amazon EKS.	

Ressources connexes

Références

- Architecture Amazon EKS modulaire et évolutive (Quick Start)
- Gestion des utilisateurs ou des rôles IAM pour votre cluster Amazon EKS
- CloudFormation Modèle AWS pour créer un nouveau plan de contrôle Amazon EKS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Déployez du code dans plusieurs régions AWS à l'aide d'AWS CodePipeline CodeCommit, AWS et AWS CodeBuild

Créée par Anand Krishna Varanasi (AWS)

Récapitulatif

Ce modèle montre comment créer une infrastructure ou une architecture dans plusieurs régions Amazon Web Services (AWS) à l'aide d'AWS CloudFormation. Il inclut l'intégration continue (CI) / le déploiement continu (CD) dans plusieurs régions AWS pour des déploiements plus rapides. Les étapes de ce modèle ont été testées pour la création d'une CodePipeline tâche AWS à déployer dans trois régions AWS, par exemple. Vous pouvez modifier le nombre de régions en fonction de votre cas d'utilisation.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- • Un CodeBuild rôle au sein d'AmazonS3 FullAccess et CloudWatchFullAccessde ses politiques. Ces politiques permettent CodeBuild de suivre les événements d'AWS CodeCommit via Amazon CloudWatch et d'utiliser Amazon Simple Storage Service (Amazon S3) comme magasin d'artefacts.
  - Un CloudFormation rôle AWS avec les politiques suivantes, qui permettent à AWS CloudFormation, lors de la phase finale de construction, de créer ou de mettre à jour des fonctions AWS Lambda, de publier ou de consulter les CloudWatch journaux Amazon, et de créer et de mettre à jour des ensembles de modifications.
    - AWSLambdaFullAccess
    - AWSCodeDeployFullAccess
    - CloudWatchFullAccess
    - AWSCloudFormationFullAccess
    - AWSCodePipelineFullAccess

> **Note**
>
> Deux rôles AWS Identity and Access Management (IAM) pour AWS CodeBuild et AWS CloudFormation dotés de politiques appropriées CodeBuild pour effectuer les tâches de

CI consistant à tester, regrouper, empaqueter les artefacts et déployer dans plusieurs régions AWS en parallèle. Vérifiez les politiques créées par CodePipeline pour vérifier qu' CodeBuild AWS CloudFormation dispose des autorisations appropriées dans les phases CI et CD.

Architecture

L'architecture multi-régions et le flux de travail de ce modèle comprennent les étapes suivantes.

1. Vous envoyez votre code dans un CodeCommit dépôt.
2. Dès réception d'une mise à jour ou d'une validation du code, CodeCommit invoque un CloudWatch événement qui, à son tour, démarre une CodePipeline tâche.
3. CodePipeline engage le CI géré par CodeBuild. Les tâches suivantes sont effectuées.
   - Test des CloudFormation modèles AWS (facultatif)
   - Packaging des CloudFormation modèles AWS pour chaque région incluse dans le déploiement. Par exemple, ce modèle se déploie en parallèle dans trois régions AWS. Il regroupe CodeBuild donc les CloudFormation modèles AWS dans trois compartiments S3, un dans chaque région spécifiée. Les compartiments S3 sont utilisés uniquement CodeBuild comme référentiels d'artefacts.
4. CodeBuild emballe les artefacts en entrée pour la prochaine phase de déploiement, qui s'exécute en parallèle dans les trois régions AWS. Si vous spécifiez un nombre différent de régions, CodePipeline sera déployé dans ces régions.

Outils

Outils

- AWS CodePipeline CodePipeline est un service de livraison continue que vous pouvez utiliser pour modéliser, visualiser et automatiser les étapes nécessaires à la publication continue des modifications apportées à vos logiciels.
- AWS CodeBuild CodeBuild est un service de génération entièrement géré qui compile votre code source, exécute des tests unitaires et produit des artefacts prêts à être déployés.

- AWS CodeCommit CodeCommit est un service de contrôle de version hébergé par Amazon Web Services que vous pouvez utiliser pour stocker et gérer des actifs privés (tels que le code source et les fichiers binaires) dans le cloud.
- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos ressources Amazon Web Services afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications exécutées dans AWS.
- AWS Identity and Access Management — AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux ressources AWS.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle d'Internet pour les développeurs.

Code

L'exemple de code suivant concerne le `BuildSpec.yaml` fichier (phase de construction).

```
---
artifacts:
discard-paths: true
files:
- packaged-first-region.yaml
- packaged-second-region.yaml
- packaged-third-region.yaml
phases:
build:
commands:
- echo "********BUILD PHASE - CF PACKAGING**********"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_FIRST_REGION --output-template-file packaged-first-region.yaml --region
 $FIRST_REGION"
- "aws cloudformation package --template-file sam-template.yaml --s3-bucket
 $S3_SECOND_REGION --output-template-file packaged-second-region.yaml --region
 $SECOND_REGION"
- "aws cloudformation package --template-file sam-template-anand.yaml --s3-bucket
 $S3_THIRD_REGION --output-template-file packaged-third-region.yaml --region
 $THIRD_REGION"
install:
commands:
- echo "********BUILD PHASE - PYTHON SETUP**********"
runtime-versions:
```

```
python: 3.8
post_build:
commands:
- echo "********BUILD PHASE - PACKAGING COMPLETION**********"
pre_build:
commands:
- echo "********BUILD PHASE - DEPENDENCY SETUP**********"
- "npm install --silent --no-progress"
- echo "********BUILD PHASE - DEPENDENCY SETUP DONE**********"
version: 0.2
```

Épopées

Préparez le code et le CodeCommit référentiel

Tâche	Description	Compétences requises
Sélectionnez la région AWS principale pour le déploiement.	Connectez-vous à votre compte AWS et choisissez la région principale pour le déploiement. Le CodeCommit dépôt se trouvera dans la région principale.	DevOps
Créez le CodeCommit référentiel.	Créez le CodeCommit référentiel et insérez-y le code requis. Le code inclut généralement les modèles AWS CloudFormation ou AWS SAM, le code Lambda le cas échéant, et les CodeBuild `buildspec.yaml` fichiers en entrée dans AWS. CodePipeline	DevOps
Insérez le code dans le CodeCommit référentiel.	Dans la section Pièces jointes, téléchargez le code de cet exemple, puis insérez-y le code requis. En général, le	DevOps

Tâche	Description	Compétences requises
	code peut inclure des modèles AWS CloudFormation ou AWS SAM, du code Lambda et les CodeBuild `buildspec .yaml` fichiers en entrée du pipeline.	

Phase source : création du pipeline

Tâche	Description	Compétences requises
Créez le CodePipeline job.	Sur la CodePipeline console, choisissez Create pipeline.	DevOps
Nommez la CodePipel ine tâche et choisissez le paramètre du rôle de service.	Entrez un nom pour la tâche et conservez le paramètre de rôle de service par défaut afin de CodePipeline créer le rôle avec les politiques nécessair es associées.	DevOps
Spécifiez l'emplacement du magasin d'artefacts.	Sous Paramètres avancés, conservez l'option par défaut afin de CodePipeline créer un compartiment S3 à utiliser pour le stockage des artefacts de code. Si vous utilisez plutôt un compartiment S3 existant, celui-ci doit se trouver dans la région principale que vous avez spécifiée dans le premier épisode épique.	DevOps
Spécifiez la clé de chiffrement.	Conservez l'option par défaut, Default AWS Managed Key,	DevOps

Tâche	Description	Compétences requises
	ou choisissez d'utiliser votre propre clé gérée par le client AWS Key Management Service (AWS KMS).	
Spécifiez le fournisseur source.	Dans Source provider, sélectionnez AWS CodeCommit.	DevOps
Spécifiez le référentiel.	Choisissez le CodeCommit dépôt que vous avez créé dans la première épopée. Si vous avez placé le code dans une branche, choisissez-la.	DevOps
Spécifiez la manière dont les modifications de code sont détectées.	Conservez la valeur par défaut, Amazon CloudWatch Events, comme déclencheur de modification CodeCommit pour démarrer la CodePipeline tâche.	DevOps

Phase de construction : Configuration du pipeline

Tâche	Description	Compétences requises
Spécifiez le fournisseur de build.	Pour le fournisseur de build, choisissez AWS CodeBuild.	DevOps
Spécifiez la région AWS.	Choisissez la région principale, que vous avez spécifiée dans la première épopée.	DevOps

Phase de construction : création et configuration du projet

Tâche	Description	Compétences requises
Création du projet	Choisissez Créer un projet, puis entrez le nom du projet.	DevOps
Spécifiez l'image de l'environnement.	Pour cette démonstration de modèle, utilisez l'image CodeBuild gérée par défaut. Vous avez également la possibilité d'utiliser une image Docker personnalisée si vous en avez une.	DevOps
Spécifiez le système d'exploitation.	Choisissez Amazon Linux 2 ou Ubuntu. **Note** Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.	DevOps
Spécifiez le rôle du service.	Choisissez le rôle pour lequel vous avez créé le poste CodeBuild avant de commencer à créer le CodePipeline travail. (Voir la section Conditions préalables.)	DevOps
Définissez des options supplémentaires.	Pour le délai d'expiration et le délai d'attente, conservez les valeurs par défaut. Pour le certificat, conservez le	DevOps

Tâche	Description	Compétences requises
	paramètre par défaut, sauf si vous souhaitez utiliser un certificat personnalisé.	
Créez les variables d'environnement.	Pour chaque région AWS dans laquelle vous souhaitez effectuer un déploiement, créez des variables d'environnement en fournissant le nom du compartiment S3 et le nom de la région (par exemple, us-east-1).	DevOps
Indiquez le nom du fichier buildspec, s'il ne s'agit pas de buildspec.yml.	Laissez ce champ vide si le nom du fichier est le nom par défaut,`buildspec.yaml` . Si vous avez renommé le fichier buildspec, entrez le nom ici. Assurez-vous qu'il correspond au nom du fichier qui se trouve dans le CodeCommit référentiel.	DevOps
Spécifiez la journalisation.	Pour consulter les journaux d'Amazon CloudWatch Events, conservez le paramètre par défaut. Vous pouvez également définir des noms de groupes ou d'enregistreurs spécifiques.	DevOps

Ignorer la phase de déploiement

Tâche	Description	Compétences requises
Ignorez la phase de déploiement et terminez la création du pipeline.	Lorsque vous configurez le pipeline, vous CodePipeline ne pouvez créer qu'une seule étape dans la phase de déploiement. Pour effectuer un déploiement dans plusieurs régions AWS, ignorez cette phase. Une fois le pipeline créé, vous pouvez ajouter plusieurs étapes de phase de déploiement.	DevOps

Phase de déploiement : configurer le pipeline pour le déploiement dans la première région

Tâche	Description	Compétences requises
Ajoutez une étape à la phase de déploiement.	Modifiez le pipeline et choisissez Ajouter une étape dans la phase de déploiement. Cette première étape concerne la région principale.	DevOps
Indiquez le nom de l'action pour l'étape.	Entrez un nom unique qui reflète la première étape (principale) et la première région. <region>Par exemple, entrez primary_ _deploy.	DevOps
Spécifiez le fournisseur d'actions.	Pour Action provider, choisissez AWS CloudFormation.	DevOps

Tâche	Description	Compétences requises
Configurez la région pour la première étape.	Choisissez la première région (principale), la même région où CodePipeline et où vous CodeBuild êtes configurés. Il s'agit de la région principale dans laquelle vous souhaitez déployer la pile.	DevOps
Spécifiez l'artefact d'entrée.	Sélectionnez BuildArtifact. Il s'agit du résultat de la phase de construction.	DevOps
Spécifiez l'action à effectuer.	Pour le mode Action, choisissez Créer ou mettre à jour une pile.	DevOps
Entrez un nom pour la CloudFormation pile.		DevOps
Spécifiez le modèle pour la première région.	Sélectionnez le nom du package spécifique à la région qui a été empaqueté CodeBuild et déposé dans le compartiment S3 pour la première région (principale).	DevOps
Spécifiez les fonctionnalités.	Des fonctionnalités sont requises si le modèle de pile inclut des ressources IAM ou si vous créez une pile directement à partir d'un modèle contenant des macros. Pour ce modèle, utilisez CAPABILITY_IAM, CAPABILITY_NAMED_IAM, CAPABILITY_AUTO_EXPAND.	DevOps

Phase de déploiement : configurer le pipeline pour le déploiement dans la deuxième région

Tâche	Description	Compétences requises
Ajoutez la deuxième étape à la phase de déploiement.	Pour ajouter une étape pour la deuxième région, modifiez le pipeline et choisissez Ajouter une étape dans la phase de déploiement. Important : Le processus de création de la deuxième région est le même que celui de la première région, à l'exception des valeurs suivantes.	DevOps
Indiquez le nom de l'action pour la deuxième étape.	Entrez un nom unique qui reflète la deuxième étape et la deuxième région.	DevOps
Configurez la région pour la deuxième étape.	Choisissez la deuxième région dans laquelle vous souhaitez déployer la pile.	DevOps
Spécifiez le modèle pour la deuxième région.	Sélectionnez le nom du package spécifique à la région qui a été empaqueté CodeBuild et déposé dans le compartiment S3 pour la deuxième région.	DevOps

Phase de déploiement : configurer le pipeline pour le déploiement dans la troisième région

Tâche	Description	Compétences requises
Ajoutez la troisième étape à la phase de déploiement.	Pour ajouter une étape pour la troisième région, modifiez le pipeline et choisissez Ajouter	DevOps

Tâche	Description	Compétences requises
	une étape dans la phase de déploiement. Important : Le processus de création de la deuxième région est identique à celui des deux régions précédentes, à l'exception des valeurs suivantes.	
Indiquez le nom de l'action pour la troisième étape.	Entrez un nom unique qui reflète la troisième étape et la troisième région.	DevOps
Configurez la région pour la troisième étape.	Choisissez la troisième région dans laquelle vous souhaitez déployer la pile.	DevOps
Spécifiez le modèle pour la troisième région.	Sélectionnez le nom du package spécifique à la région qui a été empaqueté CodeBuild et déposé dans le compartiment S3 pour la troisième région.	DevOps

Nettoyez le déploiement

Tâche	Description	Compétences requises
Supprimez les ressources AWS.	Pour nettoyer le déploieme nt, supprimez les CloudForm ation piles dans chaque région. Supprimez ensuite les CodePipeline ressources CodeCommit CodeBuild, et de la région principale.	DevOps

Ressources connexes

- Qu'est-ce qu'AWS CodePipeline ?
- Modèle d'application sans serveur AWS
- AWS CloudFormation
- Référence de structure d' CloudFormation architecture AWS pour AWS CodePipeline

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Exécutez des requêtes SQL Amazon Redshift à l'aide de Terraform

Créée par Sylvia Qi (AWS) et Aditya Ambati (AWS)

Récapitulatif

L'utilisation de l'infrastructure en tant que code (IaC) pour le déploiement et la gestion d'Amazon Redshift est une pratique courante au sein de l'entreprise. DevOps IaC facilite le déploiement et la configuration de diverses ressources Amazon Redshift, telles que les clusters, les instantanés et les groupes de paramètres. Cependant, IaC ne s'étend pas à la gestion des ressources de base de données telles que les tables, les schémas, les vues et les procédures stockées. Ces éléments de base de données sont gérés par le biais de requêtes SQL et ne sont pas directement pris en charge par les outils IaC. Bien qu'il existe des solutions et des outils pour gérer ces ressources, vous préférerez peut-être ne pas ajouter d'outils supplémentaires à votre infrastructure technologique.

Ce modèle décrit une méthodologie qui utilise Terraform pour déployer les ressources de base de données Amazon Redshift, notamment les tables, les schémas, les vues et les procédures stockées. Le modèle fait la distinction entre deux types de requêtes SQL :

- Requêtes non répétables : ces requêtes sont exécutées une seule fois lors du déploiement initial d'Amazon Redshift afin d'établir les composants essentiels de la base de données.
- Requêtes répétables : ces requêtes sont immuables et peuvent être réexécutées sans affecter la base de données. La solution utilise Terraform pour surveiller les modifications des requêtes répétables et les appliquer en conséquence.

Pour plus de détails, consultez la section Présentation de la solution dans Informations supplémentaires.

Conditions préalables et limitations

Prérequis

Vous devez disposer d'un système actif Compte AWS et installer ce qui suit sur votre machine de déploiement :

- AWS Command Line Interface (AWS CLI)
- Un AWS CLI profil configuré avec les autorisations de lecture/écriture Amazon Redshift
- Terraform version 1.6.2 ou ultérieure

- Python 3
- Boto3

Limites

- Cette solution prend en charge une seule base de données Amazon Redshift car Terraform n'autorise la création d'une seule base de données lors de la création du cluster.
- Ce modèle n'inclut pas de tests pour valider les modifications apportées aux requêtes répétables avant de les appliquer. Nous vous recommandons d'intégrer de tels tests pour une fiabilité accrue.
- Pour illustrer la solution, ce modèle fournit un exemple de `redshift.tf` fichier qui utilise un fichier d'état Terraform local. Toutefois, pour les environnements de production, nous vous recommandons vivement d'utiliser un fichier d'état distant doté d'un mécanisme de verrouillage pour améliorer la stabilité et la collaboration.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

Cette solution est développée et testée sur le correctif 179 d'Amazon Redshift.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub amazon-redshift-sql-deploy-terraform.

Architecture

Le schéma suivant illustre comment Terraform gère les ressources de base de données Amazon Redshift en gérant à la fois les requêtes SQL non répétables et répétables.

Le schéma montre les étapes suivantes :

1. Terraform applique des requêtes SQL non répétables lors du déploiement initial du cluster Amazon Redshift.
2. Le développeur valide les modifications apportées aux requêtes SQL répétables.

3. Terraform surveille les modifications apportées aux requêtes SQL répétables.
4. Terraform applique des requêtes SQL répétables à la base de données Amazon Redshift.

La solution fournie par ce modèle est basée sur le module Terraform pour Amazon Redshift. Le module Terraform fournit un cluster et une base de données Amazon Redshift. Pour améliorer le module, nous avons utilisé `terraform_data` des ressources qui invoquent un script Python personnalisé pour exécuter des requêtes SQL à l'aide de l'opération d'API Amazon ExecuteStatementRedshift. Par conséquent, le module peut effectuer les opérations suivantes :

- Déployez autant de ressources de base de données que vous le souhaitez à l'aide de requêtes SQL après le provisionnement de la base de données.
- Surveillez en permanence les modifications apportées aux requêtes SQL répétables et appliquez ces modifications à l'aide de Terraform.

Pour plus de détails, consultez la section Présentation de la solution dans Informations supplémentaires.

Outils

Services AWS

- Amazon Redshift est un service d'entrepôt de données entièrement géré à l'échelle du pétaoctet situé dans le. AWS Cloud

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.
- Python est un langage de programmation polyvalent utilisé dans ce modèle pour exécuter des requêtes SQL.

Bonnes pratiques

- Bonnes pratiques relatives à Amazon Redshift
- Utilisation de l'API Amazon Redshift Data pour interagir avec les clusters Amazon Redshift

Épopées

Déployez la solution à l'aide de Terraform

Tâche	Description	Compétences requises
Clonez le dépôt.	Pour cloner le référentiel Git contenant le code Terraform pour le provisionnement d'un cluster Amazon Redshift, utilisez la commande suivante. `git clone https://github.com/aws-samples/amazon-redshift-sql-deploy-terraform.git`	DevOps ingénieur

Mettez à jour les variables Terraform.	Pour personnaliser le déploiement du cluster Amazon Redshift en fonction de vos besoins spécifiques, mettez à jour les paramètres suivants dans le `terraform.tfvars` fichier.
	`region = "<AWS_REGION>"`
	`cluster_identifier = "<REDSHIFT_CLUSTER_IDENTIFIER>"`
	`node_type = "<REDSHIFT_NODE_TYPE>"`
	`number_of_nodes = "<REDSHIFT_NODE_COUNT>"`
		DevOps ingénieur

Tâche	Description	Compétences requises
	database_name = "<REDSHIFT_DB_NAME>" subnet_ids = "<REDSHIFT_SUBNET_IDS>" vpc_security_group_ids = "<REDSHIFT_SECURITY_GROUP_IDS>" run_nonrepeatable_queries = true run_repeatable_queries = true sql_path_bootstrap = "<BOOTSTRAP_SQLS_PATH>" sql_path_nonrepeatable = "<NON-REPEATABLE_SQLS_PATH>" sql_path_repeatable = "<REPEATABLE_SQLS_PATH>" sql_path_finalize = "<FINALIZE_SQLS_PATH>" create_random_password = false master_username = "<REDSHIFT_MASTER_USERNAME>"	

Tâche	Description	Compétences requises

Déployez les ressources à l'aide de Terraform.	1. Pour préparer le processus de déploiement, utilisez la commande suivante pour initialiser Terraform dans le référentiel cloné.
	`terraform init`
	2. Pour prévisualiser les modifications que Terraform appliquera à l'infrastructure, utilisez la commande suivante pour créer un plan d'exécution.
	`terraform plan -var-file terraform.tfvars`
	3. Pour provisionner le cluster Amazon Redshift et les ressources associées , utilisez la commande suivante pour appliquer le plan d'exécution Terraform.
	`terraform apply -var-file terraform.tfvars`
		DevOps ingénieur

Tâche	Description	Compétences requises

(Facultatif) Exécutez des requêtes SQL supplémentaires.	Le référentiel d'exemples fournit plusieurs requêtes SQL à des fins de démonstration. Pour exécuter vos propres requêtes SQL, ajoutez-les dans les dossiers suivants :
	`/bootstrap`
	`/nonrepeatable`
	`/repeatable`
	`/finalize`	

Surveiller l'exécution des instructions SQL

Tâche	Description	Compétences requises
Surveillez le déploiement des instructions SQL.	Vous pouvez surveiller les résultats des exécutions SQL sur un cluster Amazon Redshift. Pour obtenir des exemples de résultats illustrant un échec ou une exécution réussie de SQL, reportez-vous à la section Exemples d'instructions SQL dans Informations supplémentaires.	DBA, ingénieur DevOps
Nettoyez les ressources.	Pour supprimer toutes les ressources déployées par Terraform, exécutez la commande suivante.	DevOps ingénieur

Tâche	Description	Compétences requises
	`terraform destroy`	

Valider les résultats

Tâche	Description	Compétences requises
Validez les données dans le cluster Amazon Redshift.	1. Connectez-vous à la console AWS Management Console Amazon Redshift et ouvrez-la. 2. Dans le menu de navigation, choisissez Clusters. Choisissez le nom du cluster approprié dans la liste. 3. Suivez les instructions de la section Interrogation d'une base de données à l'aide de l'éditeur de requêtes Amazon Redshift v2 dans la documentation Amazon Redshift.	ADMINISTRATEUR DE BASES DE DONNÉES, AWS DevOps

Ressources connexes

AWS documentation

- Clusters provisionnés par Amazon Redshift
- Résolution des problèmes liés à l'API Amazon Redshift Data

Autres ressources

- Commande : appliquer (documentation Terraform)

Informations supplémentaires

Présentation de la solution

Pour utiliser la solution, vous devez organiser vos requêtes SQL Amazon Redshift de manière spécifique. Toutes les requêtes SQL doivent être stockées dans des fichiers dotés d'une `.sql` extension.

Dans l'exemple de code fourni avec ce modèle, les requêtes SQL sont organisées dans la structure de dossiers suivante. Vous pouvez modifier le code (`sql-queries.tf`et`sql-queries.py`) pour qu'il fonctionne avec n'importe quelle structure adaptée à votre cas d'utilisation unique.

```
/bootstrap
     |- Any # of files
     |- Any # of sub-folders
/nonrepeatable
     |- Any # of files
     |- Any # of sub-folders
/repeatable
     /udf
          |- Any # of files
          |- Any # of sub-folders
     /table
          |- Any # of files
          |- Any # of sub-folders
     /view
          |- Any # of files
          |- Any # of sub-folders
     /stored-procedure
          |- Any # of files
          |- Any # of sub-folders
/finalize
     |- Any # of files
     |- Any # of sub-folders
```

Compte tenu de la structure de dossiers précédente, lors du déploiement du cluster Amazon Redshift, Terraform exécute les requêtes dans l'ordre suivant :

1. `/bootstrap`
2. `/nonrepeatable`
3. `/repeatable`

4. `/finalize`

Le `/repeatable` dossier contient quatre sous-dossiers :`/udf`, `/table/view`, et`/stored-procedure`. Ces sous-dossiers indiquent l'ordre dans lequel Terraform exécute les requêtes SQL.

Le script Python qui exécute les requêtes SQL est`sql-queries.py`. Tout d'abord, le script lit tous les fichiers et sous-dossiers d'un répertoire source spécifique, par exemple le `sql_path_bootstrap` paramètre. Le script exécute ensuite les requêtes en appelant l'opération d'API Amazon ExecuteStatementRedshift. Vous pouvez avoir une ou plusieurs requêtes SQL dans un fichier. L'extrait de code suivant montre la fonction Python qui exécute les instructions SQL stockées dans un fichier sur un cluster Amazon Redshift.

```
def execute_sql_statement(filename, cluster_id, db_name, secret_arn, aws_region):
    """Execute SQL statements in a file"""
    redshift_client = boto3.client(
        'redshift-data', region_name=aws_region)
    contents = get_contents_from_file(filename),
    response = redshift_client.execute_statement(
        Sql=contents[0],
        ClusterIdentifier=cluster_id,
        Database=db_name,
        WithEvent=True,
        StatementName=filename,
        SecretArn=secret_arn
    )
    ...
```

Le script Terraform `sql-queries.tf` crée les ressources terraform_data qui appellent le script. `sql-queries.py` Il existe une `terraform_data` ressource pour chacun des quatre dossiers : `/bootstrap/nonrepeatable`,`/repeatable`, et`/finalize`. L'extrait de code suivant montre la `terraform_data` ressource qui exécute les requêtes SQL dans le `/bootstrap` dossier.

```
locals {
  program               = "${path.module}/sql-queries.py"
  redshift_cluster_name = try(aws_redshift_cluster.this[0].id, null)
}

resource "terraform_data" "run_bootstrap_queries" {
  count      = var.create && var.run_nonrepeatable_queries && (var.sql_path_bootstrap !
= "") && (var.snapshot_identifier == null) ? 1 : 0
```

```
  depends_on = [aws_redshift_cluster.this[0]]

  provisioner "local-exec" {
    command = "python3 ${local.program} ${var.sql_path_bootstrap}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}
 ${local.aws_region}"
  }
}
```

Vous pouvez contrôler l'exécution de ces requêtes à l'aide des variables suivantes. Si vous ne souhaitez pas exécuter de requêtes dans `sql_path_bootstrapsql_path_nonrepeatable`, `sql_path_repeatablesql_path_finalize`, ou définir leurs valeurs sur`""`.

```
  run_nonrepeatable_queries = true
  run_repeatable_queries    = true
  sql_path_bootstrap        = "src/redshift/bootstrap"
  sql_path_nonrepeatable    = "src/redshift/nonrepeatable"
  sql_path_repeatable       = "src/redshift/repeatable"
  sql_path_finalize         = "src/redshift/finalize"
```

Lorsque vous exécutez`terraform apply`, Terraform prend en compte la `terraform_data` ressource ajoutée une fois le script terminé, quels que soient les résultats du script. Si certaines requêtes SQL ont échoué et que vous souhaitez les exécuter à nouveau, vous pouvez supprimer manuellement la ressource de l'état Terraform et l'exécuter à nouveau. `terraform apply` Par exemple, la commande suivante supprime la `run_bootstrap_queries` ressource de l'état Terraform.

```
terraform state rm module.redshift.terraform_data.run_bootstrap_queries[0]
```

L'exemple de code suivant montre comment la `run_repeatable_queries` ressource surveille les modifications dans le `repeatable` dossier à l'aide du hachage sha256. Si un fichier du dossier est mis à jour, Terraform marque l'ensemble du répertoire pour une mise à jour. Ensuite, Terraform exécute à nouveau les requêtes dans le répertoire lors de la suivante. `terraform apply`

```
resource "terraform_data" "run_repeatable_queries" {
  count      = var.create_redshift && var.run_repeatable_queries &&
 (var.sql_path_repeatable != "") ? 1 : 0
  depends_on = [terraform_data.run_nonrepeatable_queries]

  # Continuously monitor and apply changes in the repeatable folder
  triggers_replace = {
```

```
    dir_sha256 = sha256(join("", [for f in fileset("${var.sql_path_repeatable}",
 "**") : filesha256("${var.sql_path_repeatable}/${f}")]))
  }

  provisioner "local-exec" {
    command = "python3 ${local.sql_queries} ${var.sql_path_repeatable}
 ${local.redshift_cluster_name} ${var.database_name} ${var.redshift_secret_arn}"
  }
}
```

Pour affiner le code, vous pouvez implémenter un mécanisme permettant de détecter et d'appliquer des modifications uniquement aux fichiers qui ont été mis à jour dans le `repeatable` dossier, plutôt que d'appliquer les modifications à tous les fichiers sans distinction.

Exemples d'instructions SQL

La sortie suivante montre un échec de l'exécution de SQL, ainsi qu'un message d'erreur.

```
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/nonrepeatable
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): src/redshift/
nonrepeatable/table/admin/admin.application_family.sql
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):
 ----------------------------------------------------------------------
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Status:
 FAILED
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): SQL execution
 failed.
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec): Error
 message: ERROR: syntax error at or near ")"
module.redshift.terraform_data.run_nonrepeatable_queries[0] (local-exec):   Position:
 244
module.redshift.terraform_data.run_nonrepeatable_queries[0]: Creation complete after 3s
 [id=ee50ba6c-11ae-5b64-7e2f-86fd8caa8b76]
```

Le résultat suivant montre une exécution SQL réussie.

```
module.redshift.terraform_data.run_bootstrap_queries[0]: Provisioning with 'local-
exec'...
```

```
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Executing:
 ["/bin/sh" "-c" "python3 modules/redshift/sql-queries.py src/redshift/bootstrap
 testcluster-1 db1 arn:aws:secretsmanager:us-east-1:XXXXXXXXXXXX:secret:/redshift/
master_user/password-8RapGH us-east-1"]
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): src/redshift/
bootstrap/db.sql
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec):
 ----------------------------------------------------------------
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): Status: FINISHED
module.redshift.terraform_data.run_bootstrap_queries[0] (local-exec): SQL execution
 successful.
module.redshift.terraform_data.run_bootstrap_queries[0]: Creation complete after 2s
 [id=d565ef6d-be86-8afd-8e90-111e5ea4a1be]
```

Exportez les rapports AWS Backup de l'ensemble d'une organisation dans AWS Organizations sous forme de fichier CSV

Créée par Aromal Raj Jayarajan (AWS) et Purushotham GK (AWS)

Récapitulatif

Ce modèle montre comment exporter les rapports de tâches AWS Backup provenant de l'ensemble d'une organisation dans AWS Organizations sous forme de fichier CSV. La solution utilise AWS Lambda et Amazon EventBridge pour classer les rapports de tâches AWS Backup en fonction de leur statut, ce qui peut faciliter la configuration d'automatisations basées sur le statut.

AWS Backup aide les entreprises à gérer et à automatiser de manière centralisée la protection des données sur l'ensemble des services AWS, dans le cloud et sur site. Toutefois, pour les tâches AWS Backup configurées dans AWS Organizations, les rapports consolidés ne sont disponibles que dans l'AWS Management Console du compte de gestion de chaque organisation. Le fait de transférer ces rapports en dehors du compte de gestion peut réduire les efforts nécessaires à l'audit et élargir le champ des automatisations, des notifications et des alertes.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une organisation active au sein d'AWS Organizations qui inclut au moins un compte de gestion et un compte de membre
- AWS Backup configuré au niveau de l'organisation dans AWS Organizations (pour plus d'informations, consultez Automatiser la sauvegarde centralisée à grande échelle sur l'ensemble des services AWS à l'aide d'AWS Backup sur le blog AWS)
- Git, installé et configuré sur votre machine locale

Limites

La solution fournie dans ce modèle identifie les ressources AWS configurées uniquement pour les tâches AWS Backup. Le rapport ne permet pas d'identifier les ressources AWS qui ne sont pas configurées pour la sauvegarde via AWS Backup.

Architecture

Pile technologique cible

- AWS Backup
- AWS CloudFormation
- Amazon EventBridge
- AWS Lambda
- AWS Security Token Service (AWS STS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Identity and Access Management (IAM)

Architecture cible

Le schéma suivant montre un exemple de flux de travail pour l'exportation des rapports de travail AWS Backup provenant de l'ensemble d'une organisation dans AWS Organizations sous forme de fichier CSV.

Le schéma suivant illustre le flux de travail suivant :

1. Une règle d' EventBridge événement planifié invoque une fonction Lambda dans le compte AWS du membre (de reporting).
2. La fonction Lambda utilise ensuite AWS STS pour assumer un rôle IAM disposant des autorisations requises pour se connecter au compte de gestion.
3. La fonction Lambda effectue ensuite les opérations suivantes :
   - Demande le rapport consolidé sur les tâches AWS Backup au service AWS Backup
   - Catégorise les résultats en fonction du statut de la tâche AWS Backup
   - Convertit la réponse en fichier CSV
   - Télécharge les résultats dans un compartiment Amazon S3 du compte de reporting, dans des dossiers étiquetés en fonction de leur date de création.

Outils

Outils

- AWS Backup est un service entièrement géré qui vous aide à centraliser et à automatiser la protection des données sur l'ensemble des services AWS, dans le cloud et sur site.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur les comptes et les régions AWS.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions AWS Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres comptes AWS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à approvisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

Le code de ce modèle est disponible dans le GitHub aws-backup-report-generatorréférentiel.

Bonnes pratiques

- Bonnes pratiques de sécurité pour Amazon S3 (Guide de l'utilisateur Amazon S3)
- Bonnes pratiques d'utilisation des fonctions AWS Lambda (Guide du développeur AWS Lambda)
- Bonnes pratiques pour le compte de gestion (Guide de l'utilisateur d'AWS Organizations)

Épopées

Déployer les composants de la solution

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Clonez le GitHub aws-backup-report-generatordépôt	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	en exécutant la commande suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/aws-backup-report-generator.git` Pour plus d'informations, consultez la section Clonage d'un dépôt dans la GitHub documentation.	

Tâche	Description	Compétences requises
Déployez les composants de la solution sur le compte AWS du membre (de reporting).	1. Dans le compte membre (reporting), connectez-vous à l'AWS Management Console, puis ouvrez la CloudFormation console. 2. Choisissez Créer une pile, puis choisissez Avec de nouvelles ressources (standard). 3. Sur la page Créer une pile, dans la section Spécifier un modèle, choisissez Télécharger un fichier modèle. 4. Sélectionnez Choose file (Choisir un fichier). Accédez ensuite au dossier racine du GitHub dépôt cloné sur votre poste de travail local et choisissez template-reporting.yaml. 5. Choisissez Ouvrir, puis Next. 6. Sur la page Spécifier les détails de la pile, dans Nom de la pile, entrez le nom de votre CloudFormation pile. 7. Pour ManagementAccountID, entrez l'ID du compte AWS du compte de gestion de votre organisation dans AWS Organizations. 8. Choisissez Next (Suivant).	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	9. Sur la page Configurer les options de pile, choisissez Next. 10. Sur la page Révision, cochez la case pour confirmer que vous avez vérifié la configuration. 11. Sélectionnez Créer la pile. La pile affiche le statut CREATE_COMPLETE lorsque les composants de la solution sont déployés dans le compte membre (reporting).	

Tester la solution

Tâche	Description	Compétences requises
Assurez-vous que la EventBridge règle s'exécute avant de procéder au test.	Assurez-vous que la EventBridge règle s'exécute en attendant au moins 24 heures ou en augmentant la fréquence des rapports dans le CloudFormation fichier template-reporting.yml du modèle. Pour augmenter la fréquence des rapports 1. Ouvrez le fichier template-reporting.yml dans le référentiel cloné.	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	2. Dans la règle d'événement dont l'identifiant logique est LambdaSchedule« », recherchez le « ScheduleExpression ». 3. Modifiez la touche ScheduleExpression« » afin qu'elle inclue une expression cron valide. Par exemple, l'expression cron suivante planifie l'exécution de la règle d'événement toutes les cinq minutes : “`cron(* /5 * * * *)`”	

Tâche	Description	Compétences requises
Vérifiez le rapport généré dans le compartiment Amazon S3.	1. Dans le compte membre (reporting), connectez-vous à l'AWS Management Console, puis ouvrez la CloudFormation console. 2. Dans le volet Stacks, sélectionnez le nom de la pile que vous avez créée. Choisissez ensuite l'onglet Ressources. 3. Dans le volet Ressources, dans la colonne Logical ID, recherchez BackupReportS3Bucket. Ouvrez ensuite le compartiment Amazon S3 associé dans un nouvel onglet en sélectionnant le lien dans la colonne Physical ID à côté de cet ID logique. 4. Assurez-vous que le bucket contient un rapport généré au format suivant : BackupReports////BackupReport- - - - .csv <yyyy><mm><dd><BACKUP JOB STATUS><dd><Mon><yyyy>	AWS DevOps, DevOps ingénieur

Nettoyage de vos ressources

Tâche	Description	Compétences requises
Supprimez les composants de la solution du compte membre (de reporting).	1. Dans le compte membre (de reporting), ouvrez le compartiment Amazon S3 de la solution. Pour obtenir des instructions, reportez-vous aux étapes 2 à 4 du compartiment Check the S3 pour connaître le rapport généré dans la section Tester la solution de ce modèle. 2. Supprimez le contenu du compartiment et videz-le. Pour obtenir des instructions, consultez la section Vidage d'un compartiment dans le guide de l'utilisateur Amazon S3. 3. Dans le compte membre (reporting), connectez-vous à l'AWS Management Console, puis ouvrez la CloudFormation console. 4. Dans le volet Stacks, cochez la case à côté du nom de la pile que vous avez créée. Ensuite, choisissez Supprimer.	AWS DevOps, DevOps ingénieur
Supprimez les composants de la solution du compte de gestion.	1. Dans le compte de gestion, connectez-vous à l'AWS Management Console, puis	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	ouvrez la CloudFormation console. 2. Dans le volet Stacks, cochez la case à côté du nom de la pile que vous avez créée. Ensuite, choisissez Supprimer.	

Ressources connexes

- Tutoriel : Utilisation d'AWS Lambda avec des événements planifiés (documentation AWS Lambda)
- Création d'événements planifiés pour exécuter les fonctions AWS Lambda (SDK AWS pour la documentation) JavaScript
- Tutoriel IAM : déléguer l'accès entre les comptes AWS à l'aide de rôles IAM (documentation IAM)
- Terminologie et concepts d'AWS Organizations (documentation AWS Organizations)
- Création de plans de rapports à l'aide de la console AWS Backup (documentation AWS Backup)
- Création d'un rapport d'audit (documentation AWS Backup)
- Création de rapports à la demande (documentation AWS Backup)
- Qu'est-ce qu'AWS Backup ? (Documentation AWS Backup)
- Automatisez la sauvegarde centralisée à grande échelle sur l'ensemble des services AWS à l'aide d'AWS Backup (article de blog AWS)

Exporter les balises d'une liste d' EC2 instances Amazon vers un fichier CSV

Créée par Sida Ju (AWS) et Pac Joonhyun (AWS)

Récapitulatif

Ce modèle montre comment exporter par programmation les balises d'une liste d'instances Amazon Elastic Compute Cloud EC2 (Amazon) vers un fichier CSV.

En utilisant l'exemple de script Python fourni, vous pouvez réduire le temps nécessaire pour examiner et classer vos EC2 instances Amazon par des balises spécifiques. Par exemple, vous pouvez utiliser le script pour identifier et classer rapidement une liste d'instances que votre équipe de sécurité a signalées comme nécessitant des mises à jour logicielles.

Conditions préalables et limitations

Prérequis

- Python 3 installé et configuré
- Interface de ligne de commande (AWS CLI) (AWS CLI) installée et configurée

Limites

L'exemple de script Python fourni dans ce modèle permet de rechercher EC2 des instances Amazon uniquement sur la base des attributs suivants :

- Instance IDs
- IPv4 Adresses privées
- IPv4 Adresses publiques

Outils

- Python est un langage de programmation informatique polyvalent.
- virtualenv vous aide à créer des environnements Python isolés.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

Référentiel de code

L'exemple de script Python pour ce modèle est disponible dans le référentiel GitHub search-ec2 -. instances-export-tags

Épopées

Installation et configuration des prérequis

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	**Note** Si vous recevez des erreurs lors de l'exécution des commandes de l'AWS CLI, assurez-vous que vous utilisez la version la plus récente de l'AWS CLI. Clonez le instances-export-tags dépôt GitHub search-ec2- en exécutant la commande Git suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/search-ec2-instances-export-tags.git`	DevOps ingénieur
Installez et activez virtualenv.	1. Installez virtualenv en exécutant la commande suivante :	DevOps ingénieur

Tâche	Description	Compétences requises

	`python3 -m pip install virtualenv`
	2. Créez un nouvel environnement virtuel en exécutant la commande suivante :
	`python3 -m venv env`
	3. Activez le nouvel environnement virtuel en exécutant la commande suivante :
	`source env/bin/activate`
	Pour plus d'informations, consultez le guide de l'utilisateur de virtualenv.	

Installez les dépendances.	1. Ouvrez le répertoire du code en exécutant la commande suivante dans le terminal :
	`cd search-ec2-instances-export-tags`
	2. Installez le `requirements.txt` fichier en exécutant la commande pip suivante :
	`pip3 install -r requirements.txt`
		DevOps ingénieur

Tâche	Description	Compétences requises
Configurez un profil nommé AWS.	Si ce n'est pas déjà fait, configurez un profil nommé AWS qui inclut les informations d'identification requises pour exécuter le script. Pour créer un profil nommé, exécutez la commande aws configure. Pour plus d'informations, consultez la section Utilisation de profils nommés dans la documentation de l'AWS CLI.	DevOps ingénieur

Configurer et exécuter le script Python

Tâche	Description	Compétences requises
Créez le fichier d'entrée.	Créez un fichier d'entrée contenant la liste des EC2 instances Amazon pour lesquelles le script doit rechercher et exporter des balises. Vous pouvez répertorier les instances IDs, IPv4 les adresses privées ou IPv4 les adresses publiques. ⚠ Important Assurez-vous que chaque EC2 instance Amazon est répertoriée sur sa propre	DevOps ingénieur

Tâche	Description	Compétences requises

	ligne dans le fichier d'entrée.
	
	Exemple de fichier d'entrée
	
	`1 i-0547c351bdfe85b9f`
	`2 54.157.194.156`
	`3 172.31.85.33`
	`4 54.165.198.144`
	`5 i-0b6223b5914111a4b`
	`6 172.31.85.44`
	`7 54.165.198.145`
	`8 172.31.80.219`
	`9 172.31.94.199`	

Tâche	Description	Compétences requises
Exécutez le script python.	Exécutez le script en exécutant la commande suivante dans le terminal : `python search_instances.py -i INPUTFILE -o OUTPUTFILE -r REGION [-p PROFILE]` **Note** Remplacez `INPUTFILE` par le nom de votre fichier d'entrée. `OUTPUTFILE` Remplacez-le par le nom que vous souhaitez attribuer au fichier de sortie CSV. `REGION`Remplacez-le par la région AWS dans laquelle se trouvent vos EC2 ressources Amazon. Si vous utilisez un profil nommé AWS, remplacez-le `PROFILE` par le profil nommé que vous utilisez. Pour obtenir la liste des paramètres pris en charge et	DevOps ingénieur

Tâche	Description	Compétences requises
	leur description, exécutez la commande suivante : `python search_instances.py -h` Pour plus d'informations et pour voir un exemple de fichier de sortie, consultez le `README.md` fichier dans le référentiel GitHub search-ec2 -. instances-export-tags	

Ressources connexes

- Configuration de l'interface de ligne de commande AWS (Guide de l'utilisateur de l'interface de ligne de commande AWS)

Générez un CloudFormation modèle AWS contenant les règles gérées par AWS Config à l'aide de Troposphere

Créée par Lucas Nation (AWS) et Freddie Wilson (AWS)

Récapitulatif

De nombreuses organisations utilisent les règles gérées par AWS Config pour évaluer la conformité de leurs ressources Amazon Web Services (AWS) par rapport aux meilleures pratiques courantes. Cependant, la maintenance de ces règles peut prendre du temps et ce modèle vous permet de tirer parti de Troposphere, une bibliothèque Python, pour générer et gérer les règles gérées par AWS Config.

Le modèle vous aide à gérer vos règles gérées par AWS Config en utilisant un script Python pour convertir une feuille de calcul Microsoft Excel contenant des règles gérées par AWS en un CloudFormation modèle AWS. Troposphere agit comme une infrastructure en tant que code (IaC), ce qui signifie que vous pouvez mettre à jour la feuille de calcul Excel avec des règles gérées, au lieu d'utiliser un fichier au format JSON ou YAML. Vous utilisez ensuite le modèle pour lancer une CloudFormation pile AWS qui crée et met à jour les règles gérées dans votre compte AWS.

Le CloudFormation modèle AWS définit chaque règle gérée par AWS Config à l'aide de la feuille de calcul Excel et vous permet d'éviter de créer manuellement des règles individuelles dans l'AWS Management Console. Le script définit par défaut les paramètres de chaque règle gérée sur un dictionnaire vide et les paramètres *`ComplianceResourceTypes`* par défaut de la portée sur. *`THE_RULE_IDENTIFIER.template file`* Pour plus d'informations sur l'identifiant de règle, consultez la section Création de règles gérées par AWS Config avec des CloudFormation modèles AWS dans la documentation AWS Config.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Connaissance de l'utilisation de CloudFormation modèles AWS pour créer des règles gérées par AWS Config. Pour plus d'informations à ce sujet, consultez la section Création de règles gérées par AWS Config avec CloudFormation des modèles AWS dans la documentation AWS Config.
- Python 3, installé et configuré. Pour plus d'informations à ce sujet, consultez la documentation Python.

- Un environnement de développement intégré (IDE) existant.
- Identifiez vos unités organisationnelles (OUs) dans une colonne de l'exemple de feuille de calcul `excel_config_rules.xlsx` Excel (ci-joint).

Épopées

Personnalisation et configuration des règles gérées par AWS Config

Tâche	Description	Compétences requises
Mettez à jour l'exemple de feuille de calcul Excel.	Téléchargez l'exemple de feuille de calcul `excel_config_rules.xlsx` Excel (ci-joint) et étiquetez `Implemented` les règles gérées par AWS Config que vous souhaitez utiliser. Les règles marquées comme étant `Implemented` seront ajoutées au CloudFormation modèle AWS.	Developer
(Facultatif) Mettez à jour le fichier config_rules_params.json avec les paramètres des règles AWS Config.	Certaines règles gérées par AWS Config nécessitent des paramètres et doivent être transmises au script Python sous forme de fichier JSON à l'aide de l'`--param-file` option. Par exemple, la règle `access-keys-rotated` gérée utilise le `maxAccessKeyAge` paramètre suivant : `{`	Developer

Tâche	Description	Compétences requises

	<pre>"access-keys-rotated": {
	"InputParameters": {
	"maxAccessKeyAge": 90
	}
	}
	}</pre>
	Dans cet exemple de paramètre, la valeur `maxAccessKeyAge` est fixée à 90 jours. Le script lit le fichier de paramètres et ajoute ceux `InputParameters` qu'il trouve.	

Tâche	Description	Compétences requises
(Facultatif) Mettez à jour le fichier config_rules_params.json avec AWS Config. ComplianceResourceTypes	Par défaut, le script Python `ComplianceResourceTypes` extrait les modèles définis par AWS. Si vous souhaitez modifier le champ d'application d'une règle gérée par AWS Config spécifique, vous devez la transmettre au script Python sous forme de fichier JSON à l'aide de l'`--param-file` option. Par exemple, l'exemple de code suivant montre comment le `ComplianceResourceTypes` formulaire `ec2-volume-inuse-check` est défini dans la `["AWS::EC2::Volume"]` liste : `{ "ec2-volume-inuse-check": { "Scope": { "ComplianceResourceTypes": [ "AWS::EC2::Volume" ] } } }`	Developer

Exécutez le script Python

Tâche	Description	Compétences requises
Installez les packages pip à partir du fichier requirements.txt.	Téléchargez le `requirements.txt` fichier (joint) et exécutez la commande suivante dans votre IDE pour installer les packages Python : `pip3 install -r requirements.txt`	Developer
Exécutez le script python.	1. Téléchargez le `aws_config_rules.py` fichier (joint) sur votre ordinateur local. 2. **Note** Exécutez la `- python3 aws_config_rules.py --ou <OU_NAME>` commande. : `--ou` définit la colonne UO à choisir dans la feuille de calcul Excel. Vous pouvez également ajouter les paramètres facultatifs suivants : • `--config-rule-option` — Définit les règles à	Developer

Tâche	Description	Compétences requises
	choisir dans la feuille de calcul Excel. La valeur par défaut est le `Implemented` paramètre. • `--excel-file` — Le chemin de la feuille de calcul Excel. L'argument par défaut est `aws_config_rules.xlsx` . • `--param-file` — Le chemin du fichier JSON de paramètres. L'argument par défaut est `config_rules_params.json` . • `--max-execution-frequency` — Définit la fréquence à laquelle les règles gérées par AWS Config sont évaluées. Les choix sont `One_Hour` `Three_Hours` , `Six_Hours` `Twelve_Hours` , ou `TwentyFour_Hours` . L'argument par défaut est `TwentyFour_Hours` .	

Déployez les règles gérées par AWS Config

Tâche	Description	Compétences requises
Lancez la CloudFormation pile AWS.	1. Connectez-vous à l'AWS Management Console, ouvrez la CloudForm	Developer

Tâche	Description	Compétences requises
	ation console AWS, puis choisissez Create stack. 2. Sur la page Spécifier le modèle, choisissez Charger un fichier modèle, puis chargez votre CloudForm ation modèle AWS. 3. Spécifiez un nom de pile, puis choisissez Next. 4. Spécifiez les balises, puis choisissez Next. 5. Sélectionnez Créer la pile.	

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Donnez aux instances de SageMaker bloc-notes un accès temporaire à un CodeCommit référentiel dans un autre compte AWS

Créée par Helge Aufderheide (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle montre comment accorder aux instances d'Amazon SageMaker Notebook et aux utilisateurs un accès temporaire à un CodeCommit référentiel AWS qui se trouve dans un autre compte AWS. Ce modèle montre également comment vous pouvez accorder des autorisations granulaires pour des actions spécifiques que chaque entité peut effectuer sur chaque référentiel.

Organisations stockent souvent CodeCommit les référentiels dans un compte AWS différent de celui qui héberge leur environnement de développement. Cette configuration multi-comptes permet de contrôler l'accès aux référentiels et de réduire le risque de suppression accidentelle de ceux-ci. Pour accorder ces autorisations entre comptes, il est recommandé d'utiliser les rôles AWS Identity and Access Management (IAM). Les identités IAM prédéfinies de chaque compte AWS peuvent ensuite assumer temporairement les rôles nécessaires pour créer une chaîne de confiance contrôlée entre les comptes.

> **Note**
>
> Vous pouvez appliquer une procédure similaire pour accorder à d'autres identités IAM l'accès entre comptes à un CodeCommit référentiel. Pour plus d'informations, consultez Configurer l'accès entre comptes à un CodeCommit référentiel AWS à l'aide de rôles dans le guide de l' CodeCommit utilisateur AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec un CodeCommit référentiel (compte A)
- Un deuxième compte AWS actif avec une instance de SageMaker bloc-notes (compte B)
- Un utilisateur AWS disposant des autorisations suffisantes pour créer et modifier des rôles IAM dans le compte A

- Un deuxième utilisateur AWS disposant des autorisations suffisantes pour créer et modifier des rôles IAM dans le compte B

Architecture

Le schéma suivant montre un exemple de flux de travail permettant d'accorder à une instance de SageMaker bloc-notes et aux utilisateurs d'un compte AWS un accès croisé à un CodeCommit référentiel :

Le schéma suivant illustre le flux de travail suivant :

1. Le rôle d'utilisateur AWS et le rôle d'instance de SageMaker bloc-notes dans le compte B supposent un profil nommé.
2. La politique d'autorisation du profil nommé spécifie un rôle d' CodeCommit accès dans le compte A que le profil assume ensuite.
3. La politique de confiance du rôle d' CodeCommit accès dans le compte A permet au profil nommé dans le compte B d'assumer le rôle CodeCommit d'accès.
4. La politique d'autorisations IAM du CodeCommit référentiel dans le compte A autorise le rôle CodeCommit d'accès à accéder au CodeCommit référentiel.

Pile technologique

- CodeCommit
- Git
- IAM
- pip
- SageMaker

Outils

- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

- Git est un système de contrôle de version distribué permettant de suivre les modifications du code source pendant le développement de logiciels.
- git-remote-codecommitest un utilitaire qui vous permet de transférer et d'extraire du code depuis des CodeCommit référentiels en étendant Git.
- pip est le programme d'installation du package pour Python. Vous pouvez utiliser pip pour installer des packages à partir de l'index des packages Python et d'autres index.

Bonnes pratiques

Lorsque vous définissez des autorisations à l'aide de politiques IAM, assurez-vous de n'accorder que les autorisations requises pour effectuer une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

Lorsque vous implémentez ce modèle, veillez à effectuer les opérations suivantes :

- Vérifiez que les principes IAM disposent uniquement des autorisations requises pour effectuer des actions spécifiques et nécessaires au sein de chaque référentiel. Par exemple, il est recommandé d'autoriser les principes IAM approuvés à appliquer et à fusionner les modifications apportées à des branches spécifiques du référentiel, mais de ne demander des fusions qu'aux branches protégées.
- Vérifiez que les principes IAM se voient attribuer différents rôles IAM en fonction de leurs rôles et responsabilités respectifs pour chaque projet. Par exemple, les autorisations d'accès d'un développeur seront différentes de celles d'un responsable de publication ou d'un administrateur AWS.

Épopées

Configuration des rôles IAM

Tâche	Description	Compétences requises
Configurez le rôle CodeCommit d'accès et la politique d'autorisations.	**Note** Pour automatiser le processus de configuration manuelle décrit dans cette	Informations générales sur AWS, AWS DevOps

Tâche	Description	Compétences requises
	épopée, vous pouvez utiliser un CloudFormation modèle AWS. Dans le compte qui contient le CodeCommit référentiel (compte A), procédez comme suit : 1. Créez un rôle IAM qui peut être assumé par le rôle d'instance de SageMaker bloc-notes dans le compte B. 2. Créez une politique IAM qui accorde l'accès au référentiel et attachez la politique au rôle. À des fins de test uniquement, choisissez la politique gérée par AWSCodeCommitPowerUserAWS. Cette politique accorde toutes les CodeCommit autorisations, à l'exception de la possibilité de supprimer des ressources. 3. Modifiez la politique de confiance du rôle afin que le compte B soit répertorié comme entité de confiance.	

Tâche	Description	Compétences requises
	Important Avant de transférer cette configuration dans votre environnement de production, il est recommandé de rédiger votre propre politique IAM qui applique les autorisations du moindre privilège. Pour plus d'informations, consultez la section Informations supplémentaires de ce modèle.	

Tâche	Description	Compétences requises
Accordez à l'instance du SageMaker bloc-notes l'autorisation d'assumer le rôle CodeCommit d'accès dans le compte A.	Dans le compte qui contient le rôle IAM de l'instance de SageMaker bloc-notes (compte B), procédez comme suit : 1. Créez une politique IAM qui permet à un rôle ou à un utilisateur IAM d'assumer le rôle d' CodeCommit accès dans le compte A. Exemple de politique d'autorisations IAM qui permet à un rôle ou à un utilisateur IAM d'assumer un rôle multicompte `{ "Version": "2012-10-17", "Statement": [ { "Sid": "VisualEditor0", "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam:::accountA_ID:role/accountArole_ID" } }` 2. Associez la politique au rôle de votre instance de	Informations générales sur AWS, AWS DevOps

Tâche	Description	Compétences requises
	SageMaker bloc-notes dans le compte B. 3. Faites en sorte que le rôle de l'instance du SageMaker bloc-notes dans le compte B assume le rôle CodeCommit d'accès dans le compte A. **Note** Pour consulter le nom de ressource Amazon (ARN) de votre dépôt, consultez Afficher les détails CodeCommit du référentiel dans le guide de CodeCommit l'utilisateur AWS.	

Configurez votre instance de SageMaker bloc-notes dans le compte B

Tâche	Description	Compétences requises
Configurez un profil utilisateur sur l'instance de SageMaker bloc-notes AWS pour assumer le rôle dans le compte A.	**Important** Assurez-vous que la dernière version de l'interface de ligne de commande AWS (AWS CLI) est installée.	Informations générales sur AWS, AWS DevOps

Tâche	Description	Compétences requises

	Dans le compte qui contient l'instance de SageMaker bloc-notes (compte B), procédez comme suit :
	
	1. Connectez-vous à AWS Management Console et ouvrez la console SageMaker .
	2. Accédez à votre instance de SageMaker bloc-notes. L'interface Jupyter s'ouvre.
	3. Choisissez Nouveau, puis Terminal. Une nouvelle fenêtre de terminal s'ouvre dans votre environnement Jupyter.
	4. Accédez au fichier ~/.aws/config de l'instance de SageMaker bloc-notes. Ajoutez ensuite un profil utilisateur au fichier en saisissant l'instruction suivante :
	
	`------.aws/config-------------`
	`[profile remoterepouser]`
	`role_arn = arn:aws:iam::<ID of Account A>:role/<rolename>`
	`role_session_name = remoteaccesssession`
	`region = eu-west-1`	

Tâche	Description	Compétences requises
	`credential_source = Ec2InstanceMetadata`	
Installez l' git-remote-codecommitutilitaire.	Suivez les instructions de l'étape 2 : Installation git-remote-codecommit dans le guide de CodeCommit l'utilisateur AWS.	Spécialiste des données

Accédez au référentiel

Tâche	Description	Compétences requises
Accédez au CodeCommit référentiel à l'aide des commandes Git ou SageMaker.	Pour utiliser Git Les principaux IAM qui assument le rôle de l'instance de SageMaker bloc-notes dans le compte B peuvent désormais exécuter des commandes Git pour accéder au CodeCommit référentiel du compte A. Par exemple, les utilisateurs peuvent exécuter des commandes telles que `git clone` `git pull`, et. `git push` Pour obtenir des instructions, consultez la section Se connecter à un CodeCommit référentiel AWS dans le guide	Git, console bash

Tâche	Description	Compétences requises
	de CodeCommit l'utilisateur AWS. Pour plus d'informations sur l'utilisation de Git avec CodeCommit, consultez Getting started with AWS CodeCommit dans le guide de CodeCommit l'utilisateur AWS. À utiliser SageMaker Pour utiliser Git depuis la SageMaker console, vous devez autoriser Git à récupérer les informati ons d'identification de votre CodeCommit dépôt. Pour obtenir des instructions, consultez la section Associer un CodeCommit référentiel d'un autre compte AWS à une instance de bloc-notes dans la SageMaker documentation.	

Ressources connexes

- Configurer l'accès entre comptes à un CodeCommit référentiel AWS à l'aide de rôles (CodeCommit documentation AWS)
- Tutoriel IAM : déléguer l'accès entre les comptes AWS à l'aide de rôles IAM (documentation IAM)

Informations supplémentaires

Restreindre CodeCommit les autorisations à des actions spécifiques

Pour limiter les actions qu'un principal IAM peut effectuer dans le CodeCommit référentiel, modifiez les actions autorisées dans la politique CodeCommit d'accès.

Pour plus d'informations sur les opérations CodeCommit d'API, consultez la référence CodeCommit des autorisations dans le guide de CodeCommit l'utilisateur AWS.

> **Note**
>
> Vous pouvez également modifier la politique gérée par AWSCodeCommitPowerUserAWS en fonction de votre cas d'utilisation.

Restreindre CodeCommit les autorisations à des référentiels spécifiques

Pour créer un environnement mutualisé dans lequel plusieurs référentiels de code ne sont accessibles qu'à des utilisateurs spécifiques, procédez comme suit :

1. Créez plusieurs rôles CodeCommit d'accès dans le compte A. Configurez ensuite la politique de confiance de chaque rôle d'accès pour permettre à des utilisateurs spécifiques du compte B d'assumer le rôle.
2. Limitez les référentiels de code que chaque rôle peut assumer en ajoutant une condition « Ressource » à la politique de chaque rôle CodeCommit d'accès.

Exemple de condition de « ressource » qui restreint l'accès d'un principal IAM à un référentiel spécifique CodeCommit

```
"Resource" : [<REPOSITORY_ARN>,<REPOSITORY_ARN> ]
```

> **Note**
>
> Pour aider à identifier et à différencier plusieurs référentiels de code dans le même compte AWS, vous pouvez attribuer différents préfixes aux noms des référentiels. Par exemple, vous pouvez nommer les référentiels de code avec des préfixes correspondant à différents groupes de développeurs, tels que myproject-subproject1-repo1 et myproject-subproject2-repo1. Vous pouvez ensuite créer un rôle IAM pour chaque groupe de développeurs en fonction des préfixes qui leur ont été attribués. Par exemple, vous pouvez créer un rôle

nommé myproject-subproject1-repoaccess et lui accorder l'accès à tous les référentiels de code qui incluent le préfixe myproject-subproject1.

Exemple de condition de « ressource » faisant référence à un ARN de référentiel de code qui inclut un préfixe spécifique

```
"Resource" : arn:aws:codecommit:<region>:<account-id>:myproject-subproject1-*
```

Mettre en œuvre une stratégie GitHub de branchement Flow pour les environnements multi-comptes DevOps

Créée par Mike Stephens (AWS) et Abhilash Vinod (AWS)

Récapitulatif

Lors de la gestion d'un référentiel de code source, différentes stratégies de branchement affectent les processus de développement et de publication des logiciels utilisés par les équipes de développement. Trunk, Flow et GitHub Gitflow sont des exemples de stratégies de branchement courantes. Ces stratégies utilisent différentes branches et les activités effectuées dans chaque environnement sont différentes. Organisations qui mettent en œuvre DevOps des processus bénéficieraient d'un guide visuel pour les aider à comprendre les différences entre ces stratégies de branchement. L'utilisation de ce visuel dans votre organisation aide les équipes de développement à aligner leur travail et à respecter les normes organisationnelles. Ce modèle fournit ce visuel et décrit le processus de mise en œuvre d'une stratégie de branchement GitHub Flow dans votre organisation.

Ce modèle fait partie d'une série de documentation sur le choix et la mise en œuvre de stratégies de DevOps succursales pour les organisations qui en ont plusieurs Comptes AWS. Cette série est conçue pour vous aider à appliquer la bonne stratégie et les meilleures pratiques dès le départ, afin de rationaliser votre expérience dans le cloud. GitHub Flow n'est qu'une des stratégies de branchement possibles que votre organisation peut utiliser. Cette série de documentation couvre également les modèles de branchement Trunk et Gitflow. Si ce n'est pas déjà fait, nous vous recommandons de consulter Choisir une stratégie de branchement Git pour les DevOps environnements multi-comptes avant de mettre en œuvre les instructions de ce modèle. Veuillez faire preuve de diligence raisonnable pour choisir la bonne stratégie de succursale pour votre organisation.

Ce guide fournit un schéma qui montre comment une organisation peut mettre en œuvre la stratégie GitHub Flow. Il est recommandé de consulter le guide AWS DevOps Well-Architected pour passer en revue les meilleures pratiques. Ce modèle inclut les tâches, les étapes et les restrictions recommandées pour chaque étape du DevOps processus.

Conditions préalables et limitations

Prérequis

- Git, installé. Il est utilisé comme outil de dépôt de code source.

- Draw.io, installé. Cette application permet de visualiser et de modifier le diagramme.

Architecture

Architecture cible

Le schéma suivant peut être utilisé comme un carré de Punnett (Wikipedia). Vous alignez les branches sur l'axe vertical avec les AWS environnements sur l'axe horizontal pour déterminer les actions à effectuer dans chaque scénario. Les chiffres indiquent la séquence des actions du flux de travail. Cet exemple vous emmène d'une `feature` succursale à un déploiement en production.

Pour plus d'informations sur les Comptes AWS environnements et les branches d'une approche GitHub Flow, consultez Choisir une stratégie de branchement Git pour les environnements multi-comptes DevOps .

Automatisation et mise à l'échelle

L'intégration continue et la livraison continue (les CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CD pipelines) fournissent également une gouvernance et des garanties aux équipes de développement en garantissant la cohérence, les normes, les meilleures pratiques et les niveaux d'acceptation minimaux pour l'acceptation et le déploiement des fonctionnalités. Pour plus d'informations, voir Pratiquer l'intégration continue et la livraison continue sur AWS.

AWS propose une suite de services de développement conçus pour vous aider à créer des pipelines CI/CD. Par exemple, AWS CodePipelineil s'agit d'un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. AWS CodeBuildcompile le code source, exécute des tests et produit des ready-to-deploy progiciels. Pour plus d'informations, consultez la section Outils de développement sur AWS.

Outils

AWS services et outils

AWS fournit une suite de services de développement que vous pouvez utiliser pour implémenter ce modèle :

- AWS CodeArtifactest un service de référentiel d'artefacts géré hautement évolutif qui vous permet de stocker et de partager des progiciels pour le développement d'applications.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeDeployautomatise les déploiements vers Amazon Elastic Compute Cloud EC2 (Amazon) ou vers des instances, des AWS Lambda fonctions ou des services Amazon Elastic Container Service (Amazon ECS) sur site.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.

Autres outils

- Draw.io Desktop est une application pour créer des organigrammes et des diagrammes. Le référentiel de code contient des modèles au format .drawio pour Draw.io.
- Figma est un outil de conception en ligne conçu pour la collaboration. Le référentiel de code contient des modèles au format .fig pour Figma.

Référentiel de code

Ce fichier source pour le diagramme de ce modèle est disponible dans le référentiel GitHub Git Branching Strategy for GitHub Flow. Il inclut des fichiers aux formats PNG, draw.io et Figma. Vous pouvez modifier ces diagrammes pour soutenir les processus de votre organisation.

Bonnes pratiques

Suivez les meilleures pratiques et recommandations décrites dans AWS DevOps Well-Architected Guidance et Choosing a Git Branching strategy pour les environnements multi-comptes. DevOps Ils vous aident à mettre en œuvre efficacement le développement GitHub basé sur Flow, à favoriser la collaboration, à améliorer la qualité du code et à rationaliser le processus de développement.

Épopées

Révision des GitHub flux de travail Flow

Tâche	Description	Compétences requises
Passez en revue le processus GitHub Flow standard.	1. Dans l'environnement sandbox, le développeur crée une `feature` branche à partir de cette `main` branche et utilise le modèle `feature/<ticket>_<initials>_<short description>` de dénomination. 2. Le développeur ajoute un ou plusieurs validations à la `feature` branche, chacune représentant une modification ou une amélioration discrète. 3. Le développeur ouvre une demande de fusion (MR) pour fusionner les modifications dans la `main` branche. Cela lance un processus de révision. 4. Au cours du processus de révision, les développeurs discutent des modifications apportées au code et fournissent des commentaires. L'objectif est de s'assurer que les modifications sont de haute qualité et	DevOps ingénieur

Tâche	Description	Compétences requises
	répondent aux normes du projet. 5. Une fois que le développeur a créé la demande de fusion, un processus de génération automatique démarre et déploie les modifications apportées à la `feature` branche dans l'environnement de développement. 6. Des tests automatisés vérifient l'intégrité et la qualité des modifications encapsulées dans la demande de fusion. Une compilation réussie, un déploiement réussi et des tests réussis sont nécessaires pour terminer la demande de fusion. 7. Lorsque le processus de révision est terminé, les modifications sont fusionnées dans la `main` branche. 8. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de test. 9. Un approbateur approuve manuellement le déploiement des artefacts de version	

Tâche	Description	Compétences requises
	dans l'environnement intermédiaire. 10. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de production.	

Tâche	Description	Compétences requises
Passez en revue le processus de correction de bogues GitHub Flow.	1. Le développeur crée une `bugfix` branche à partir de cette `main` branche et utilise le modèle de dénominationbugfix/<ticket number>_<developer initials>_<descriptor> . 2. Le développeur résout le problème, valide le correctif et crée la `bugfix` branche. 3. Le développeur ouvre une demande de fusion pour fusionner la `bugfix` branche dans la `main` branche. Cela lance un processus de révision. 4. Au cours du processus de révision, les développeurs discutent des modifications apportées au code et fournissent des commentaires. 5. Une fois l'examen terminé et approuvé, le développeur complète la demande de fusion de la `bugfix` succursale avec la `main` succursale. 6. Un approbateur approuve manuellement le déploiement des artefacts de version	DevOps ingénieur

Tâche	Description	Compétences requises
	dans des environnements supérieurs.	

Tâche	Description	Compétences requises
Passez en revue le processus du correctif GitHub Flow.	GitHub Flow est conçu pour permettre une diffusion continue, dans le cadre de laquelle les modifications de code sont déployées fréquemment et de manière fiable dans des environnements supérieurs. L'essentiel est que chaque `feature` branche puisse être déployée à tout moment. `Hotfix`les branches, qui sont apparentées à `feature` ou à `bugfix` des branches, peuvent suivre le même processus que l'une ou l'autre de ces branches. Cependant, étant donné leur urgence, les correctifs ont généralement une priorité plus élevée. En fonction des politiques de l'équipe et de l'urgence de la situation, certaines étapes du processus pourraient être accélérées. Par exemple, les révisions de code pour les correctifs peuvent être accélérées. Par conséquent, bien que le processus de correction soit parallèle au processus de correction des fonctionnalités ou des bogues, l'urgence des correctifs peut justifier des modifications de	DevOps ingénieur

Tâche	Description	Compétences requises
	la conformité procédurale. Il est essentiel d'établir des directives relatives à la gestion des correctifs afin de s'assurer qu'ils sont gérés de manière efficace et sécurisée.	

Résolution des problèmes

Problème	Solution
Conflits entre branches	Un problème courant qui peut survenir avec le modèle GitHub Flow est lorsqu'un correctif doit être appliqué en production`feature`, `bugfix` mais qu'une modification correspondante doit se produire dans une `hotfix` branche ou une branche où les mêmes ressources sont modifiées. Nous vous recommandons de fusionner fréquemment les modifications depuis `main` les branches inférieures afin d'éviter des conflits importants lors de la fusion avec`main`.
Maturité des équipes	GitHub Flow encourage les déploiements quotidiens vers des environnements supérieur s, en adoptant une véritable intégration continue et une livraison continue (CI/CD). Il est impératif que l'équipe possède la maturité technique nécessaire pour créer des fonctionn alités et créer des tests d'automatisation pour celles-ci. L'équipe doit effectuer un examen exhaustif des demandes de fusion avant que les modifications ne soient approuvées. Cela favorise une solide culture d'ingénierie qui

Problème	Solution
	favorise la qualité, la responsabilité et l'efficac ité du processus de développement.

Ressources connexes

Ce guide n'inclut pas de formation à Git ; toutefois, de nombreuses ressources de haute qualité sont disponibles sur Internet si vous avez besoin de cette formation. Nous vous recommandons de commencer par le site de documentation Git.

Les ressources suivantes peuvent vous aider dans votre parcours de branchement GitHub Flow dans le AWS Cloud.

AWS DevOps orientation

- AWS DevOps Orientations
- AWS Architecture de référence du pipeline de déploiement
- Qu'est-ce que c'est DevOps ?
- DevOps resources

GitHub Guidage du flux

- GitHub Tutoriel de démarrage rapide de Flow () GitHub
- Pourquoi GitHub Flow ?

Autres ressources

- Méthodologie d'application à douze facteurs (12factor.net)

Mettre en œuvre une stratégie de branchement Gitflow pour les environnements multi-comptes DevOps

Créée par Mike Stephens (AWS), Stephen DiCato (AWS), Tim Wondergem (AWS) et Abhilash Vinod (AWS)

Récapitulatif

Lors de la gestion d'un référentiel de code source, différentes stratégies de branchement affectent les processus de développement et de publication des logiciels utilisés par les équipes de développement. Trunk, Gitflow et Flow sont des exemples de stratégies de branchement courantes. GitHub Ces stratégies utilisent différentes branches et les activités effectuées dans chaque environnement sont différentes. Organisations qui mettent en œuvre DevOps des processus bénéficieraient d'un guide visuel pour les aider à comprendre les différences entre ces stratégies de branchement. L'utilisation de ce visuel dans votre organisation aide les équipes de développement à aligner leur travail et à respecter les normes organisationnelles. Ce modèle fournit ce visuel et décrit le processus de mise en œuvre d'une stratégie de branchement Gitflow dans votre organisation.

Ce modèle fait partie d'une série de documentation sur le choix et la mise en œuvre de stratégies de DevOps succursales pour les organisations qui en ont plusieurs Comptes AWS. Cette série est conçue pour vous aider à appliquer la bonne stratégie et les meilleures pratiques dès le départ, afin de rationaliser votre expérience dans le cloud. Gitflow n'est qu'une des stratégies de branchement possibles que votre organisation peut utiliser. Cette série de documentation couvre également les modèles de branchement Trunk et GitHub Flow. Si ce n'est pas déjà fait, nous vous recommandons de consulter Choisir une stratégie de branchement Git pour les DevOps environnements multi-comptes avant de mettre en œuvre les instructions de ce modèle. Veuillez faire preuve de diligence raisonnable pour choisir la bonne stratégie de succursale pour votre organisation.

Ce guide fournit un schéma qui montre comment une organisation peut mettre en œuvre la stratégie Gitflow. Il est recommandé de consulter le guide AWS DevOps Well-Architected pour connaître les meilleures pratiques. Ce modèle inclut les tâches, les étapes et les restrictions recommandées pour chaque étape du DevOps processus.

Conditions préalables et limitations

Prérequis

- Git, installé. Il est utilisé comme outil de dépôt de code source.
- Draw.io, installé. Cette application permet de visualiser et de modifier le diagramme.

- (Facultatif) Plugin Gitflow, installé.

Architecture

Architecture cible

Le schéma suivant peut être utilisé comme un carré de Punnett (Wikipedia). Vous alignez les branches sur l'axe vertical avec les AWS environnements sur l'axe horizontal pour déterminer les actions à effectuer dans chaque scénario. Les chiffres indiquent la séquence des actions du flux de travail. Cet exemple vous emmène d'une branche fonctionnelle au déploiement en production.

Pour plus d'informations sur les Comptes AWS environnements et les branches d'une approche Gitflow, consultez Choisir une stratégie de branchement Git pour les environnements DevOps multi-comptes.

Automatisation et mise à l'échelle

L'intégration continue et la livraison continue (les CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CD pipelines) fournissent également une gouvernance et des garanties aux équipes de développement en garantissant la cohérence, les normes, les meilleures pratiques et les niveaux d'acceptation minimaux pour l'acceptation et le déploiement des fonctionnalités. Pour plus d'informations, voir Pratiquer l'intégration continue et la livraison continue sur AWS.

AWS propose une suite de services de développement conçus pour vous aider à créer des pipelines CI/CD. Par exemple, AWS CodePipelineil s'agit d'un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. AWS CodeBuildcompile le code source, exécute des tests et produit des ready-to-deploy progiciels. Pour plus d'informations, consultez la section Outils de développement sur AWS.

Outils

AWS services et outils

AWS fournit une suite de services de développement que vous pouvez utiliser pour implémenter ce modèle :

- AWS CodeArtifactest un service de référentiel d'artefacts géré hautement évolutif qui vous permet de stocker et de partager des progiciels pour le développement d'applications.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeDeployautomatise les déploiements vers Amazon Elastic Compute Cloud EC2 (Amazon) ou vers des instances, des AWS Lambda fonctions ou des services Amazon Elastic Container Service (Amazon ECS) sur site.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.

Autres outils

- Draw.io Desktop est une application pour créer des organigrammes et des diagrammes. Le référentiel de code contient des modèles au format .drawio pour Draw.io.
- Figma est un outil de conception en ligne conçu pour la collaboration. Le référentiel de code contient des modèles au format .fig pour Figma.
- (Facultatif) Le plugin Gitflow est une collection d'extensions Git qui fournissent des opérations de dépôt de haut niveau pour le modèle de branchement Gitflow.

Référentiel de code

Ce fichier source pour le diagramme de ce modèle est disponible dans le GitFlow référentiel GitHub Git Branching Strategy for. Il inclut des fichiers aux formats PNG, draw.io et Figma. Vous pouvez modifier ces diagrammes pour soutenir les processus de votre organisation.

Bonnes pratiques

Suivez les meilleures pratiques et recommandations décrites dans AWS DevOps Well-Architected Guidance et Choosing a Git Branching strategy pour les environnements multi-comptes. DevOps Ils vous aident à mettre en œuvre efficacement le développement basé sur Gitflow, à favoriser la collaboration, à améliorer la qualité du code et à rationaliser le processus de développement.

Épopées

Révision des flux de travail Gitflow

Tâche	Description	Compétences requises
Passez en revue le processus standard de Gitflow.	1. Dans l'environnement sandbox, le développeur crée une `feature` branche à partir de cette `develop` branche et utilise le modèle `feature/<ticket>_<initials>_<short description>` de dénomination. 2. Le développeur développe le code et le déploie dans l'environnement sandbox de manière itérative afin de terminer le ticket. **Note** Le développeur peut éventuellement créer une `sandbox` branche pour exécuter un pipeline de génération ou de déploiement automatique dans l'environnement sandbox. 3. Le développeur crée une demande de fusion entre la `feature` branche et la	DevOps ingénieur

Tâche	Description	Compétences requises
	`develop` branche à l'aide d'une fusion par squash. 4. Un pipeline d'intégration et de livraison continues (CI/CD) crée et déploie automatiquement la `develop` branche dans l'environnement de développement. 5. (Facultatif) Un développeur intègre des `feature` branches supplémentaires dans la branche de développement avant de poursuivre les activités de publication. 6. Lorsque vous êtes prêt à publier les fonctionnalités de la `develop` branche, le développeur crée une `release` branche nommée `release/v<number>` à partir de la `develop` branche. 7. Le développeur crée la branche release, qui publie les artefacts à réutiliser dans d'autres environnements. 8. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de test.	

Tâche	Description	Compétences requises
	9. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement intermédiaire. 10. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de production. 11. Le développeur fusionne la `release` branche dans la `main` branche. Idéalement, le développeur utilise un script automatique pour effectuer une fusion rapide. N'utilisez pas de squash merge. 12. Le développeur fusionne la `release` branche dans la `develop` branche. Idéalement, le développeur utilise un script automatique pour effectuer une fusion rapide. N'utilisez pas de squash merge.	

Tâche	Description	Compétences requises
Passez en revue le processus Gitflow du correctif.	1. Le développeur crée une `hotfix` branche à partir de cette `main` branche et utilise le modèle de dénomination`hotfix/<ticket>_<initials>_<short description>` . 2. Le développeur crée une `release` branche à partir de cette `main` branche et lui donne un nom`release/v<number>` . 3. Le développeur résout le problème, valide le correctif et crée la `hotfix` branche. 4. Le développeur crée une demande de fusion entre la `hotfix` branche et la `release/v<number>` branche à l'aide d'une fusion par squash. 5. Le développeur crée la `release` branche, qui publie les artefacts à réutiliser dans d'autres environnements. 6. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de test.	DevOps ingénieur

Tâche	Description	Compétences requises
	7. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement intermédiaire. 8. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de production. 9. Le développeur fusionne la `release` branche dans la `main` branche. Idéalement, le développeur utilise un script automatique pour effectuer une fusion rapide. N'utilisez pas de squash merge. 10. Le développeur fusionne la `release` branche dans la `develop` branche. Idéalement, le développeur utilise un script automatique pour effectuer une fusion rapide. N'utilisez pas de squash merge. 11. Si un conflit est détecté, les développeurs reçoivent une alerte et résolvent le conflit par le biais d'une demande de fusion.	

Tâche	Description	Compétences requises
Passez en revue le processus de correction de bogues Gitflow.	1. Le développeur crée une `bugfix` branche à partir de la `release/v<number>` branche actuelle et utilise le modèle de dénominat ion`bugfix/<ticket number>_<developer initials>_<descriptor>` . 2. Le développeur résout le problème, valide le correctif et crée la `bugfix` branche. 3. Le développeur crée une demande de fusion entre la `bugfix` branche et la `release/v<number>` branche à l'aide d'une fusion par squash. 4. Le développeur crée la `release` branche, qui publie les artefacts à réutiliser dans d'autres environnements. 5. Un approbateur approuve manuellement le déploieme nt des artefacts de version dans l'environnement de test. 6. Un approbateur approuve manuellement le déploieme nt des artefacts de version dans l'environnement Stage.	DevOps ingénieur

Tâche	Description	Compétences requises
	7. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de production. 8. Le développeur fusionne la `release` branche dans la `main` branche. Idéalement, le développeur utilise un script automatique pour effectuer une fusion rapide. N'utilisez pas de squash merge. 9. Le développeur fusionne la `release` branche dans la `develop` branche. Idéalement, le développeur utilise un script automatique pour effectuer une fusion rapide. N'utilisez pas de squash merge. 10. Si un conflit est détecté, les développeurs reçoivent une alerte et résolvent le conflit par le biais d'une demande de fusion.	

Résolution des problèmes

Problème	Solution
Conflits entre branches	Un problème courant qui peut survenir avec le modèle Gitflow est celui où un correctif

Problème	Solution
	doit être apporté en production, mais une modification correspondante doit se produire dans un environnement inférieur, où une autre branche modifie les mêmes ressources. Nous vous recommandons de n'avoir qu'une seule branche de version active à la fois. Si plusieurs d'entre elles sont actives à la fois, les modificat ions apportées aux environnements peuvent se répercuter et vous risquez de ne pas être en mesure de faire passer une succursale en production.
Fusion	Les versions doivent être fusionnées dans la version principale et développées dès que possible afin de consolider le travail dans les branches principales.
Fusion de squash	N'utilisez une fusion par squash que lorsque vous fusionnez d'une `feature` branche à une autre`develop`. L'utilisation de fusions de courges dans les branches supérieures pose des difficultés lors de la fusion des modificat ions vers les branches inférieures.

Ressources connexes

Ce guide n'inclut pas de formation à Git ; toutefois, de nombreuses ressources de haute qualité sont disponibles sur Internet si vous avez besoin de cette formation. Nous vous recommandons de commencer par le site de documentation Git.

Les ressources suivantes peuvent vous aider dans votre parcours de création de succursales Gitflow dans le. AWS Cloud

AWS DevOps orientation

- AWS DevOps Orientations

- AWS Architecture de référence du pipeline de déploiement
- Qu'est-ce que c'est DevOps ?
- DevOps resources

Guidage Gitflow

- Le blog original de Gitflow (article de blog de Vincent Driessen)
- Flux de travail Gitflow (Atlassian)
- Gitflow on GitHub : Comment utiliser les flux de travail Git Flow avec GitHub Based Repos (YouTube vidéo)
- Exemple d'initialisation de Git Flow (YouTube vidéo)
- La branche de lancement de Gitflow du début à la fin (YouTube vidéo)

Autres ressources

Méthodologie d'application à douze facteurs (12factor.net)

Mettre en œuvre une stratégie de branchement de type Trunk pour les environnements multi-comptes DevOps

Créée par Mike Stephens (AWS) et Rayjan Wilson (AWS)

Récapitulatif

Lors de la gestion d'un référentiel de code source, différentes stratégies de branchement affectent les processus de développement et de publication des logiciels utilisés par les équipes de développement. Trunk, Flow et GitHub Gitflow sont des exemples de stratégies de branchement courantes. Ces stratégies utilisent différentes branches et les activités effectuées dans chaque environnement sont différentes. Organisations qui mettent en œuvre DevOps des processus bénéficieraient d'un guide visuel pour les aider à comprendre les différences entre ces stratégies de branchement. L'utilisation de ce visuel dans votre organisation aide les équipes de développement à aligner leur travail et à respecter les normes organisationnelles. Ce modèle fournit ce visuel et décrit le processus de mise en œuvre d'une stratégie de branchement Trunk dans votre organisation.

Ce modèle fait partie d'une série de documentation sur le choix et la mise en œuvre de stratégies de DevOps succursales pour les organisations qui en ont plusieurs Comptes AWS. Cette série est conçue pour vous aider à appliquer la bonne stratégie et les meilleures pratiques dès le départ, afin de rationaliser votre expérience dans le cloud. Trunk n'est qu'une des stratégies de branchement possibles que votre organisation peut utiliser. Cette série de documentation couvre également les modèles de branchement GitHub Flow et Gitflow. Si ce n'est pas déjà fait, nous vous recommandons de consulter Choisir une stratégie de branchement Git pour les DevOps environnements multi-comptes avant de mettre en œuvre les instructions de ce modèle. Veuillez faire preuve de diligence raisonnable pour choisir la bonne stratégie de succursale pour votre organisation.

Ce guide fournit un schéma qui montre comment une organisation peut mettre en œuvre la stratégie Trunk. Il est recommandé de consulter le guide officiel AWS DevOps Well-Architected pour connaître les meilleures pratiques. Ce modèle inclut les tâches, les étapes et les restrictions recommandées pour chaque étape du DevOps processus.

Conditions préalables et limitations

Prérequis

- Git, installé. Il est utilisé comme outil de dépôt de code source.
- Draw.io, installé. Cette application permet de visualiser et de modifier le diagramme.

Architecture

Architecture cible

Le schéma suivant peut être utilisé comme un carré de Punnett (Wikipedia). Vous alignez les branches sur l'axe vertical avec les AWS environnements sur l'axe horizontal pour déterminer les actions à effectuer dans chaque scénario. Les chiffres indiquent la séquence des actions du flux de travail. Cet exemple vous permet de passer d'une `feature` succursale à un déploiement en production.

Pour plus d'informations sur les Comptes AWS environnements et les branches d'une approche Trunk, consultez Choisir une stratégie de branchement Git pour les environnements multi-comptes DevOps .

Automatisation et mise à l'échelle

L'intégration continue et la livraison continue (les CI/CD) is the process of automating the software release lifecycle. It automates much or all of the manual processes traditionally required to get new code from an initial commit into production. A CI/CD pipeline encompasses the sandbox, development, testing, staging, and production environments. In each environment, the CI/CD pipeline provisions any infrastructure that is needed to deploy or test the code. By using CI/CD, development teams can make changes to code that are then automatically tested and deployed. CI/CD pipelines) fournissent également une gouvernance et des garanties aux équipes de développement en garantissant la cohérence, les normes, les meilleures pratiques et les niveaux d'acceptation minimaux pour l'acceptation et le déploiement des fonctionnalités. Pour plus d'informations, voir Pratiquer l'intégration continue et la livraison continue sur AWS.

AWS propose une suite de services de développement conçus pour vous aider à créer des pipelines CI/CD. Par exemple, AWS CodePipelineil s'agit d'un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. AWS CodeBuildcompile le code source, exécute des tests et produit des ready-to-deploy progiciels. Pour plus d'informations, consultez la section Outils de développement sur AWS.

Outils

AWS services et outils

AWS fournit une suite de services de développement que vous pouvez utiliser pour implémenter ce modèle :

- AWS CodeArtifactest un service de référentiel d'artefacts géré hautement évolutif qui vous permet de stocker et de partager des progiciels pour le développement d'applications.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeDeployautomatise les déploiements vers Amazon Elastic Compute Cloud EC2 (Amazon) ou vers des instances, des AWS Lambda fonctions ou des services Amazon Elastic Container Service (Amazon ECS) sur site.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.

Autres outils

- Draw.io Desktop — Une application pour créer des organigrammes et des diagrammes.
- Figma est un outil de conception en ligne conçu pour la collaboration. Le référentiel de code contient des modèles au format .fig pour Figma.

Référentiel de code

Ce fichier source pour le diagramme de ce modèle est disponible dans le référentiel GitHub Git Branching Strategy for Trunk. Il inclut des fichiers aux formats PNG, draw.io et Figma. Vous pouvez modifier ces diagrammes pour soutenir les processus de votre organisation.

Bonnes pratiques

Suivez les meilleures pratiques et recommandations décrites dans AWS DevOps Well-Architected Guidance et Choosing a Git Branching strategy pour les environnements multi-comptes. DevOps Ils vous aident à mettre en œuvre efficacement le développement basé sur Trunk, à favoriser la collaboration, à améliorer la qualité du code et à rationaliser le processus de développement.

Épopées

Révision du flux de travail Trunk

Tâche	Description	Compétences requises
Passez en revue le processus Trunk standard.	1. Dans l'environnement sandbox, le développeur crée une `feature` branche à partir de cette `main` branche et utilise le modèle `feature/<ticket>_<initials>_<short description>` de dénomination. 2. Le développeur développe le code et le déploie dans l'environnement sandbox de manière itérative afin de terminer le ticket. **Note** Le développeur peut éventuellement créer une `sandbox` branche pour exécuter un pipeline de génération ou de déploiement automatique dans l'environnement sandbox. 3. Le développeur crée une demande de fusion entre la `feature` branche et la	DevOps ingénieur

Tâche	Description	Compétences requises
	`main` branche à l'aide d'une fusion par squash. 4. Un pipeline d'intégration et de livraison continues (CI/CD) crée et publie automatiquement les artefacts de la `main` branche vers l'environnement de développement. 5. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de développement. 6. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de test. 7. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement intermédiaire. 8. Un approbateur approuve manuellement le déploiement des artefacts de version dans l'environnement de production.	

Résolution des problèmes

Problème	Solution
Conflits entre branches	Un problème courant qui peut survenir avec le modèle Trunk est lorsqu'un correctif doit être appliqué en production, mais qu'un changement correspondant doit se produire dans une `feature` succursale, où les mêmes ressources sont modifiées. Nous vous recommandons de fusionner fréquemment les modifications depuis `main` les branches inférieures afin d'éviter des conflits importants lors de la fusion vers`main`.

Ressources connexes

Ce guide n'inclut pas de formation à Git ; toutefois, de nombreuses ressources de haute qualité sont disponibles sur Internet si vous avez besoin de cette formation. Nous vous recommandons de commencer par le site de documentation Git.

Les ressources suivantes peuvent vous aider dans votre parcours de branchement Trunk dans le AWS Cloud.

AWS DevOps orientation

- AWS DevOps Orientations
- Architecture de référence des pipelines de déploiement d'AWS
- Qu'est-ce que c'est DevOps ?
- DevOps resources

Guidage du coffre

- Développement basé sur le tronc

Autres ressources

- Méthodologie d'application à douze facteurs (12factor.net)

Mettez en œuvre une analyse Checkov personnalisée et centralisée pour appliquer la politique avant de déployer AWS l'infrastructure

Créée par Benjamin Morris (AWS)

Récapitulatif

Ce modèle fournit un cadre d' GitHub actions pour écrire des politiques Checkov personnalisées dans un référentiel qui peut être réutilisé au sein d'une GitHub organisation. En suivant ce modèle, une équipe de sécurité de l'information peut rédiger, ajouter et gérer des politiques personnalisées en fonction des exigences de l'entreprise. Les politiques personnalisées peuvent être intégrées automatiquement à tous les pipelines de l' GitHub organisation. Cette approche peut être utilisée pour appliquer les normes de l'entreprise en matière de ressources avant que celles-ci ne soient déployées.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une GitHub organisation utilisant des GitHub actions
- AWS infrastructure déployée avec HashiCorp Terraform ou AWS CloudFormation

Limites

- Ce modèle est écrit pour GitHub Actions. Cependant, il peut être adapté à des cadres d'intégration continue et de livraison continue (CI/CD) similaires tels que. GitLab Aucune version payante spécifique de GitHub n'est requise.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité des régions, consultez la section Points de terminaison et quotas du service dans la AWS documentation, puis choisissez le lien correspondant au service.

Architecture

Ce modèle est conçu pour être déployé sous forme de GitHub référentiel contenant un flux de travail GitHub réutilisable et des politiques Checkov personnalisées. Le flux de travail réutilisable peut analyser à la fois Terraform et les référentiels CloudFormation d'infrastructure en tant que code (IaC).

Le schéma suivant montre le référentiel des GitHub flux de travail réutilisables et le référentiel des politiques Custom Checkov sous forme d'icônes distinctes. Toutefois, vous pouvez implémenter ces référentiels en tant que référentiels distincts ou en tant que référentiel unique. L'exemple de code utilise un référentiel unique, avec des fichiers pour les flux de travail (`.github/workflows`) et des fichiers pour les politiques personnalisées (`custom_policies`dossier et fichier de `.checkov.yml` configuration) dans le même référentiel.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur crée une pull request dans un GitHub référentiel.
2. Les flux de travail du pipeline commencent dans GitHub Actions, y compris une référence à un flux de travail réutilisable Checkov.
3. Le flux de travail de pipeline télécharge le flux de travail réutilisable Checkov référencé depuis un référentiel externe et exécute ce flux de travail de Checkov à l'aide GitHub d'Actions.
4. Le flux de travail réutilisable Checkov télécharge les politiques personnalisées à partir d'un référentiel externe.
5. Le flux de travail réutilisable Checkov évalue l'iAc du GitHub référentiel par rapport aux politiques Checkov intégrées et personnalisées. Le flux de travail réutilisable Checkov réussit ou échoue selon que des problèmes de sécurité sont détectés ou non.

Automatisation et évolutivité

Ce modèle permet une gestion centralisée de la configuration de Checkov, afin que les mises à jour des politiques puissent être appliquées en un seul endroit. Toutefois, ce modèle nécessite que chaque référentiel utilise un flux de travail contenant une référence au flux de travail réutilisable central. Vous pouvez ajouter cette référence manuellement ou utiliser des scripts pour transférer le fichier vers le `.github/workflows` dossier de chaque référentiel.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions. Checkov peut scanner CloudFormation.

Autres outils

- Checkov est un outil d'analyse de code statique qui vérifie les erreurs de configuration liées à la sécurité et à la conformité dans iAC.
- GitHub Actions est intégré à la GitHub plateforme pour vous aider à créer, partager et exécuter des flux de travail au sein de vos GitHub référentiels. Vous pouvez utiliser GitHub les actions pour automatiser des tâches telles que la création, le test et le déploiement de votre code.
- Terraform est un outil IaC HashiCorp qui vous aide à créer et à gérer des ressources sur site et dans le cloud. Checkov peut scanner Terraform.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub centralized-custom-checkov-sastréférentiel.

Bonnes pratiques

- Pour maintenir une posture de sécurité cohérente, alignez les politiques de sécurité de votre entreprise sur les politiques de Checkov.
- Au cours des premières phases de mise en œuvre des politiques personnalisées de Checkov, vous pouvez utiliser l'option soft-fail de votre scan Checkov pour autoriser la fusion des iAc présentant des problèmes de sécurité. Au fur et à mesure que le processus arrive à maturité, passez de l'option soft-fail à l'option hardfail.

Épopées

Créez un référentiel Checkov central pour les politiques personnalisées

Tâche	Description	Compétences requises
Créez un référentiel Checkov central.	Créez un référentiel pour stocker les politiques Checkov personnalisées qui seront utilisées au sein de l'organisation. Pour un démarrage rapide, vous pouvez copier le contenu	DevOps ingénieur

Tâche	Description	Compétences requises
	du référentiel de ce modèle dans votre GitHub centralized-custom-checkov-sast référentiel central Checkov.	
Créez un référentiel pour les flux de travail réutilisables.	Si un référentiel pour les flux de travail réutilisables existe déjà, ou si vous prévoyez d'inclure des fichiers de flux de travail réutilisables dans le même référentiel que les politiques Checkov personnalisées, vous pouvez ignorer cette étape. Créez un GitHub référentiel contenant les flux de travail réutilisables. Les pipelines d'autres référentiels référenceront ce référentiel.	DevOps ingénieur

Créez des flux de travail Checkov réutilisables et exemples

Tâche	Description	Compétences requises
Ajoutez un flux de travail Checkov réutilisable.	Créez un flux de travail d' GitHub actions Checkov réutilisable (fichier YAML) dans le référentiel de flux de travail réutilisables. Vous pouvez adapter ce flux de travail réutilisable à partir du fichier de flux de travail fourni dans ce modèle.	DevOps ingénieur

Tâche	Description	Compétences requises
	Un exemple de modification que vous pourriez vouloir apporter est de modifier le flux de travail réutilisable pour utiliser l'option soft-fail. Le réglage `soft-fail` sur `true` permet de terminer le travail avec succès même en cas d'échec du scan Checkov. Pour obtenir des instructions, consultez la section Défaillance matérielle et logicielle dans la documentation de Checkov.	
Ajoutez un exemple de flux de travail.	Ajoutez un exemple de flux de travail Checkov qui fait référence au `reusable` flux de travail. Cela fournira un modèle expliquant comment réutiliser le `reusable` flux de travail. Dans le référentiel d'exemples, `checkov-source.yaml` se trouve le flux de travail réutilisable et `checkov-scan.yaml` l'exemple qui consomme`checkov-source` . Pour plus de détails sur la rédaction d'un exemple de flux de travail Checkov, voir Informations supplémentaires.	DevOps ingénieur

Associer les politiques de l'entreprise aux politiques personnalisées de Checkov

Tâche	Description	Compétences requises
Déterminez les politiques qui peuvent être appliquées avec Checkov.	1. Passez en revue les politiques de l'entreprise liées à la sécurité de l'infrastructure et les exigences à mettre en place. 2. Déterminez les exigences qui peuvent être mises en œuvre à l'aide des politiques personnalisées de Checkov. 3. Créez une convention de dénomination qui associe le contrôle des politiques à la politique personnalisée de Checkov. Généralement, les politiques personnalisées de Checkov ont un identifiant avec un nom Checkov, la source de la politique (personnalisée) et un numéro de politique (par exemple,`CKV2_CUSTOM_123`). Pour plus de détails sur la création de politiques personnalisées Checkov, consultez la section Présentation des politiques personnalisées dans la documentation de Checkov.	Sécurité et conformité

Tâche	Description	Compétences requises
Ajoutez des politiques personnalisées de Checkov.	Convertissez les politique s d'entreprise identifiées en politiques Checkov personnal isées dans le référentiel central. Vous pouvez écrire des politiques Checkov simples en Python ou en YAML.	Sécurité

Mettre en œuvre des politiques personnalisées Checkov centralisées

Tâche	Description	Compétences requises
Ajoutez le flux de travail réutilisable Checkov à tous les référentiels.	À ce stade, vous devriez avoir un exemple de flux de travail Checkov qui fait référence au flux de travail réutilisa ble. Copiez l'exemple de flux de travail Checkov qui fait référence au flux de travail réutilisable dans chaque référentiel qui l'exige.	DevOps ingénieur
Créez un mécanisme pour garantir que Checkov s'exécute avant les fusions.	Pour garantir que le flux de travail Checkov est exécuté pour chaque pull request, créez une vérification de statut qui nécessite un flux de travail Checkov réussi avant de pouvoir fusionner les pull requests. GitHub vous permet d'exiger l'exécution de flux de travail spécifiques avant	DevOps ingénieur

Tâche	Description	Compétences requises
	de pouvoir fusionner les pull requests.	
Créez un PAT à l'échelle de l'organisation et partagez-le en tant que secret.	Si votre GitHub organisation est visible publiquement, vous pouvez ignorer cette étape. Ce modèle nécessite que le flux de travail Checkov soit en mesure de télécharger des politiques personnalisées à partir du référentiel de politiques personnalisées de votre GitHub organisation. Vous devez fournir des autorisations permettant au flux de travail Checkov d'accéder à ces référentiels. Pour ce faire, créez un jeton d'accès personnel (PAT) autorisé à lire les référentiels de l'organisation. Partagez ce PAT avec les référentiels, soit sous forme de secret à l'échelle de l'organisation (si vous utilisez un forfait payant), soit sous forme de secret dans chaque référentiel (version gratuite). Dans l'exemple de code, le nom par défaut du secret est`ORG_PAT`.	DevOps ingénieur

Tâche	Description	Compétences requises
(Facultatif) Protégez les fichiers du flux de travail Checkov contre toute modification.	Pour protéger les fichiers du flux de travail Checkov contre les modifications indésirables, vous pouvez utiliser un `CODEOWNERS` fichier. Le `CODEOWNERS` fichier est généralement déployé à la racine du répertoire. Par exemple, pour demander l'approbation du `secEng` groupe de votre GitHub organisation lorsque le `checkov-scan.yaml` fichier est modifié, ajoutez ce qui suit au `CODEOWNERS` fichier d'un référentiel : `[Checkov] .github/workflows /checkov-scan.yaml @myOrg/secEng` Un `CODEOWNERS` fichier est spécifique au référentiel dans lequel il se trouve. Pour protéger le flux de travail Checkov utilisé par le référentiel, vous devez ajouter (ou mettre à jour) un `CODEOWNERS` fichier dans chaque référentiel. Pour plus d'informations sur la protection des fichiers de flux de travail Checkov, voir	DevOps ingénieur

Tâche	Description	Compétences requises
	Informations supplémentaires. Pour plus d'informations sur `CODEOWNERS` les fichiers, consultez la documentation officielle de votre fournisseur de CI/CD (par exemple). GitHub	

Ressources connexes

- Présentation des politiques personnalisées de Checkov
- CloudFormation Analyse de configuration
- GitHub Actions > Workflows réutilisables

Informations supplémentaires

Écrire des fichiers de flux de travail Checkov

Lorsque vous écrivez`checkov-scan.yaml`, réfléchissez au moment où vous voulez qu'il s'exécute. La on clé de niveau supérieur détermine le moment où le flux de travail s'exécute. Dans le référentiel d'exemple, le flux de travail s'exécute lorsqu'une pull request cible la `main` branche (et chaque fois que la branche source de cette pull request est modifiée). Le flux de travail peut également être exécuté selon les besoins grâce à la `workflow_dispatch` clé.

Vous pouvez modifier les conditions de déclenchement du flux de travail en fonction de la fréquence à laquelle vous souhaitez que le flux de travail s'exécute. Par exemple, vous pouvez modifier le flux de travail pour qu'il s'exécute chaque fois que du code est envoyé vers une branche en le `pull_request` remplaçant par `push` et en supprimant la `branches` clé.

Vous pouvez modifier l'exemple de fichier de flux de travail que vous avez créé dans un référentiel individuel. Par exemple, vous pouvez modifier le nom de la branche cible de `main` à `production` si un référentiel est structuré autour d'une `production` branche.

Protection des fichiers de flux de travail Checkov

L'analyse Checkov fournit des informations utiles sur d'éventuelles erreurs de configuration de sécurité. Cependant, certains développeurs peuvent percevoir cela comme un obstacle à leur productivité et tenter de supprimer ou de désactiver le flux de numérisation.

Il existe plusieurs moyens de résoudre ce problème, notamment une meilleure communication sur la valeur à long terme de l'analyse de sécurité et une documentation plus claire sur le déploiement d'une infrastructure sécurisée. Il s'agit d'approches « souples » importantes en matière de DevSecOps collaboration qui peuvent être considérées comme la solution à la cause première de ce problème. Cependant, vous pouvez également utiliser des contrôles techniques tels qu'un `CODEOWNERS` fichier comme garde-fous pour aider les développeurs à rester sur la bonne voie.

Schéma de test dans un bac à sable

Pour tester ce modèle dans un environnement sandbox, procédez comme suit :

1. Créez une nouvelle GitHub organisation. Créez un jeton avec accès en lecture seule à tous les référentiels de l'organisation. Ce jeton étant destiné à un environnement sandbox et non à un environnement payant, vous ne pourrez pas le stocker dans un secret à l'échelle de l'organisation.
2. Créez un `checkov` référentiel pour contenir la configuration Checkov et un `github-workflows` référentiel pour contenir la configuration du flux de travail réutilisable. Remplissez les référentiels avec le contenu du référentiel d'exemple.
3. Créez un référentiel d'applications, puis copiez et collez le `checkov-scan.yaml` flux de travail `.github/workflows` dans son dossier. Ajoutez un secret au référentiel qui contient le PAT que vous avez créé pour l'accès en lecture seule de l'organisation. Le secret par défaut est`ORG_PAT`.
4. Créez une pull request qui ajoute du Terraform ou CloudFormation du code au référentiel d'applications. Checkov doit scanner et renvoyer un résultat.

Détectez automatiquement les modifications et lancez différents CodePipeline pipelines pour un monorepo dans CodeCommit

Créée par Helton Ribeiro (AWS), Petrus Batalha (AWS) et Ricardo Morais (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Remarque : n' AWS Cloud9 est plus disponible pour les nouveaux clients. Les clients existants de AWS Cloud9 peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle vous permet de détecter automatiquement les modifications apportées au code source d'une application monorepo, puis de lancer un pipeline AWS CodePipeline qui exécute l'intégration AWS CodeCommit et la livraison continues (CI/CD) automation for each microservice. This approach means that each microservice in your monorepo-based application can have a dedicated CI/CDpipeline), ce qui garantit une meilleure visibilité, un partage facilité du code et une collaboration, une standardisation et une découvrabilité améliorées.

La solution décrite dans ce modèle n'effectue aucune analyse de dépendance entre les microservices du monorepo. Il détecte uniquement les modifications du code source et lance le pipeline CI/CD correspondant.

Le modèle est utilisé AWS Cloud9 comme environnement de développement intégré (IDE) et AWS Cloud Development Kit (AWS CDK) pour définir une infrastructure en utilisant deux AWS CloudFormation piles : `MonoRepoStack` et`PipelinesStack`. La `MonoRepoStack` pile crée le monorepo dans AWS CodeCommit et la AWS Lambda fonction qui initie les pipelines CI/CD. La `PipelinesStack` pile définit l'infrastructure de votre pipeline.

> **Important**
>
> Le flux de travail de ce modèle est une preuve de concept (PoC). Nous vous recommandons de l'utiliser uniquement dans un environnement de test. Si vous souhaitez utiliser l'approche de ce modèle dans un environnement de production, consultez les meilleures pratiques de sécurité dans IAM dans la documentation AWS Identity and Access Management (IAM) et apportez les modifications requises à vos rôles IAM et. Services AWS

Conditions préalables et limitations

Prérequis

- Un AWS compte actif.
- AWS Command Line Interface (AWS CLI), installé et configuré. Pour plus d'informations, consultez la section Installation, mise à jour et désinstallation du AWS CLI dans la AWS CLI documentation.
- Python 3 et`pip`, installé sur votre machine locale. Pour plus d'informations, consultez la documentation Python.
- AWS CDK, installé et configuré. Pour plus d'informations, consultez la section Mise en route avec le AWS CDK dans la AWS CDK documentation.
- Un AWS Cloud9 IDE, installé et configuré. Pour plus d'informations, consultez la section Configuration AWS Cloud9 dans la AWS Cloud9 documentation.
- Le référentiel de déclencheurs multi-pipelines GitHub AWS CodeCommit monorepo, cloné sur votre machine locale.
- Répertoire existant contenant le code d'application que vous souhaitez utiliser pour créer et déployer CodePipeline.
- Connaissance et expérience des DevOps meilleures pratiques en matière de AWS Cloud. Pour vous familiariser davantage DevOps, vous pouvez utiliser le modèle Créez une architecture faiblement couplée avec des microservices en utilisant des DevOps pratiques et AWS Cloud9 sur le site Web du guide AWS prescriptif.

Architecture

Le schéma suivant montre comment utiliser le AWS CDK pour définir une infrastructure à deux AWS CloudFormation piles : `MonoRepoStack` et`PipelinesStack`.

Le schéma suivant illustre le flux de travail suivant :

1. Le processus bootstrap utilise le AWS CDK pour créer les AWS CloudFormation piles et`MonoRepoStack`. `PipelinesStack`
2. La `MonoRepoStack` pile crée le CodeCommit référentiel pour votre application et la fonction `monorepo-event-handler` Lambda qui est lancée après chaque validation.
3. La `PipelinesStack` pile crée les pipelines CodePipeline initiés par la fonction Lambda. Chaque microservice doit disposer d'un pipeline d'infrastructure défini.

4. Le pipeline pour `microservice-n` est initié par la fonction Lambda et démarre ses étapes CI/CD isolées basées sur le code source dans. CodeCommit
5. Le pipeline pour `microservice-1` est initié par la fonction Lambda et démarre ses étapes CI/CD isolées basées sur le code source dans. CodeCommit

Le schéma suivant montre le déploiement des AWS CloudFormation stacks `MonoRepoStack` et `PipelinesStack` dans un compte.

1. Un utilisateur modifie le code dans l'un des microservices de l'application.
2. L'utilisateur transfère les modifications d'un dépôt local vers un CodeCommit dépôt.
3. L'activité push lance la fonction Lambda qui reçoit tous les push vers le référentiel. CodeCommit
4. La fonction Lambda lit un paramètre dans Parameter Store, une fonctionnalité de AWS Systems Manager, pour récupérer l'ID de validation le plus récent. Le paramètre a le format de dénomination :`/MonoRepoTrigger/{repository}/{branch_name}/LastCommit`. Si le paramètre n'est pas trouvé, la fonction Lambda lit le dernier ID de validation dans le CodeCommit référentiel et enregistre la valeur renvoyée dans Parameter Store.
5. Après avoir identifié l'ID de validation et les fichiers modifiés, la fonction Lambda identifie les pipelines pour chaque répertoire de microservices et lance le pipeline requis. CodePipeline

Outils

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel permettant de définir l'infrastructure cloud dans le code et de la provisionner via AWS CloudFormation ce dernier.
- Python est un langage de programmation qui vous permet de travailler rapidement et d'intégrer des systèmes plus efficacement.

Code

Le code source et les modèles de ce modèle sont disponibles dans le référentiel de déclencheurs multi-pipelines GitHub AWS CodeCommit monorepo.

Bonnes pratiques

- Cet exemple d'architecture n'inclut pas de solution de surveillance pour l'infrastructure déployée. Si vous souhaitez déployer cette solution dans un environnement de production, nous vous recommandons d'activer la surveillance. Pour plus d'informations, consultez la section Surveiller vos applications sans serveur avec CloudWatch Application Insights dans la documentation AWS Serverless Application Model (AWS SAM).
- Lorsque vous modifiez l'exemple de code fourni par ce modèle, suivez les meilleures pratiques de développement et de déploiement de l'infrastructure cloud décrites dans la AWS CDK documentation.
- Lorsque vous définissez vos pipelines de microservices, consultez les meilleures pratiques de sécurité décrites dans la AWS CodePipeline documentation.
- Vous pouvez également vérifier les meilleures pratiques de votre AWS CDK code à l'aide de l'utilitaire cdk-nag. Cet outil utilise un ensemble de règles, regroupées par packs, pour évaluer votre code. Les packs disponibles sont les suivants :
  - AWS Bibliothèque de solutions
  - Sécurité de la Health Insurance Portability and Accountability Act (HIPAA)
  - Institut national des normes et de la technologie (NIST) 800-53 rev 4
  - NIST 800-53 version 5
  - Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) 3.2.1

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Créez un environnement Python virtuel.	Dans votre AWS Cloud9 IDE, créez un environnement Python virtuel et installez les dépendances requises en exécutant la commande suivante : `make install`	Developer

Tâche	Description	Compétences requises
Bootstrap le Compte AWS et Région AWS pour le. AWS CDK	Démarrez le fichier requis Compte AWS et la région en exécutant la commande suivante : `make bootstrap account-id=<your-AWS-account-ID> region=<required-region>`	Developer

Ajouter un nouveau pipeline pour un microservice

Tâche	Description	Compétences requises
Ajoutez votre exemple de code dans le répertoire de votre application.	Ajoutez le répertoire contenant votre exemple de code d'application au `monorepo-sample` répertoire du référentiel de déclencheurs GitHub AWS CodeCommit monorepo multi-pipelines clonés.	Developer
Modifiez le fichier `monorepo-main.json` .	Ajoutez le nom du répertoire du code de votre application et le nom du pipeline au `monorepo-main.json` fichier du référentiel cloné.	Developer
Créez le pipeline.	Dans le `Pipelines` répertoire du référentiel, ajoutez le pipeline `class` de votre application. Le répertoire contient deux	Developer

Tâche	Description	Compétences requises
	exemples de fichiers, `pipeline_hotsite.py` et `pipeline_demo.py`. Chaque fichier comporte trois étapes : source, génération et déploiement. Vous pouvez copier l'un des fichiers et y apporter des modifications conformément aux exigences de votre application.	

Tâche	Description	Compétences requises

Modifiez le fichier `monorepo_config.py` .	Dans`service_map` , ajoutez le nom du répertoire de votre application et la classe que vous avez créée pour le pipeline.
	
	Par exemple, le code suivant montre une définition de pipeline dans le `Pipelines` répertoire qui utilise un fichier nommé `pipeline_mysample.py` avec une `MySamplePipeline` classe :
	
	`...`
	`# Pipeline definition imports`
	`from pipelines.pipeline_demo import DemoPipeline`
	`from pipelines.pipeline_hotsite import HotsitePipeline`
	`from pipelines.pipeline_mysample import MySampleP ipeline`
	
	`### Add your pipeline configuration here`
	`service_map: Dict[str, ServicePipeline] = {`
	`# folder-name -> pipeline-class`
	`'demo': DemoPipel ine(),`
	`'hotsite': HotsitePipeline(),`
		Developer

Tâche	Description	Compétences requises
	`'mysample': MySamplePipeline() }`	

Déployez la MonoRepoStack pile

Tâche	Description	Compétences requises
Déployez la AWS CloudFormation pile.	Déployez la AWS CloudFormation `MonoRepoStack` pile avec les valeurs de paramètres par défaut dans le répertoire racine du référentiel cloné en exécutant la `make deploy-core` commande. Vous pouvez modifier le nom du dépôt en exécutant la `make deploy-core monorepo-name=<repo_name>` commande. **Note** Vous pouvez déployer les deux pipelines simultanément à l'aide de la `make deploy monorepo-name=<repo_name>` commande.	Developer
Validez le CodeCommit référentiel.	Vérifiez que vos ressources ont été créées en exécutant	Developer

Tâche	Description	Compétences requises
	la `aws codecommit get-repository --repository-name <repo_name>` commande. **Important** Comme la AWS CloudFormation pile crée le CodeCommit dépôt dans lequel le monorepo est stocké, n'exécutez pas la `cdk destroy MonoRepoStack` commande si vous avez commencé à y apporter des modifications.	
Validez les résultats de la AWS CloudFormation pile.	Vérifiez que la AWS CloudFormation `MonoRepoStack` pile est correctement créée et configurée en exécutant la commande suivante : `aws cloudformation list-stacks --stack-status-filter CREATE_COMPLETE --query 'StackSummaries[?StackName == 'MonoRepoStack']'`	Developer

Déployez la PipelinesStack pile

Tâche	Description	Compétences requises
Déployez la AWS CloudFormation pile.	La AWS CloudFormation `PipelinesStack` pile doit être déployée après le déploiement de la `MonoRepoStack` pile. La taille de la pile augmente lorsque de nouveaux microservices sont ajoutés à la base de code du monorepo et est redéployée lorsqu'un nouveau microservice est intégré. Déployez la PipelinesStack pile en exécutant la `make deploy-pipelines` commande. **Note** Vous pouvez également déployer simultanément les deux pipelines en exécutant la `make deploy monorepo-name=<repo_name>` commande. L'exemple de sortie suivant montre comment le `PipelinesStacks`	Developer

Tâche	Description	Compétences requises
	déploiement imprime URLs les microservices à la fin de l'implémentation : `Outputs: PipelinesStack.dem ourl = .cloudfront.net PipelinesStack.hotsi teurl = .cloudfro nt.net`	
Validez les résultats de la AWS CloudFormation pile.	Vérifiez que la AWS CloudFormation `Pipelines Stacks` pile est correctem ent créée et configurée en exécutant la commande suivante : `aws cloudformation list-stacks --stack-s tatus-filter CREATE_CO MPLETE UPDATE_COMPLETE --query 'StackSum maries[?StackName == 'PipelinesStack']'`	Developer

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez vos AWS CloudFormation piles.	Exécutez la commande `make destroy`.	Developer
Supprimez les compartiments S3 de vos pipelines.	1. Connectez-vous à la console Amazon Simple Storage Service (Amazon	Developer

Tâche	Description	Compétences requises
	S3) AWS Management Consoleet ouvrez-la. 2. Supprimez les compartiments S3 associés à vos pipelines et utilisez le nom suivant : `pipelines stack-codepipeline *`	

Résolution des problèmes

Problème	Solution
J'ai rencontré AWS CDK des problèmes.	Consultez la section Résolution AWS CDK des problèmes courants dans la documentation AWS CDK.
J'ai envoyé mon code de microservice, mais le pipeline de microservices n'a pas fonctionné.	Validation de configuration Vérifiez la configuration de la branche : • Assurez-vous de transférer votre code vers la bonne branche. Ce pipeline est configuré pour s'exécuter uniquement lorsque des modifications sont apportées à la `main` branche. Les push vers d'autres branches n'initient pas le pipeline à moins qu'ils ne soient spécifiquement configurés. • Après avoir envoyé votre code, vérifiez si le commit est visible AWS CodeCommit pour vous assurer que le push a réussi et que la connexion entre votre environnement local et le référentiel est intacte. Actualisez vos informations d'identification en cas de problème lors de la transmission du code.

Problème	Solution
	Validez les fichiers de configuration : • Vérifiez que la `service_map` variable in reflète `monorepo_config.py` correctem ent la structure de répertoire actuelle de vos microservices. Cette variable joue un rôle crucial dans le mappage de votre code push sur le pipeline correspondant. • Assurez-vous qu'il `monorepo-main.json` est mis à jour pour inclure le nouveau mappage de votre microservice. Ce fichier est essentiel pour que le pipeline reconnais se et gère correctement les modifications apportées à votre microservice. Résolution des problèmes sur la console AWS CodePipeline chèques : • Sur le AWS Management Console, confirmez que vous vous trouvez bien dans l' Région AWS endroit où votre pipeline est hébergé. Ouvrez la CodePipeline console et vérifiez si le pipeline correspondant à votre microserv ice a été lancé. Analyse des erreurs : si le pipeline a été lancé mais a échoué, consultez les messages d'erreur ou les journaux fournis CodePipeline pour comprendre ce qui s'est mal passé. AWS Lambda résolution des problèmes : • Sur la AWS Lambda console, ouvrez la fonction `monorepo-event-handler`

Problème	Solution
	Lambda. Vérifiez que la fonction a été lancée en réponse au code push. Analyse des journaux : examinez les journaux de la fonction Lambda pour détecter tout problème. Les journaux peuvent fournir des informations détaillées sur ce qui s'est passé lors de l'exécution de la fonction et aider à déterminer si la fonction a traité l'événement comme prévu.

Problème	Solution
Je dois redéployer tous mes microservices.	Il existe deux approches pour forcer le redéploiement de tous les microservices. Choisissez l'option qui correspond à vos besoins. Approche 1 : supprimer un paramètre dans Parameter Store Cette méthode implique la suppression d'un paramètre spécifique dans le magasin de paramètres de Systems Manager qui suit le dernier ID de validation utilisé pour le déploiement. Lorsque vous supprimez ce paramètre, le système est obligé de redéploye r tous les microservices lors du prochain déclencheur, car il le perçoit comme un nouvel état. Étapes : 1. Localisez l'entrée du magasin de paramètre s spécifique qui contient l'ID de validation ou un marqueur de déploiement associé pour votre monorepo. Le nom du paramètre suit le format suivant : `"/MonoRepoTrigger/{repository}/{branch_name}/LastCommit"` 2. Envisagez de sauvegarder la valeur du paramètre si elle est critique ou si vous souhaitez conserver un enregistrement de l'état du déploiement avant de le réinitialiser. 3. Utilisez AWS Management Console le AWS CLI ou SDKs pour supprimer le paramètre identifié. Cette action réinitialise le marqueur de déploiement.

Problème	Solution
	4. Après la suppression, le prochain push vers le référentiel devrait amener le système à déployer tous les microservices, car il recherche le dernier commit à prendre en compte pour le déploiement. Avantages : • Simple et rapide à mettre en œuvre avec un minimum d'étapes. • Il n'est pas nécessaire d'apporter des modifications arbitraires au code pour lancer les déploiements. Inconvénients : • Contrôle moins précis du processus de déploiement. • Potentiellement risqué si le magasin de paramètres est utilisé pour gérer d'autres configurations critiques. Approche 2 : envoyer un commit dans chaque sous-dossier monorepo Cette méthode consiste à apporter une modification mineure et à l'insérer dans chaque sous-dossier de microservice du monorepo pour initier leurs pipelines individuels. Étapes : 1. Répertoriez tous les microservices du monorepo qui doivent être redéployés.

Problème	Solution
	2. Pour chaque microservice, apportez une modification minimale et sans impact dans son sous-dossier. Il peut s'agir de la mise à jour d'un `README` fichier, de l'ajout d'un commentaire dans un fichier de configuration ou de toute modification n'affectant pas les fonctionnalités du service. 3. Apportez ces modifications à l'aide d'un message clair (tel que « Initiez le redéploie ment des microservices ») et transférez-les vers le référentiel. Assurez-vous d'appliqu er les modifications à la branche qui lance le déploiement. 4. Surveillez les pipelines de chaque microserv ice afin de vous assurer qu'ils sont lancés et qu'ils se terminent correctement. Avantages : • Fournit un contrôle granulaire sur les microservices qui sont redéployés. • Plus sûr car cela n'implique pas de supprimer les paramètres de configuration qui pourraien t être utilisés à d'autres fins. Inconvénients : • Cela prend plus de temps, en particulier avec un grand nombre de microservices. • Nécessite d'apporter des modifications de code inutiles susceptibles d'encombrer l'historique des validations.

Ressources connexes

- Intégration et livraison continues (CI/CD) à l'aide de CDK Pipelines (documentation)AWS CDK
- module aws-cdk/pipelines (référence d'API)AWS CDK

Intégrer un référentiel Bitbucket à AWS Amplify à l'aide d'AWS CloudFormation

Créée par Alwin Abraham (AWS)

Récapitulatif

AWS Amplify vous aide à déployer et à tester rapidement des sites Web statiques sans avoir à configurer l'infrastructure généralement requise. Vous pouvez déployer l'approche de ce modèle si votre entreprise souhaite utiliser Bitbucket pour le contrôle de source, que ce soit pour migrer le code d'application existant ou créer une nouvelle application. En utilisant AWS CloudFormation pour configurer automatiquement Amplify, vous offrez une visibilité sur les configurations que vous utilisez.

Ce modèle décrit comment créer un pipeline et un environnement de déploiement continus (CI/CD) frontaux en utilisant AWS CloudFormation pour intégrer un référentiel Bitbucket à AWS Amplify. L'approche du modèle signifie que vous pouvez créer un pipeline frontal Amplify pour des déploiements répétables.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- Un compte Bitbucket actif avec accès administrateur
- Accès à un terminal utilisant cURL ou l'application Postman
- Connaissance d'Amplify
- Connaissance d'AWS CloudFormation
- Connaissance des fichiers au format YAML

Architecture

Pile technologique

- Amplify
- AWS CloudFormation
- Bitbucket

Outils

- AWS Amplify — Amplify aide les développeurs à développer et à déployer des applications mobiles et Web basées sur le cloud.
- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos ressources AWS afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications exécutées dans AWS.
- Bitbucket — Bitbucket est une solution de gestion de référentiels Git conçue pour les équipes professionnelles. Il vous offre un emplacement central pour gérer les référentiels Git, collaborer sur votre code source et vous guider tout au long du processus de développement.

Code

Le `bitbucket-amplify.yml` fichier (joint) contient le CloudFormation modèle AWS pour ce modèle.

Épopées

Configuration du référentiel Bitbucket

Tâche	Description	Compétences requises
(Facultatif) Créez un dépôt Bitbucket.	1. Connectez-vous à votre compte Bitbucket et créez un nouveau dépôt. Pour plus d'informations à ce sujet, consultez la section Création d'un dépôt Git dans la documentation de Bitbucket. 2. Enregistrez le nom de l'espace de travail.	DevOps ingénieur

Tâche	Description	Compétences requises
	Note Vous pouvez également utiliser un dépôt Bitbucket existant.	
Ouvrez les paramètres de l'espace de travail.	1. Ouvrez l'espace de travail et choisissez l'onglet Référentiel. 2. Choisissez le référentiel que vous souhaitez intégrer à Amplify. 3. Choisissez le nom de l'espace de travail situé au-dessus du nom du référentiel. 4. Dans la barre latérale, choisissez Réglages.	DevOps ingénieur

Tâche	Description	Compétences requises
Créez un OAuth consommateur.	1. Dans la section Applications et fonctionnalités, sélectionnez OAuth consommateurs, puis sélectionnez Ajouter un consommateur. 2. Entrez le nom de votre consommateur, par exemple,`Amplify Integration .` 3. Entrez une URL de rappel. Bien que ce champ soit une entrée obligatoire, il n'est pas utilisé pour terminer l'intégration. La valeur peut donc être `http://localhost:3000` 4. Cochez la case Ceci est un consommateur privé. 5. Choisissez les autorisations suivantes : • Projet — `Read` • Référentiels — `Admin` • Pull requests — `Read` • Webhooks — et `Read Write` 6. Conservez les choix par défaut pour tous les autres champs et choisissez Soumettre. 7. Enregistrez la clé et le secret générés.	DevOps ingénieur

Tâche	Description	Compétences requises
Obtenez un jeton OAuth d'accès.	1. Ouvrez une fenêtre de terminal et exécutez la commande suivante : `curl -X POST -u "KEY:SECRET" https://bitbucket.org/site/oauth2/access_token -d grant_type=client_credentials` **Important** Remplacez `KEY` et `SECRET` par la clé et le secret que vous avez enregistrés précédemment. 2. Enregistrez le jeton d'accès sans utiliser les guillemets. Le jeton n'est valide que pour une durée limitée et la durée par défaut est de deux heures. Vous devez exécuter le CloudFormation modèle AWS dans ce délai.	DevOps ingénieur

Création et déploiement de la CloudFormation pile AWS

Tâche	Description	Compétences requises
Téléchargez le CloudFormation modèle AWS.	Téléchargez le CloudFormation modèle `bitbucket-amplify.yml` AWS (ci-joint). Ce modèle crée le pipeline CI/CD dans Amplify, en plus du projet et de la branche Amplify.	
Créez et déployez la CloudFormation pile AWS.	1. Connectez-vous à la console de gestion AWS de la région AWS dans laquelle vous souhaitez déployer et ouvrez la CloudFormation console AWS. 2. Choisissez Create Stack (avec de nouvelles ressources), puis choisissez Upload a Template File. 3. Chargez le fichier `bitbucket-amplify.yml` . 4. Choisissez Next, entrez un nom de pile, puis entrez les paramètres suivants : • Jeton d'accès : collez le jeton OAuth d'accès que vous avez créé précédemment. • URL du dépôt : ajoutez l'URL du dépôt du projet Bitbucket. L'URL est	DevOps ingénieur

Tâche	Description	Compétences requises
	généralement au format suivant : `https://bitbucket.org/<WORKSPACE_NAME>/<REPO_NAME>` • Nom de branche : il doit correspondre au nom d'une branche de votre dépôt Bitbucket. Cette branche n'a pas besoin d'exister lorsque vous exécutez la CloudFormation pile AWS, mais elle est nécessaire pour déployer du code dans l'environnement. • Nom du projet : il s'agit du nom à associer au projet Amplify. 5. Choisissez Next, puis Create Stack.	

Testez le pipeline CI/CD

Tâche	Description	Compétences requises
Déployez le code dans la branche de votre référentiel.	1. Clonez votre dépôt Bitbucket en exécutant la commande suivante : `git clone https://bitbucket.org/<WORK`	Développeur d’applications

Tâche	Description	Compétences requises
	SPACE_NAME>/<REPO_NAME> 2. Vérifiez le nom de branche utilisé lors de l'exécution du CloudFormation script AWS. Pour créer et extraire une nouvelle branche, exécutez la `git checkout -b <BRANCH_NAME>` commande. Pour récupérer une branche existante, exécutez la `git checkout <BRANCH_NAME>` commande 3. Validez le code dans la branche et envoyez-le vers la branche distante en exécutant les `git push` commandes `git commit` and. 4. Amplify construit et déploie ensuite l'application. Pour plus d'informations à ce sujet, consultez les commandes Git de base dans la documentation de Bitbucket.	

Ressources connexes

Méthodes d'authentification (documentation Atlassian)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Lancez un CodeBuild projet sur des comptes AWS à l'aide de Step Functions et d'une fonction proxy Lambda

Créée par Richard Milner-Watts (AWS) et Amit Anjarlekar (AWS)

Récapitulatif

Ce modèle montre comment lancer un CodeBuild projet AWS de manière asynchrone sur plusieurs comptes AWS à l'aide d'AWS Step Functions et d'une fonction de proxy AWS Lambda. Vous pouvez utiliser l'exemple de machine à états Step Functions du modèle pour tester le succès de votre CodeBuild projet.

CodeBuild vous aide à lancer des tâches opérationnelles à l'aide de l'interface de ligne de commande AWS (AWS CLI) à partir d'un environnement d'exécution entièrement géré. Vous pouvez modifier le comportement de votre CodeBuild projet au moment de l'exécution en remplaçant les variables d'environnement. En outre, vous pouvez l'utiliser CodeBuild pour gérer les flux de travail. Pour plus d'informations, consultez Service Catalog Tools sur le site Web d'AWS Workshop et Schedule jobs in Amazon RDS for PostgreSQL using AWS et EventBridge Amazon sur le blog de base de données CodeBuild AWS.

Conditions préalables et limitations

Prérequis

- Deux comptes AWS actifs : un compte source pour appeler une fonction proxy Lambda avec Step Functions et un compte cible pour créer un CodeBuild exemple de projet à distance

Limites

- Ce modèle ne peut pas être utilisé pour copier des artefacts entre comptes.

Architecture

Le schéma suivant montre l'architecture créée par ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. La machine d'état Step Functions analyse la carte d'entrée fournie et invoque la fonction proxy Lambda (`codebuild-proxy-lambda`) pour chaque compte, région et projet que vous avez définis.
2. La fonction de proxy Lambda utilise AWS Security Token Service (AWS STS) pour assumer un rôle de proxy IAM (`codebuild-proxy-role`), qui est associé à une politique IAM (`codebuild-proxy-policy`) dans le compte cible.
3. À l'aide du rôle assumé, la fonction Lambda lance le CodeBuild projet et renvoie l'ID de CodeBuild tâche. La machine à états Step Functions boucle et interroge la CodeBuild tâche jusqu'à ce qu'elle reçoive un statut de réussite ou d'échec.

La logique de la machine à états est illustrée dans l'image suivante.

Pile technologique

- AWS CloudFormation
- CodeBuild
- IAM
- Lambda
- Step Functions
- X-Ray

Outils

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS CloudFormation Designer fournit un éditeur JSON et YAML intégré qui vous permet de visualiser et de modifier des CloudFormation modèles.
- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire

et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise.
- AWS X-Ray vous aide à collecter des données sur les demandes traitées par votre application et fournit des outils que vous pouvez utiliser pour visualiser, filtrer et obtenir des informations sur ces données afin d'identifier les problèmes et les opportunités d'optimisation.

Code

L'exemple de code pour ce modèle est disponible dans le référentiel GitHub Cross Account CodeBuild Proxy. Ce modèle utilise la bibliothèque AWS Lambda Powertools for Python pour fournir des fonctionnalités de journalisation et de suivi. Pour plus d'informations sur cette bibliothèque et ses utilitaires, consultez Powertools for AWS Lambda (Python).

Bonnes pratiques

1. Ajustez les valeurs du temps d'attente dans la machine d'état Step Function afin de minimiser les demandes d'interrogation concernant le statut du travail. Utilisez le temps d'exécution prévu pour le CodeBuild projet.
2. Ajustez la `MaxConcurrency` propriété de la carte dans Step Functions pour contrôler le nombre de CodeBuild projets pouvant être exécutés en parallèle.
3. Si nécessaire, consultez l'exemple de code pour connaître l'état de préparation à la production. Déterminez quelles données peuvent être enregistrées par la solution et déterminez si le CloudWatch chiffrement Amazon par défaut est suffisant.

Épopées

Créez la fonction de proxy Lambda et le rôle IAM associé dans le compte source

Tâche	Description	Compétences requises
Enregistrez le compte AWS IDs.	Un compte AWS IDs est requis pour configurer l'accès entre les comptes.	AWS DevOps

Tâche	Description	Compétences requises
	Enregistrez l'ID de compte AWS pour vos comptes source et cible. Pour plus d'informations, consultez la section Trouver votre identifiant de compte AWS dans la documentation IAM.	
Téléchargez les CloudFormation modèles AWS.	1. Téléchargez le CloudFormation modèle `sample_target_codebuild_template.yaml` AWS depuis le GitHub référentiel correspondant à ce modèle. 2. Téléchargez le CloudFormation modèle `codebuild_lambda_proxy_template.yaml` AWS depuis le GitHub référentiel correspondant à ce modèle. **Note** Dans les CloudFormation modèles AWS, `<SourceAccountId>` il s'agit de l'ID de compte AWS du compte source et `<TargetAccountId>` de l'ID de compte AWS du compte cible.	AWS DevOps

Tâche	Description	Compétences requises
Créez et déployez la CloudFormation pile AWS.	1. Connectez-vous à l'AWS Management Console pour votre compte source, ouvrez la CloudFormation console AWS, puis choisissez Stacks. 2. Choisissez Créer une pile, puis choisissez Avec de nouvelles ressources (standard). 3. Pour Source du modèle, choisissez Charger un fichier de modèle. 4. Pour Télécharger un fichier modèle, choisissez fichier, puis sélectionnez le `codebuild_lambda_proxy_template.yaml` fichier que vous avez téléchargé. Choisissez Suivant. 5. Dans Nom de la pile, entrez le nom de la pile (par exemple,`codebuild-lambda-proxy`). 6. **Note** Remplacez le `crossAccountTargetRoleArn` paramètre par votre `<TargetAc`	AWS DevOps

Tâche	Description	Compétences requises
	countId> (par exemple,<arn:aws:iam::123456789012:role/proxy-lambda-codebuild-role>). : vous n'êtes pas obligé de mettre à jour la valeur par défaut du **targetCodeBuildProject** paramètre. 7. Choisissez Next, acceptez les options de création de pile par défaut, puis choisissez Next. 8. Cochez la case Je reconnais qu'AWS CloudFormation pourrait créer des ressources IAM avec des noms personnalisés, puis choisissez Create stack. **Note** Vous devez créer la CloudFormation pile AWS pour la fonction proxy Lambda avant de créer des	

Tâche	Description	Compétences requises
	ressources dans des comptes cibles. Lorsque vous créez une politique de confiance dans un compte cible, le rôle IAM est traduit du nom du rôle en identifiant interne. C'est pourquoi le rôle IAM doit déjà exister.	
Confirmez la création de la fonction proxy et de la machine à états.	1. Attendez que la CloudFormation pile AWS atteigne le statut CREATE_COMPLETE. Cela devrait prendre moins d'une minute. 2. Ouvrez la console AWS Lambda, choisissez Functions, puis recherchez la `lambda-proxy-ProxyLambda-<GUID>` fonction. 3. Ouvrez la console AWS Step Functions, choisissez State Machines, puis recherchez la machine `sample-crossaccount-codebuild-state-machine` State Machine.	AWS DevOps

Créez un rôle IAM dans le compte cible et lancez un exemple CodeBuild de projet

Tâche	Description	Compétences requises
Créez et déployez la CloudFormation pile AWS.	1. Connectez-vous à l'AWS Management Console pour votre compte cible, ouvrez la CloudFormation console AWS, puis choisissez Stacks. 2. Choisissez Create Stack, puis choisissez Avec de nouvelles ressources (standard). 3. Pour Source du modèle, choisissez Charger un fichier de modèle. 4. Pour Télécharger un fichier modèle, choisissez Choisir un fichier, puis sélectionnez le `sample_target_codebuild_template.yaml` fichier. Choisissez Suivant. 5. Dans Nom de la pile, entrez le nom de la pile (par exemple :`sample-codebuild-stack`). 6. Remplacez le `crossAccountSourceRoleArn` paramètre par votre `<SourceAccountId>` (par exemple,`<arn:aws:iam::123456789012:role/codebuild-proxy-lambda-role>`).	AWS DevOps

Tâche	Description	Compétences requises
	7. Choisissez Next, acceptez les options de création de pile par défaut, puis choisissez Next. 8. Cochez la case Je reconnais qu'AWS CloudFormation pourrait créer des ressources IAM avec des noms personnal isés, puis choisissez Create stack.	
Vérifiez la création de l'exemple de CodeBuild projet.	1. Attendez que la CloudForm ation pile AWS atteigne le statut CREATE_CO MPLETE. Cela devrait prendre moins d'une minute. 2. Ouvrez la CodeBuild console AWS, puis recherchez le `sample-codebuild-project` projet.	AWS DevOps

Testez la fonction de proxy Lambda entre comptes

Tâche	Description	Compétences requises
Lancez la machine à états.	1. Connectez-vous à l'AWS Management Console pour votre compte source, ouvrez la console AWS Step Functions, puis choisissez State machines.	AWS DevOps

Tâche	Description	Compétences requises
	2. Choisissez la machine à `sample-crossaccount-codebuild-state-machine` états, puis choisissez Démarrer l'exécution. 3. Dans l'éditeur d'entrée, entrez le code JSON suivant et `<TargetAccountID>` remplacez-le par l'ID de compte AWS du compte contenant le CodeBuild projet. `{ "crossAccountTargetRoleArns": [ { "arn": "arn:aws:iam::<TargetAccountID>:role/proxy-lambda-codebuild-role", "region": "eu-west-1", "codeBuildProject": "sample-codebuild-project", "SampleValue1": "Value1", "SampleValue2": "Value2" } ] }`	

Tâche	Description	Compétences requises
	Note Les paires clé-valeur sont transmises en tant que variables d'environnement de la fonction du compte source au CodeBuild projet du compte cible. 4. Choisissez Start execution (Démarrer l'exécution). 5. Dans l'onglet Détails de la page State Machine, vérifiez si le statut d'exécution est défini sur Successed. Cela confirme que votre machine d'état est en cours d'exécution. Remarque : Cela peut prendre environ 30 secondes pour que la machine à états atteigne le statut Successed. 6. Pour voir la sortie et l'entrée d'une étape dans la machine à états, développez cette étape dans la section Historique des événements d'exécution. Par exemple, développez l'étape Lambda - CodeBuild Proxy — Start. La sortie inclut des détails sur les	

Tâche	Description	Compétences requises
	variables d'environnement remplacées, la charge utile d'origine et l' CodeBuild ID de tâche.	
Validez les variables d'environnement.	1. Connectez-vous à l'AWS Management Console pour votre compte cible. 2. Ouvrez la CodeBuild console AWS, développez Build, puis choisissez Build projects. 3. Choisissez le `sample-codebuild-project` projet, puis cliquez sur Afficher les détails. 4. Dans l'onglet Historique des constructions, choisissez la version la plus récente du projet, puis choisissez Afficher les journaux. 5. Dans la sortie du journal, vérifiez que les variables d'environnement imprimées sur STDOUT correspondent aux variables d'environnement de l'exemple de machine d'état Step Functions.	AWS DevOps

Résolution des problèmes

Problème	Solution
L'exécution de Step Functions prend plus de temps que prévu.	Ajustez les `MaxConcurrency` propriétés de la carte dans la machine d'état Step Function pour contrôler le nombre de CodeBuild projets pouvant être exécutés en parallèle.
L'exécution des CodeBuild travaux prend plus de temps que prévu.	1. Ajustez les valeurs du temps d'attente dans la machine d'état Step Functions afin de minimiser le nombre de demandes d'interrogation concernant le statut du travail. Utilisez le temps d'exécution prévu pour le CodeBuild projet. 2. Déterminez si CodeBuild c'est l'outil approprié à utiliser. Par exemple, le temps nécessaire pour initialiser une CodeBuild tâche peut être nettement plus long que celui d'AWS Lambda. Si un débit élevé et des délais d'exécution rapides sont nécessaires, envisagez de migrer la logique métier vers AWS Lambda et d'utiliser une architecture ventilée.

Gérez le basculement multi-AZ pour les clusters EMR à l'aide d'Application Recovery Controller

Créée par Aarti Rajput (AWS), Ashish Bhatt (AWS), Neeti Mishra (AWS) et Nidhi Sharma (AWS)

Récapitulatif

Ce modèle propose une stratégie de reprise après sinistre efficace pour les charges de travail Amazon EMR afin de garantir la haute disponibilité et la cohérence des données entre plusieurs zones de disponibilité au sein d'une même zone. Région AWS La conception utilise Amazon Application Recovery Controller et un Application Load Balancer pour gérer les opérations de basculement et la distribution du trafic pour un cluster EMR basé sur Apache Spark.

Dans des conditions standard, la zone de disponibilité principale héberge un cluster EMR actif et une application avec des fonctionnalités de lecture/écriture complètes. En cas de défaillance inattendue d'une zone de disponibilité, le trafic est automatiquement redirigé vers la zone de disponibilité secondaire, où un nouveau cluster EMR est lancé. Les deux zones de disponibilité accèdent à un bucket Amazon Simple Storage Service (Amazon S3) partagé via des points de terminaison de passerelle dédiés, ce qui garantit une gestion cohérente des données. Cette approche minimise les temps d'arrêt et permet une restauration rapide des charges de travail critiques liées au Big Data en cas de défaillance de la zone de disponibilité. La solution est utile dans des secteurs tels que la finance ou le commerce de détail, où les analyses en temps réel sont cruciales.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Amazon EMR sur Amazon Elastic Compute Cloud (Amazon) EC2
- Accès depuis le nœud principal du cluster EMR à Amazon S3.
- AWS Infrastructure multi-AZ

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Versions du produit

- Amazon EMR 6.x et versions ultérieures

Architecture

Pile technologique cible

- Cluster Amazon EMR
- Contrôleur Amazon Application Recovery
- Application Load Balancer
- Compartiment Amazon S3
- Points de terminaison de passerelle pour Amazon S3

Architecture cible

Cette architecture assure la résilience des applications en utilisant plusieurs zones de disponibilité et en mettant en œuvre un mécanisme de restauration automatique via l'Application Recovery Controller.

1. L'Application Load Balancer achemine le trafic vers l'environnement Amazon EMR actif, qui est généralement le cluster EMR principal de la zone de disponibilité principale.
2. Le cluster EMR actif traite les demandes d'application et se connecte à Amazon S3 via son point de terminaison dédié à la passerelle Amazon S3 pour les opérations de lecture et d'écriture.
3. Amazon S3 sert de référentiel de données central et est potentiellement utilisé comme point de contrôle ou comme stockage partagé entre des clusters EMR. Les clusters EMR préservent la cohérence des données lorsqu'ils écrivent directement sur Amazon S3 via le `s3://` protocole et le système de fichiers EMR (EMRFS).
4. Application Recovery Controller surveille en permanence l'état de santé de la zone de disponibilité principale et gère automatiquement les opérations de basculement lorsque cela est nécessaire.
5. Si l'Application Recovery Controller détecte une défaillance dans le cluster EMR principal, il prend les mesures suivantes :
   - Lance le processus de basculement vers le cluster EMR secondaire dans la zone de disponibilité 2.
   - Met à jour les configurations de routage pour diriger le trafic vers le cluster secondaire.

Outils

Services AWS

- Amazon Application Recovery Controller vous aide à gérer et à coordonner la restauration de vos applications dans toutes Régions AWS les zones de disponibilité. Ce service simplifie le processus et améliore la fiabilité de la restauration des applications en réduisant les étapes manuelles requises par les outils et processus traditionnels.
- Application Load Balancer fonctionne au niveau de la couche application, qui est la septième couche du modèle d'interconnexion des systèmes ouverts (OSI). Il répartit le trafic applicatif entrant sur plusieurs cibles, telles que EC2 les instances, dans plusieurs zones de disponibilité. La disponibilité de votre application s'en trouve accrue.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- Amazon EMR est une plateforme de mégadonnées qui fournit le traitement des données, l'analyse interactive et l'apprentissage automatique pour les frameworks open source tels qu'Apache Spark, Apache Hive et Presto.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon S3 fournit une interface de service Web simple que vous pouvez utiliser pour stocker et récupérer n'importe quel volume de données, à tout moment et en tout lieu. Grâce à ce service, vous pouvez facilement créer des applications qui utilisent le stockage cloud natif.
- Les points de terminaison de passerelle pour Amazon S3 sont des passerelles que vous spécifiez dans votre table de routage pour accéder à Amazon S3 depuis votre cloud privé virtuel (VPC) via le réseau. AWS

Bonnes pratiques

- Suivez les AWS meilleures pratiques en matière de sécurité, d'identité et de conformité afin de garantir une architecture robuste et sécurisée.
- Alignez l'architecture avec le AWS Well-Architected Framework.
- Utilisez Amazon S3 Access Grants pour gérer l'accès à Amazon S3 depuis votre cluster EMR basé sur Spark. Pour plus de détails, consultez le billet de blog Use Amazon EMR with S3 Access Grants to Spark Access to Amazon S3.
- Améliorez les performances de Spark avec Amazon S3.

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises
Connectez-vous au AWS Management Console.	Connectez-vous au en AWS Management Consoletant qu'utilisateur IAM. Pour obtenir des instructions, consultez la AWS documentation.	AWS DevOps
Configurez le AWS CLI.	Installez le AWS CLI ou mettez-le à jour vers la dernière version afin de pouvoir interagir avec Services AWS le AWS Managemen t Console. Pour obtenir des instructions, consultez la AWS CLI documentation.	AWS DevOps

Déployez une application Spark sur votre cluster EMR

Tâche	Description	Compétences requises
Créez un compartiment S3.	1. Créez un compartiment S3 pour stocker le jeu de données en entrée, les journaux, les applications et les données de sortie. Pour obtenir des instructions, consultez la documentation Amazon S3. 2. Organisez le compartim ent dans des dossiers distincts pour les données d'entrée (`dataset`), les	AWS DevOps

Tâche	Description	Compétences requises
	journaux (`logs`), l'application Spark (`spark-app `) et les données de sortie (`output`).	

Tâche	Description	Compétences requises

Créez un cluster EMR.	1. Utilisez les AWS CLI commandes suivantes pour créer un cluster EMR (par exemple, version 6.12 ou ultérieure) avec des instances réparties sur deux zones de disponibilité (telles que `us-east-1a` et `us-east-1b`) pour une haute disponibilité. La commande indique le type d'`m4.large` instance à titre d'exemple.
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-1> \ --release-label emr-6.12.0 \ --instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large`
	
	`aws emr create-cluster \ --ec2-attributes AvailabilityZone=<AZ-name-2> \ --release-label emr-6.12.0 \`
		AWS DevOps

Tâche	Description	Compétences requises
	`--instance-groups InstanceGroupType=MASTER,InstanceCount=1,InstanceType=m4.large InstanceGroupType=CORE,InstanceCount=2,InstanceType=m4.large` Pour plus d'informations, consultez la commande create-cluster et la documentation Amazon EMR. 2. Fournissez à la paire de clés, au rôle de service et au profil d'instance les autorisations requises, le cas échéant.	

Tâche	Description	Compétences requises
Configurez les paramètres de sécurité pour le cluster EMR.	1. Identifiez le groupe de sécurité associé au nœud principal du cluster EMR à l'aide de la commande AWS CLI describe-cluster : `aws emr describe-cluster --cluster-id j-XXXXXXXX` 2. Pour améliorer la sécurité, modifiez les paramètres du groupe de sécurité pour autoriser l'accès SSH (port TCP 22) au nœud principal , mais limitez-le à votre adresse IP spécifique. Pour plus d'informations, consultez la documentation Amazon EMR.	AWS DevOps

Tâche	Description	Compétences requises

Connectez-vous au cluster EMR.	Connectez-vous au nœud principal du cluster EMR via SSH à l'aide de la paire de clés fournie.
	
	Assurez-vous que le fichier de paires de clés se trouve dans le même répertoire que votre application.
	
	Exécutez les commandes suivantes pour définir les autorisations correctes pour la paire de clés et établir la connexion SSH :
	
	`chmod 400 <key-pair-name>`
	`ssh -i ./<key-pair-name> hadoop@<master-node-public-dns>`
		AWS DevOps

Tâche	Description	Compétences requises

Déployez l'application Spark.	Après avoir établi la connexion SSH, vous serez dans la console Hadoop.
	
	1. Créez ou modifiez le fichier d'application Spark (`main.py`) à l'aide d'un éditeur de texte tel que vim :
	
	`vim main.py`
	
	Pour plus d'informations sur la création et la modification de l'application Spark, consultez la documentation Amazon EMR.
	2. Soumettez l'application Spark au cluster EMR, en spécifiant les emplacements des données d'entrée et de sortie dans le compartiment S3 :
	
	`spark-submit main.py –data_source <input-data-folder-in-s3> –output_uri <output-folder-in-s3>`
	
	Voici un exemple basé sur les dossiers que vous avez configurés précédemment :
		AWS DevOps

Tâche	Description	Compétences requises

	`spark-submit main.py –data_source dataset –output_uri output`
	3. Surveillez la progression de l'application en consultant les journaux de l'application :
	`yarn logs -applicationId <application-id>`	

Surveillez l'application Spark.	1. Ouvrez une autre fenêtre de terminal et établissez un tunnel SSH vers l'interface utilisateur Web du gestionnaire de ressources du cluster EMR : `ssh -i <key-pair-name> -N -L 8157:<resource-manager-public-dns>:8088 hadoop@<resource-manager-public-dns>` 2. Pour surveiller l'application, accédez à l'interface utilisateur Web du gestionnaire de ressources en accédant `http://localhost:8157` à votre navigateur Web.	AWS DevOps

Transférer le trafic vers une autre zone de disponibilité

Tâche	Description	Compétences requises
Créez un Application Load Balancer.	Configurez le groupe cible qui achemine le trafic entre les nœuds principaux Amazon EMR déployés dans deux zones de disponibilité au sein d'un. Région AWS Pour obtenir des instructions, consultez la section Création d'un groupe cible pour votre Application Load Balancer dans la documentation d'Elastic Load Balancing.	AWS DevOps
Configurez le décalage zonal dans Application Recovery Controller.	Au cours de cette étape, vous allez utiliser la fonction de changement de zone d'Application Recovery Controller pour transférer le trafic vers une autre zone de disponibilité. 1. Ouvrez la console Application Recovery Controller. 2. Sous Mise en route, choisissez Déplacement de zone, puis Démarrer le décalage de zone. 3. Sélectionnez la zone de disponibilité à partir de laquelle vous souhaitez déplacer le trafic. 4. Sélectionnez une ressource prise en charge (par	AWS DevOps

Tâche	Description	Compétences requises
	exemple, Application Load Balancer) pour le décalage de zone dans le tableau Resources. 5. Pour Définir l'expiration du décalage de zone, choisissez ou entrez une date d'expiration pour le décalage de zone. Vous pouvez définir une durée comprise entre 1 minute et trois jours (72 heures). Tous les changements de zone sont temporaires. Vous devez définir une date d'expiration, mais vous pouvez mettre à jour les équipes actives ultérieur ement pour définir une nouvelle période d'expirat ion pouvant aller jusqu'à trois jours. 6. Entrez un commentaire à propos de ce changement de zone. 7. Cochez la case pour confirmer que le lancement d'un changement de zone réduira la capacité disponibl e pour votre application en déplaçant le trafic hors de la zone de disponibilité. 8. Sélectionnez Démarrer.	

Tâche	Description	Compétences requises
	Pour utiliser le AWS CLI, consultez les exemples d'utilisation du AWS CLI avec décalage de zone dans la documentation d'Application Recovery Controller.	

Tâche	Description	Compétences requises

Vérifiez la configuration et la progression du changement de zone.	1. Vérifiez les ressources enregistrées avec Zonal Shift :
	`aws arc-zonal-shift list-managed-resources --region <AWS-region-name>`
	Par exemple, le résultat suivant confirme que les ressources sont opérationnelles dans les deux zones de disponibilité.
	`"appliedWeights": { "use1-az1": 1.0, "use1-az2": 1.0 },`
	2. Pour visualiser le décalage de zone, utilisez la AWS CLI commande suivante pour démarrer le décalage de zone :
	`aws arc-zonal-shift start-zonal-shift \ --resource-identifier <application-load-balancer-arn> \ --away-from <source-AZ> \ --expires-in 10m --comment "testing" \`
		AWS DevOps

Tâche	Description	Compétences requises

	<pre>--region <AWS-regi
	on-name></pre>
	où se <source-AZ> trouve l'identifiant de la zone de disponibilité dont vous souhaitez éloigner le trafic et <application-load-balancer-arn> l'Amazon Resource Name (ARN) de votre Application Load Balancer.
	3. Vérifiez que le trafic s'est déplacé vers une autre zone de disponibilité.
	<pre>aws arc-zonal-shift
	get-managed-resour
	ce \
	--resource-identif
	ier <application-
	load-balancer-arn> \
	--region <AWS-regi
	on-name></pre>
	Vous pouvez voir le décalage zonal confirmé par ces pondérations :
	<pre>"appliedWeights": {
	"use1-az1":
	0.0,
	"use1-az2":
	1.0
	},</pre>	

Ressources connexes

- AWS CLI commandes :
  - create-cluster
  - décrive-cluster
  - arc-zonal-shift
- Configuration des types d'instances de cluster Amazon EMR et meilleures pratiques pour les instances Spot (documentation Amazon EMR)
- Bonnes pratiques de sécurité dans l'IAM (documentation IAM)
- Utiliser des profils d'instance (documentation IAM)
- Utiliser le décalage de zone et le décalage automatique de zone pour restaurer les applications dans ARC (documentation Application Recovery Controller)

Gérez les déploiements bleu/vert de microservices vers plusieurs comptes et régions à l'aide des services de code AWS et des clés multirégionales AWS KMS

Créée par Balaji Vedagiri (AWS), Ashish Kumar (AWS), Faisal Shahdad (AWS), Anand Krishna Varanasi (AWS), Vanitha Dontireddy (AWS) et Vivek Thangamuthu (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle décrit comment déployer une application de microservices globale à partir d'un compte AWS central vers plusieurs comptes de charge de travail et régions conformément à une stratégie de déploiement bleu/vert. Le modèle prend en charge les éléments suivants :

- Les logiciels sont développés dans un compte central, tandis que les charges de travail et les applications sont réparties sur plusieurs comptes et régions AWS.
- Une seule clé multirégionale du système de gestion des clés AWS (AWS KMS) est utilisée pour le chiffrement et le déchiffrement afin de couvrir la reprise après sinistre.
- La clé KMS est spécifique à une région et doit être maintenue ou créée dans trois régions différentes pour les artefacts du pipeline. Une clé multirégionale KMS permet de conserver le même identifiant de clé dans toutes les régions.
- Le modèle de branchement du flux de travail Git est implémenté avec deux branches (development et main) et le code est fusionné à l'aide de pull requests (PRs). La fonction AWS Lambda déployée à partir de cette pile crée un PR entre la branche de développement et la branche principale. La fusion des relations publiques avec la succursale principale lance un CodePipeline pipeline AWS, qui orchestre le flux d'intégration continue et de livraison continue (CI/CD) et déploie les stacks sur tous les comptes.

Ce modèle fournit un exemple de configuration d'infrastructure sous forme de code (IaC) via AWS CloudFormation Stacks pour illustrer ce cas d'utilisation. Le déploiement bleu/vert de microservices est mis en œuvre à l'aide d'AWS. CodeDeploy

Conditions préalables et limitations

Prérequis

- Quatre comptes AWS actifs :
  - Un compte d'outils pour gérer le pipeline de code et maintenir le CodeCommit référentiel AWS.
  - Trois comptes de charge de travail (test) pour déployer la charge de travail des microservices.
- Ce modèle utilise les régions suivantes. Si vous souhaitez utiliser d'autres régions, vous devez apporter les modifications appropriées aux piles multirégionales AWS CodeDeploy et AWS KMS.
  - Compte Tools (AWS CodeCommit) : `ap-south-1`
  - Compte de charge de travail (test) 1 : `ap-south-1`
  - Compte de charge de travail (test) 2 : `eu-central-1`
  - Compte de charge de travail (test) 3 : `us-east-1`
- Trois compartiments Amazon Simple Storage Service (Amazon S3) pour les régions de déploiement de chaque compte de charge de travail. (Ils sont appelés`S3BUCKETNAMETESTACCOUNT1`, `S3BUCKETNAMETESTACCOUNT2` et `S3BUCKETNAMETESTACCOUNT3` plus tard dans ce modèle.)

  Par exemple, vous pouvez créer ces compartiments dans des comptes et des régions spécifiques avec des noms de compartiments uniques comme suit (remplacez xxxx par un nombre aléatoire) :

```
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-xxxx-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-xxxx-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-xxxx-us-east-1 --region us-east-1

#Example
##In Test Account 1
aws s3 mb s3://ecs-codepipeline-18903-ap-south-1 --region ap-south-1
##In Test Account 2
aws s3 mb s3://ecs-codepipeline-18903-eu-central-1 --region eu-central-1
##In Test Account 3
aws s3 mb s3://ecs-codepipeline-18903-us-east-1 --region us-east-1
```

Limites

Le modèle utilise AWS CodeBuild et d'autres fichiers de configuration pour déployer un exemple de microservice. Si vous avez un autre type de charge de travail (par exemple, sans serveur), vous devez mettre à jour toutes les configurations pertinentes.

Architecture

Pile technologique cible

- AWS CloudFormation
- AWS CodeCommit
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline

Architecture cible

Automatisation et mise à l'échelle

La configuration est automatisée à l'aide de modèles de CloudFormation pile AWS (iAc). Il peut être facilement adapté à plusieurs environnements et comptes.

Outils

Services AWS

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS CodeDeploy automatise les déploiements vers Amazon Elastic Compute Cloud EC2 (Amazon) ou des instances sur site, les fonctions AWS Lambda ou les services Amazon Elastic Container Service (Amazon ECS).
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.

- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Outils supplémentaires

- Git est un système de contrôle de version distribué open source qui fonctionne avec le CodeCommit référentiel AWS.
- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs. Ce modèle utilise Docker pour créer et tester des images de conteneurs localement.
- cfn-lint et cfn-nag sont des outils open source qui vous aident à examiner les CloudFormation piles pour détecter d'éventuelles erreurs ou problèmes de sécurité.

Référentiel de code

Le code de ce modèle est disponible dans les déploiements GitHub mondiaux bleu/vert dans plusieurs régions et dans le référentiel de comptes.

Épopées

Configuration des variables d'environnement

Tâche	Description	Compétences requises
Exportez les variables d'environnement pour le déploiement de la CloudFormation pile.	Définissez les variables d'environnement qui seront utilisées comme entrée dans les CloudFormation piles ultérieurement dans ce modèle. 1. Mettez à jour les noms de bucket que vous avez créés	AWS DevOps

Tâche	Description	Compétences requises

	dans les trois comptes et régions, comme expliqué précédemment dans la section Conditions préalables :
	
	`export S3BUCKETNAMETESTACCOUNT1=<S3BUCKETACCOUNT1>`
	`export S3BUCKETNAMETESTACCOUNT2=<S3BUCKETACCOUNT2>`
	`export S3BUCKETNAMETESTACCOUNT3=<S3BUCKETACCOUNT3>`
	
	2. Définissez une chaîne aléatoire pour créer des compartiments d'artefacts, car les noms de compartiments doivent être uniques à l'échelle mondiale :
	
	`export BUCKETSTARTNAME=ecs-codepipeline-artifacts-19992`
	
	3. Définissez et exportez le compte IDs et les régions :
	
	`export TOOLSACCOUNT=<TOOLSACCOUNT>`
	`export CODECOMMITACCOUNT=<CODECOMMITACCOUNT>`
	`export CODECOMMITREGION=ap-south-1`	

Tâche	Description	Compétences requises

	`export CODECOMMI TREPONAME=Poc`
	`export TESTACCOU NT1=<TESTACCOUNT1>`
	`export TESTACCOU NT2=<TESTACCOUNT2>`
	`export TESTACCOU NT3=<TESTACCOUNT3>`
	`export TESTACCOU NT1REGION=ap-south -1`
	`export TESTACCOU NT2REGION=eu-centr al-1`
	`export TESTACCOU NT3REGION=us-east-1`
	`export TOOLSACCO UNTREGION=ap-south -1`
	`export ECRREPOSI TORYNAME=web`	

Package et déploiement des CloudFormation stacks pour l'infrastructure

Tâche	Description	Compétences requises

Pour cloner le référentiel.	Clonez le référentiel d'échantillons dans un nouveau référentiel sur votre lieu de travail :
	`##In work location`
	`git clone https://github.com/aws-samples/ecs-blue-green-global-deployment-with-multiregion-cmk-codepipeline.git`
		AWS DevOps

Tâche	Description	Compétences requises

Package des ressources Cloudformation.	Au cours de cette étape, vous devez empaqueter les artefacts locaux CloudFormation auxquels les modèles font référence pour créer les ressources d'infrastructure requises pour des services tels qu'Amazon Virtual Private Cloud (Amazon VPC) et Application Load Balancer.
	
	Les modèles sont disponibles dans le `Infra` dossier du référentiel de code.
	
	`##In TestAccount1##`
	`aws cloudformation package \`
	`--template-file mainInfraStack.yaml \`
	`--s3-bucket $S3BUCKETNAMETESTACCOUNT1 \`
	`--s3-prefix infraStack \`
	`--region $TESTACCOUNT1REGION \`
	`--output-template-file infrastructure_${TESTACCOUNT1}.template`
	
	`##In TestAccount2##`
	`aws cloudformation package \`
	`--template-file mainInfraStack.yaml \`
		AWS DevOps

Tâche	Description	Compétences requises

	`--s3-bucket $S3BUCKETNAMETESTACCOUNT2 \ --s3-prefix infraStack \ --region $TESTACCOUNT2REGION \ --output-template-file infrastructure_${TESTACCOUNT2}.template`
	
	`##In TestAccount3## aws cloudformation package \ --template-file mainInfraStack.yaml \ --s3-bucket $S3BUCKETNAMETESTACCOUNT3 \ --s3-prefix infraStack \ --region $TESTACCOUNT3REGION \ --output-template-file infrastructure_${TESTACCOUNT3}.template`	

Tâche	Description	Compétences requises

Validez les modèles de package.	Validez les modèles de package :
	
	`aws cloudformation validate-template \ --template-body file://infrastructure_${TESTACCOUNT1}.template`
	
	`aws cloudformation validate-template \ --template-body file://infrastructure_${TESTACCOUNT2}.template`
	
	`aws cloudformation validate-template \ --template-body file://infrastructure_${TESTACCOUNT3}.template`
		AWS DevOps

Tâche	Description	Compétences requises

Déployez les fichiers du package dans les comptes de charge de travail,	1. Mettez à jour les valeurs d'espace réservé et les noms de compte dans le `nfraParameters.jso n` script i en fonction de votre configuration.
	2. Déployez les modèles de package dans vos trois comptes de charge de travail.
	
	`##In TestAccount1## aws cloudformation deploy \ --template-file infrastructure_${TESTACCOUNT1}.template \ --stack-name mainInfrastack \ --parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT1REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM`
	
	`##In TestAccount2## aws cloudformation deploy \ --template-file infrastructure_${TESTACCOUNT2}.template \ --stack-name mainInfrastack \`
		AWS DevOps

Tâche	Description	Compétences requises
	--parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT2REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM ##In TestAccount3## aws cloudformation deploy \ --template-file infrastructure_${TESTACCOUNT3}.template \ --stack-name mainInfrastack \ --parameter-overrides file://infraParameters.json \ --region $TESTACCOUNT3REGION \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM	

Envoyez un exemple d'image et redimensionnez Amazon ECS

Tâche	Description	Compétences requises
Transférez un exemple d'image dans le référentiel Amazon ECR.	Transférez un exemple d'image (NGINX) dans le référentiel Amazon Elastic Container Registry (Amazon ECR) web nommé (tel que	AWS DevOps

Tâche	Description	Compétences requises

	défini dans les paramètres). Vous pouvez personnaliser l'image selon vos besoins.
	
	Pour vous connecter et définir les informations d'identification permettant de transférer une image vers Amazon ECR, suivez les instructions de la documentation Amazon ECR.
	
	Les commandes sont les suivantes :
	
	`docker pull nginx`
	`docker images`
	`docker tag <imageid> aws_account_id.dkr.ecr.region.amazonaws.com/<web>:latest`
	`docker push <aws_account_id>.dkr.ecr.<region>.amazonaws.com/<web>:tag`	

Tâche	Description	Compétences requises
Faites évoluer Amazon ECS et vérifiez l'accès.	1. Faites évoluer Amazon ECS pour créer deux répliques : `aws ecs update-service --cluster QA-Cluster --service Poc-Service --desired-count 2` où `Poc-Service` fait référence à votre exemple d'application. 2. Vérifiez que les services sont accessibles depuis l'Application Load Balancer en utilisant un nom de domaine complet (FQDN) ou un DNS depuis un navigateur ou en utilisant la commande curl.	AWS DevOps

Configurer les services et les ressources de code

Tâche	Description	Compétences requises
Créez un CodeCommit référentiel dans le compte Tools.	Créez un CodeCommit référentiel dans le compte d'outils à l'aide du `codecommit.yaml` modèle, qui se trouve dans le `code` dossier du GitHub référentiel. Vous ne devez créer ce référentiel que dans la seule région où	AWS DevOps

Tâche	Description	Compétences requises
	vous prévoyez de développer le code. `aws cloudformation deploy --stack-name codecommitrepoStack --parameter-overrides CodeCommitReponame=$CODECOMMITREPONAME \ ToolsAccount=$TOOLSACCOUNT --template-file codecommit.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`	

Tâche	Description	Compétences requises
Créez un compartiment S3 pour gérer les artefacts générés par CodePipeline.	Créez un compartiment S3 pour gérer les artefacts CodePipeline générés à l'aide du `pre-reqs-bucket.yaml` modèle, qui se trouve dans le `code` dossier du GitHub référentiel. Les piles doivent être déployées dans les trois comptes de charge de travail (test) et d'outils et dans les régions. `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM`  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketSta`	AWS DevOps

Tâche	Description	Compétences requises
	rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ TestAccount1=$TE STACCOUNT1 TestAccou nt2=$TESTACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts	

Tâche	Description	Compétences requises
	`-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabilities CAPABILITY_NAMED_IAM`	

Tâche	Description	Compétences requises
Configurez une clé KMS multirégionale.	1. Créez une clé KMS multirégionale avec les clés principales et répliques qui CodePipeline seront utilisées. Dans notre exemple, `ToolsAccount1region - ap-south-1` ce sera la région principale. `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION` 2. Définissez les variables CMKARN à transmettre aux CodeBuild projets. Les valeurs sont disponibles dans la sortie de la pile de modèles ecs-codepipeline-pre-reqs -KMS (l'ID de clé sera le même dans toutes les régions et	AWS DevOps

Tâche	Description	Compétences requises

	commence par`mrk-`). Vous pouvez également obtenir les valeurs CMKARN à partir du compte des outils. Exportez-les dans toutes les sessions du compte :
	
	`export CMKARN1=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN2=arn:aws:kms:eu-central-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMKARN3=arn:aws:kms:us-east-1:<TOOLSACCOUNTID>:key/mrk-xxx`
	`export CMARNTOOLS=arn:aws:kms:ap-south-1:<TOOLSACCOUNTID>:key/mrk-xxx`	

Tâche	Description	Compétences requises

Configurez le CodeBuild projet dans le compte Outils.	1. Utilisez le `codebuild_IAM.yaml` modèle figurant `code` dans le dossier du GitHub référentiel pour configurer AWS Identity and Access Management (IAM) pour AWS CodeBuild dans une seule région dans le compte tools :
	`#In ToolsAccount aws cloudformation deploy --stack-name ecs-codebuild-iam \ --template-file codebuild_IAM.yaml --region $TOOLSACCOUNTREGION \ --capabilities CAPABILITY_NAMED_IAM`
	2. Utilisez le `codebuild.yaml` modèle CodeBuild pour configurer votre projet de construction. Déployez ce modèle dans les trois régions comme suit :
	`aws cloudformation deploy --stack-name ecscodebuildstack -- parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName= $CODECOMMITREPONAME`
		AWS DevOps

Tâche	Description	Compétences requises
	ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT1 \ TestAccount3=$TESTACCOUNT3 CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN1 \ --template-file codebuild.yaml --region $TESTACCOUNT1REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN2 \ --template-file codebuild.yaml --region $TESTACCOUNT2REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name	

Tâche	Description	Compétences requises
	ecscodebuildstack --parameter-overrides ToolsAccount=$TOOLSACCOUNT \ CodeCommitRepoName=$CODECOMMITREPONAME ECRRepositoryName=$ECRREPOSITORYNAME APPACCOUNTID=$TESTACCOUNT3 \ CodeCommitRegion=$CODECOMMITREGION CMKARN=$CMKARN3 \ --template-file codebuild.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM	

Tâche	Description	Compétences requises

Configurez CodeDeploy dans les comptes de charge de travail.	Utilisez le `codedeploy.yaml` modèle figurant dans le `code` dossier du GitHub référentiel pour le configurer CodeDeploy dans les trois comptes de charge de travail. La sortie de `mainInfraStack` inclut les Amazon Resource Names (ARNs) du cluster Amazon ECS et l'écouteur Application Load Balancer.
	
	Note
	Les valeurs des piles d'infrastructure sont déjà exportées, elles sont donc importées par les modèles de CodeDeploy pile.
	
	`##WorkloadAccount1##`
	`aws cloudformation deploy --stack-name ecscodedeploystack \`
	`--parameter-overrides ToolsAccount=$TOOLSACCOUNT mainInfrastackname=mainInfrastack \`
	`--template-file codedeploy.yaml --region $TESTACCOUNT1REGION --capabil`
		AWS DevOps

Tâche	Description	Compétences requises
	ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount2## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM ##WorkloadAccount3## aws cloudformation deploy --stack-name ecscodedeploystack \ --parameter-overrides ToolsAccount=$TOOL SACCOUNT mainInfra stackname=mainInfr astack \ --template-file codedeploy.yaml --region $TESTACCO UNT3REGION --capabil ities CAPABILIT Y_NAMED_IAM	

Configuration CodePipeline dans le compte d'outils

Tâche	Description	Compétences requises
Créez un pipeline de code dans le compte Tools.	Dans le compte des outils, exécutez la commande : `aws cloudformation deploy --stack-name ecscodepipelinestack --parameter-overrides \ TestAccount1=$TESTACCOUNT1 TestAccount1Region=$TESTACCOUNT1REGION \ TestAccount2=$TESTACCOUNT2 TestAccount2Region=$TESTACCOUNT2REGION \ TestAccount3=$TESTACCOUNT3 TestAccount3Region=$TESTACCOUNT3REGION \ CMKARNTools=$CMKTROOLSARN CMKARN1=$CMKARN1 CMKARN2=$CMKARN2 CMKARN3=$CMKARN3 \ CodeCommitRepoName=$CODECOMMITREPONAME BucketStartName=$BUCKETSTARTNAME \ --template-file codepipeline.yaml --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps
Fournissez un accès CodePipeline et des CodeBuild rôles dans la	1. Fournissez un accès CodePipeline et des	AWS DevOps

Tâche	Description	Compétences requises
politique clé d'AWS KMS et dans la politique de compartiment S3.	CodeBuild rôles dans la politique clé d'AWS KMS : `aws cloudformation deploy --stack-name ecs-codepipeline-pre-reqs-KMS \ --template-file pre-reqs_KMS.yaml --parameter-overrides \ CodeBuildCondition=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT --region $TOOLSACCOUNTREGION`  2. Mettez à jour la politique du compartiment S3 pour autoriser l'accès CodePipeline et CodeDeploy les rôles :  `aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1`	

Tâche	Description	Compétences requises
	TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT1REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter- overrides BucketSta rtName=$BUCKETSTAR TNAME \ PutS3BucketPolic y=true TestAccou nt1=$TESTACCOUNT1 TestAccount2=$TEST ACCOUNT2 \ TestAccount3=$TE STACCOUNT3 CodeCommi tAccount=$CODECOMM ITACCOUNT ToolsAcco unt=$TOOLSACCOUNT \ --template-file pre- reqs_bucket.yaml --region $TESTACCO UNT2REGION --capabil ities CAPABILIT Y_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts -bucket --parameter-	

Tâche	Description	Compétences requises
	overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TESTACCOUNT3REGION --capabilities CAPABILITY_NAMED_IAM aws cloudformation deploy --stack-name pre-reqs-artifacts-bucket --parameter-overrides BucketStartName=$BUCKETSTARTNAME \ PutS3BucketPolicy=true TestAccount1=$TESTACCOUNT1 TestAccount2=$TESTACCOUNT2 \ TestAccount3=$TESTACCOUNT3 CodeCommitAccount=$CODECOMMITACCOUNT ToolsAccount=$TOOLSACCOUNT \ --template-file pre-reqs_bucket.yaml --region $TOOLSACCOUNTREGION --capabil	

Tâche	Description	Compétences requises
	`ities CAPABILIT Y_NAMED_IAM`	

Appelez et testez le pipeline

Tâche	Description	Compétences requises
Transférez les modifications au CodeCommit référentiel.	1. Clonez le CodeCommit référentiel créé dans le à `codecommitrepoStac k` l'aide de la `git clone` commande, comme décrit dans la CodeCommit documentation AWS. 2. Mettez à jour les artefacts d'entrée avec les détails requis : • Fichier JSON : mise à jour `AccountID` dans le fichier à trois endroits de ce fichier. Renommez les trois fichiers pour inclure le compte IDs. • Fichiers YAML : mettez à jour l'ARN et la version de la définition de la tâche. Renommez les trois fichiers pour inclure le compte IDs. 3. Modifiez le `index.htm l` fichier pour apporter quelques modifications	

Tâche	Description	Compétences requises

	mineures à la page d'accueil.
	4. Copiez les fichiers suivants dans le référentiel et validez :
	`index.html`
	`Dockerfile`
	`buildspec.yaml`
	`appspec_<accountid>.yaml (3 files - one per account )`
	`taskdef<accountid>.json (3 files - one per account)`
	5. Démarrez ou redémarrez le pipeline et vérifiez les résultats.
	6. Accédez au service depuis l'Application Load Balancer à l'aide d'un FQDN ou d'un DNS, et vérifiez que les mises à jour ont été déployées.	

Nettoyage

Tâche	Description	Compétences requises
Nettoyez toutes les ressources déployées.	1. Réduisez Amazon ECS à zéro instance : `aws ecs update-service --cluster QA-Cluster --service`	

Tâche	Description	Compétences requises
	Poc-Service -- desired-count 0 2. Supprimez les CloudFormation piles de chaque compte et de chaque région : ##In Tools Account## aws cloudformation delete-stack -- stack-name ecscodepipelinestack --region $TOOLSACCOUNTREGION aws cloudformation delete-stack -- stack-name ecscodebuildstack --region $TESTACCOUNT1REGION aws cloudformation delete-stack -- stack-name ecscodebuildstack --region $TESTACCOUNT2REGION aws cloudformation delete-stack -- stack-name ecscodebuildstack --region $TESTACCOUNT3REGION aws cloudformation delete-stack -- stack-name ecs-codepipeline-pre-reqs-KMS --region $TOOLSACCOUNTREGION aws cloudformation delete-stack -- stack-name codecommitrepoStack --region $TOOLSACCOUNTREGION	

Tâche	Description	Compétences requises
	aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TESTACCOUNT1REGION aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TESTACCOUNT2REGION aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TESTACCOUNT3REGION aws cloudformation delete-stack --stack-name pre-reqs-artifacts-bucket --region $TOOLSACCOUNTREGION aws cloudformation delete-stack --stack-name ecs-codebuild-iam --region $TOOLSACCOUNTREGION ##NOTE: Artifact buckets will not get deleted if there are artifacts so it has to be emptied manually before deleting.##	
	##In Workload / Test Accounts## ##Account:1##	

Tâche	Description	Compétences requises
	`aws cloudformation delete-stack --stack-name ecscodedeployst ack --region $TESTACCOUNT1REGION aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT1REGION ##Account:2## aws cloudformation delete-stack --stack-name ecscodedeployst ack --region $TESTACCOUNT2REGION aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT2REGION ##Account:3## aws cloudformation delete-stack --stack-name ecscodedeployst ack --region $TESTACCOUNT3REGION aws cloudformation delete-stack --stack-name mainInfrastack --region $TESTACCOUNT3REGION ##NOTE: Amazon ECR (web) will not get deleted if the registry still includes images. It can be manually cleaned up if not required.`	

Résolution des problèmes

Problème	Solution
Les modifications que vous avez apportées au référentiel ne sont pas déployées.	• Vérifiez les CodeBuild journaux pour détecter les erreurs lors de l'action de compilation de Docker. Pour plus d'informations, consultez la documentation CodeBuild . • Vérifiez le CodeDeploy déploiement pour détecter tout problème de déploiement d'Amazon ECS.

Ressources connexes

- Transférer une image Docker (documentation Amazon ECR)
- Connectez-vous à un CodeCommit référentiel AWS (CodeCommit documentation AWS)
- Résolution des problèmes liés à AWS CodeBuild (CodeBuild documentation AWS)

Surveillez les référentiels Amazon ECR pour détecter les autorisations génériques à l'aide d'AWS et d'AWS Config CloudFormation

Créée par Vikrant Telkar (AWS), Sajid Momin (AWS) et Wassim Benhallam (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs qui prend en charge les référentiels privés dotés d'autorisations basées sur les ressources à l'aide d'AWS Identity and Access Management (IAM).

IAM prend en charge le caractère générique « * » dans les attributs de ressource et d'action, ce qui facilite le choix automatique de plusieurs éléments correspondants. Dans votre environnement de test, vous pouvez autoriser tous les utilisateurs AWS authentifiés à accéder à un référentiel Amazon ECR en utilisant l'autorisation `ecr:*` générique dans un élément principal de votre déclaration de politique de dépôt. L'autorisation `ecr:*` générique peut être utile lors du développement et des tests dans des comptes de développement qui ne peuvent pas accéder à vos données de production.

Cependant, vous devez vous assurer que l'autorisation `ecr:*` générique n'est pas utilisée dans vos environnements de production car elle peut entraîner de graves failles de sécurité. L'approche de ce modèle vous aide à identifier les référentiels Amazon ECR qui contiennent l'autorisation `ecr:*` générique dans les déclarations de politique relatives aux référentiels. Le modèle fournit des étapes et un CloudFormation modèle AWS pour créer une règle personnalisée dans AWS Config. Une fonction AWS Lambda surveille ensuite les déclarations de politique de votre référentiel Amazon ECR pour `ecr:*` détecter les autorisations génériques. S'il trouve des déclarations de politique de dépôt non conformes, Lambda demande à AWS Config d'envoyer un événement à EventBridge EventBridge Amazon, puis lance une rubrique Amazon Simple Notification Service (Amazon SNS). La rubrique SNS vous informe par e-mail des déclarations de politique de dépôt non conformes.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée. Pour plus d'informations à ce sujet, consultez la section Installation, mise à jour et désinstallation de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS.
- Un référentiel Amazon ECR existant avec une déclaration de politique jointe, installé et configuré dans votre environnement de test. Pour plus d'informations à ce sujet, consultez les sections

Création d'un référentiel privé et Définition d'une déclaration de politique de dépôt dans la documentation Amazon ECR.

- AWS Config, configuré dans votre région AWS préférée. Pour plus d'informations à ce sujet, consultez Getting started with AWS Config dans la documentation AWS Config.
- Le `aws-config-cloudformation.template` fichier (joint), téléchargé sur votre ordinateur local.

Limites

- La solution de ce modèle est régionale et vos ressources doivent être créées dans la même région.

Architecture

Le schéma suivant montre comment AWS Config évalue les déclarations de politique du référentiel Amazon ECR.

Le schéma suivant illustre le flux de travail suivant :

1. AWS Config initie une règle personnalisée.
2. La règle personnalisée invoque une fonction Lambda pour évaluer la conformité des déclarations de politique du référentiel Amazon ECR. La fonction Lambda identifie ensuite les déclarations de politique de référentiel non conformes.
3. La fonction Lambda envoie le statut de non-conformité à AWS Config.
4. AWS Config envoie un événement à EventBridge.
5. EventBridge publie les notifications de non-conformité sur une rubrique SNS.
6. Amazon SNS envoie une alerte par e-mail à vous ou à un utilisateur autorisé.

Automatisation et évolutivité

La solution de ce modèle peut surveiller un certain nombre de déclarations de politique relatives au référentiel Amazon ECR, mais toutes les ressources que vous souhaitez évaluer doivent être créées dans la même région.

Outils

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.
- AWS Config — AWS Config fournit une vue détaillée de la configuration des ressources AWS dans votre compte AWS. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, pour que vous puissiez observer comment les configurations et les relations changent au fil du temps.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs géré par AWS qui est sécurisé, évolutif et fiable. Amazon ECR prend en charge les référentiels privés avec des autorisations basées sur les ressources à l'aide d' IAM.

- Amazon EventBridge — Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel provenant de vos applications, de vos applications SaaS et des services AWS à des cibles telles que les fonctions AWS Lambda, les points de terminaison d'invocation HTTP utilisant des destinations d'API ou les bus d'événements d'autres comptes.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Le code de ce modèle est disponible dans le `aws-config-cloudformation.template` fichier (joint).

Épopées

Création de la CloudFormation pile AWS

Tâche	Description	Compétences requises
Créez la CloudFormation pile AWS.	Créez une CloudFormation pile AWS en exécutant la commande suivante dans l'AWS CLI : `$ aws cloudformation create-stack --stack-name=AWSConfigECR \ --template-body file://aws-config-cloudformation.template \ --parameters ParameterKey=<email>,ParameterValue=<myemail@example.com> \ --capabilities CAPABILITY_NAMED_IAM`	AWS DevOps

Testez la règle personnalisée AWS Config

Tâche	Description	Compétences requises
Testez la règle personnalisée AWS Config.	1. Connectez-vous à l'AWS Management Console, ouvrez la console AWS Config, puis choisissez Resources. 2. Sur la page Inventaire des ressources, vous pouvez filtrer par catégorie	AWS DevOps

Tâche	Description	Compétences requises
	de ressource, type de ressource et statut de conformité. 3. Un référentiel Amazon ECR qui contient de l'`ecr:*`est `NON-COMPLIANT?` et un référentiel Amazon ECR qui ne le contient `ecr:*` pas. `COMPLIANT` 4. L'adresse e-mail abonnée à la rubrique SNS reçoit des notifications si un référentiel Amazon ECR contient des déclarations de politique non conformes.	

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Optimisez les déploiements multicomptes sans serveur en utilisant les flux de travail et AWS CDK Actions GitHub

Créée par Sarat Chandra Pothula (AWS) et VAMSI KRISHNA SUNKAVALLI (AWS)

Récapitulatif

Organisations qui déploient une infrastructure sans serveur sur plusieurs Comptes AWS environnements sont souvent confrontées à des défis tels que la duplication de code, les processus manuels et les pratiques incohérentes. La solution de ce modèle montre comment utiliser les flux de travail réutilisables AWS Cloud Development Kit (AWS CDK) in Go et GitHub Actions pour rationaliser la gestion de l'infrastructure sans serveur multi-comptes. Cette solution montre comment définir les ressources cloud sous forme de code, implémenter des processus standardisés integration/continuous deployment (CI/CD (continus) et créer des composants modulaires et réutilisables.

En utilisant ces outils, les entreprises peuvent gérer efficacement les ressources entre comptes, mettre en œuvre des pipelines de déploiement cohérents et simplifier les architectures sans serveur complexes. Cette approche améliore également la sécurité et la conformité en appliquant des pratiques normalisées d'utilisation Comptes AWS, ce qui permet d'améliorer la productivité et de réduire les erreurs lors du développement et du déploiement d'applications sans serveur.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Identity and Access Management Les rôles et autorisations (IAM) sont en place pour le processus de déploiement. Cela inclut les autorisations pour accéder aux référentiels Amazon Elastic Container Registry (Amazon ECR), AWS Lambda créer des fonctions et toute autre ressource requise sur l'ensemble de la cible. Comptes AWS
- AWS Command Line Interface (AWS CLI) version 2.9.11 ou ultérieure, installée et configurée.
- AWS Cloud Development Kit (AWS CDK) version 2.114.1 ou ultérieure, installée et démarrée.
- Go 1.22 ou version ultérieure, installé.
- Docker 24.0.6 ou version ultérieure, installé.

Limites

- Compatibilité linguistique — Go est un langage populaire pour les applications sans serveur. Cependant, outre Go, il AWS CDK prend en charge d'autres langages de programmation, notamment C#, Java, Python et TypeScript. Si votre organisation possède déjà des bases de code ou une expertise dans d'autres langages, vous devrez peut-être adapter ou apprendre Go pour utiliser pleinement la solution décrite dans le modèle.
- Courbe d'apprentissage — L' AWS CDK adoption de flux de travail « Go » (s'il s'agit d'une nouveauté pour l'entreprise) et GitHub réutilisables peut impliquer une courbe d'apprentissage pour les développeurs et les DevOps équipes. Une formation et une documentation peuvent être nécessaires pour garantir une adoption harmonieuse et une utilisation efficace de ces technologies.

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Cette solution exécute les étapes suivantes :

1. Le développeur clone le référentiel, crée une nouvelle branche et modifie le code de l'application dans son environnement local.
2. Le développeur valide ces modifications et envoie la nouvelle branche dans le GitHub référentiel.
3. Le développeur crée une pull request dans le GitHub référentiel, proposant de fusionner sa branche de fonctionnalité ou de nouvelle fonctionnalité dans la branche principale.
4. Cette pull request déclenche le flux de travail des GitHub actions d'intégration continue (CI). Les flux de travail CI et de déploiement continu (CD) de ce modèle utilisent des flux de travail réutilisables, qui sont des modèles modulaires prédéfinis qui peuvent être partagés et exécutés dans différents projets ou référentiels. Les flux de travail réutilisables favorisent la standardisation et l'efficacité des processus CI/CD.
5. Le flux de travail CI configure l'environnement nécessaire, génère une balise Docker pour l'image et crée l'image Docker à l'aide du code de l'application.
6. Le flux de travail CI s'authentifie AWS en utilisant le rôle central Compte AWS GitHub OIDC. Pour les flux de travail CI, le rôle Compte AWS GitHub OIDC central utilise AWS Security Token Service (AWS STS) pour obtenir des informations d'identification temporaires. Ces informations d'identification permettent au rôle de créer et de transférer des images Docker vers le référentiel Amazon ECR de la centrale. Compte AWS
7. Le flux de travail CI envoie l'image Docker créée vers Amazon ECR.

8. Le flux de travail CI stocke la balise d'image dans le magasin de paramètres de Systems Manager.
9. Une fois le flux de travail CI terminé avec succès, la balise d'image Docker est sortie.
10. Lors du déclenchement du flux de travail sur CD, le développeur saisit manuellement la balise d'image de l'image Docker qu'il souhaite déployer. Cette balise d'image correspond à la balise qui a été générée et envoyée à Amazon ECR pendant le flux de travail CI.
11. Le développeur déclenche manuellement le flux de travail sur CD, qui utilise le flux de travail réutilisable sur CD.
12. Le flux de travail du CD s'authentifie à AWS l'aide du rôle central Compte AWS GitHub OIDC. Pour le flux de travail sur CD, AWS STS il est d'abord utilisé pour assumer le rôle central de l' Compte AWS GitHub OIDC. Ce rôle assume ensuite les rôles d'amorçage du CDK pour les déploiements de comptes cibles.
13. Le flux de travail sur CD utilise le AWS CDK pour synthétiser des AWS CloudFormation modèles.
14. Le flux de travail CD déploie l'application sur la cible Compte AWS à l'aide de CDK deploy, en utilisant la balise image spécifiée manuellement pour la fonction Lambda.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS. CloudFormation fait partie intégrante du processus de AWS CDK déploiement. Le CDK synthétise les CloudFormation modèles, puis les utilise CloudFormation pour créer ou mettre à jour les ressources de l' AWS environnement.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- GitHub Actions est une plateforme d'intégration et de livraison continues (CI/CD) étroitement intégrée aux GitHub référentiels. Vous pouvez utiliser GitHub les actions pour automatiser votre pipeline de création, de test et de déploiement.
- Go est un langage de programmation open source pris en charge par Google.

Référentiel de code

Le code de ce modèle est disponible dans le cicd-github-actions référentiel GitHub aws-cdk-golang-serverless-.

Bonnes pratiques

- Conception modulaire : organisez votre AWS CDK code en structures ou en piles modulaires et réutilisables, afin de promouvoir la réutilisation et la maintenabilité du code sur plusieurs comptes et projets.
- Séparation des préoccupations — Séparez le code d'infrastructure du code d'application, ce qui permet un déploiement et une gestion indépendants de chaque composant.
- Gestion des versions et immuabilité : traitez votre infrastructure comme du code (IaC) et utilisez Git pour le contrôle de version. Adoptez des principes d'infrastructure immuables en créant de nouvelles ressources au lieu de modifier les ressources existantes.
- Tests et validation : mettez en œuvre des stratégies de test complètes, notamment des tests unitaires, des tests d'intégration et end-to-end des tests, afin de garantir l'exactitude et la fiabilité de votre AWS CDK code et de vos déploiements.
- Sécurité et conformité : suivez les meilleures pratiques en matière de AWS sécurité, telles que l'accès au moindre privilège, les communications sécurisées et le chiffrement des données. Mettez en œuvre des contrôles de conformité et des mécanismes d'audit pour garantir le respect des politiques organisationnelles et des exigences réglementaires. Mettez en œuvre les meilleures pratiques de sécurité pour les images de conteneur, telles que l'analyse des vulnérabilités, l'application de la signature des images et le respect des exigences de conformité de votre entreprise.
- Surveillance et journalisation : configurez des mécanismes de surveillance et de journalisation pour suivre l'état et les performances de vos applications et infrastructures sans serveur. Services AWS

À utiliser comme Amazon CloudWatch AWS CloudTrail, et à des AWS X-Ray fins de surveillance et d'audit.

- Automatisation et CI/CD : utilisez des flux de travail GitHub réutilisables et d'autres outils CI/CD pour automatiser les processus de création, de test et de déploiement, ce qui peut contribuer à garantir des déploiements cohérents et reproductibles sur plusieurs comptes.
- Gestion de l'environnement : maintenez des environnements distincts (par exemple, développement, mise en scène et production). Mettez en œuvre des stratégies pour promouvoir les changements entre les environnements, en garantissant des tests et une validation appropriés avant les déploiements en production.
- Documentation et collaboration — Documentez le code de votre infrastructure, les processus de déploiement et les meilleures pratiques pour faciliter le partage des connaissances et la collaboration au sein de votre équipe.
- Optimisation des coûts — Mettez en œuvre des stratégies de surveillance et d'optimisation des coûts, telles que la rationalisation des ressources, l'utilisation de l'auto-scaling et la mise à profit de services d'optimisation des AWS coûts tels que et. AWS Budgets AWS Cost Explorer
- Reprise après sinistre et sauvegarde : planifiez des scénarios de reprise après sinistre en mettant en œuvre des mécanismes de sauvegarde et de restauration pour vos applications sans serveur et vos ressources d'infrastructure.
- Amélioration continue — Passez régulièrement en revue et mettez à jour vos pratiques, outils et processus afin de les aligner sur les meilleures pratiques, les recommandations de sécurité et les avancées technologiques les plus récentes de l'écosystème sans serveur.
- Améliorez le niveau de sécurité : AWS PrivateLinkà utiliser pour améliorer le niveau de sécurité de votre cloud privé virtuel (VPC) en configurant les points de terminaison VPC d'interface pour Amazon ECR et Parameter Store. AWS Lambda AWS Systems Manager

Épopées

Configuration des environnements

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR dans le centre Compte AWS.	Pour partager des images de conteneurs entre plusieurs Comptes AWS, vous devez configurer l'accès entre	AWS DevOps

Tâche	Description	Compétences requises
	comptes pour Amazon ECR. Tout d'abord, créez un référentiel Amazon ECR dans le centre Compte AWS. Pour créer un référentiel Amazon ECR, exécutez la commande suivante : `aws ecr create-repository --repository-name sample-repo` Dans une tâche ultérieure, accordez l'accès pull à l'autre Comptes AWS personne qui doit utiliser l'image du conteneur.	

Tâche	Description	Compétences requises
Ajoutez des autorisations entre comptes au référentiel Amazon ECR.	Pour ajouter des autorisations entre comptes au référentiel Amazon ECR dans le système central Compte AWS, exécutez le code suivant : `{ "Version": "2008-10-17", "Statement": [{ "Sid": "LambdaECRImageRetrievalPolicy", "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": ["ecr:BatchGetImage", "ecr:GetDownloadUrlForLayer",], "Condition": { "StringLike": { "aws:sourceArn": "arn:aws:lambda:<Target_Region>:<Target_Account_ID>:function:*" } } }, { "Sid": "new statement", "Effect": "Allow",`	AWS DevOps

Tâche	Description	Compétences requises
	"Principal": { "AWS": "arn:aws:iam::<Target_Account_ID>:root" }, "Action": ["ecr:BatchGetImage", "ecr:GetDownloadUrlForLayer",], }] }	

Tâche	Description	Compétences requises
Configurez un rôle pour le rôle GitHub OIDC dans la centrale Compte AWS.	1. Configurez AWS pour faire confiance à GitHub l'OIDC en tant qu'identité fédérée, ce qui inclut l'ajout du fournisseur GitHub OIDC et la configuration du rôle AWS et de la politique de confiance dans IAM. Pour ce faire, suivez les instructions de la section Configuration d'OpenID Connect dans Amazon Web Services dans la GitHub documentation. 2. Une fois le rôle créé, ajoutez-y les autorisations nécessaires. Par exemple, ajoutez des autorisations pour Amazon ECR et AWS Systems Manager Parameter Store. Pour plus d'informations, consultez la section Configuration d'un rôle pour le fournisseur d'identité GitHub OIDC dans la documentation IAM.	AWS DevOps

Tâche	Description	Compétences requises
Démarrez l' AWS environnement dans la cible Comptes AWS.	Configurez un environnement CDK dans un environnement spécifique Région AWS qui permet Compte AWS les déploiements entre comptes à partir d'un compte central et applique le principe du moindre privilège au rôle d'exécution. CloudFormation Pour démarrer un AWS environnement, exécutez la commande suivante : `cdk bootstrap aws://<Target_Account_ID>/<Target_Region> --trust <Central_Account_ID> --cloudformation-execution-policies arn:aws:iam::aws:policy/<Least_Privilege_Policy>`	AWS DevOps

Tâche	Description	Compétences requises
Accordez l'accès aux rôles Compte AWS OIDC centraux aux rôles Compte AWS bootstrap cibles.	Le bootstrap du CDK crée les rôles IAM suivants, conçus pour être assumés par le central au Compte AWS cours des différentes étapes du processus de déploiement du CDK : • Rôle de publication de fichiers • Rôle de publication d'images • Rôle de recherche • Rôle de déploiement Chaque rôle dispose d'autoris ations spécifiques adaptées à son objectif, conformém ent au principe du moindre privilège. Le `Target_Ac count_ID` et `Target_Re gion` dans le nom de chaque rôle indique que ces rôles sont uniques selon Comptes AWS les différentes régions. Cette approche permet une identific ation et une gestion claires dans les configurations multi-comptes et multi-régions. `Target Account CDK Bootstrap Roles arn:aws:iam::<Target_ Account_ID>:role/c dk-deploy-role-<Ta`	AWS DevOps

Tâche	Description	Compétences requises

	<pre>rget_Account_ID>-
	Target_Region>
	arn:aws:iam::<Target_
	Account_ID>:role/cdk-
	file-publishing-role-
	<Target_Account_ID>-<
	Target_Region>
	arn:aws:iam::<Target_
	Account_ID>:role/cdk-
	image-publishing-role-
	<Target_Account_ID>-
	<Target_Region>
	arn:aws:iam::<Target
	_Account_ID>:role/
	cdk-lookup-role-<T
	arget_Account_ID>-
	<Target_Region></pre>
	• Mettez à jour la politique d'autorisation pour le rôle OIDC dans le compte central afin de lui permettre d'assumer des rôles dans le compte cible. Cette configuration permet le déploiement de piles CDK sur différentes plateform es. Comptes AWS En autorisant le rôle OIDC du compte central à adopter les autorisations nécessair es depuis le compte cible, vous créez un pont sécurisé pour les déploiements de CDK entre comptes. Cette approche permet de maintenir un contrôle	

Tâche	Description	Compétences requises
	d'accès approprié tout en facilitant la gestion fluide de l'infrastructure multi-comptes. Pour mettre à jour la politique d'autorisation pour le rôle OIDC dans la centrale Compte AWS, utilisez le code suivant : `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": ["arn:aws:iam::<Target_Account_ID>:role/cdk-deploy-role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-file-publishing-role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-image-publishing-`	

Tâche	Description	Compétences requises
	role-<Target_Account_ID>-<Target_Region>”, “arn:aws:iam::<Target_Account_ID>:role/cdk-lookup-role-<Target_Account_ID>-<Target_Region>”] }] }	

Créez l'image Docker

Tâche	Description	Compétences requises
Clonez le référentiel du projet.	Pour cloner le GitHub dépôt de ce modèle, exécutez la commande suivante : `git clone https://github.com/aws-samples/aws-cdk-golang-serverless-cicd-github-actions.git`	AWS DevOps
Accédez au chemin Dockerfile.	Pour accéder au chemin Dockerfile, exécutez la commande suivante : `cd lambda`	AWS DevOps
Authentifiez Docker avec Amazon ECR.	Amazon ECR nécessite un accès sécurisé à vos référentiels de conteneurs privés. En	AWS DevOps

Tâche	Description	Compétences requises
	signant de cette manière, vous autorisez Docker sur votre machine locale ou votre environnement CI/CD à interagir avec Amazon ECR en toute sécurité. Pour authentifier Docker auprès d'Amazon ECR, exécutez la commande suivante : `aws ecr get-login -password --region <AWS_REGION> | docker login --username AWS --password-stdin <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com` Révisez les espaces réservés `AWS_REGION` et `AWS_Account_ID` utilisez vos informations.	
Développez l'image Docker.	Pour créer l'image Docker, exécutez la commande suivante : `docker build --platform linux/arm64 -t sample-app .`	AWS DevOps

Tâche	Description	Compétences requises

Marquez et appuyez sur l'image Docker.	Pour étiqueter et transférer l'image Docker vers le référentiel Amazon ECR, exécutez les commandes suivantes :
	`docker tag sample-app:latest <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/<ECR_REPOSITORY>:<DOCKER_TAG>`
	`docker push <AWS_ACCOUNT_ID>.dkr.ecr.<AWS_REGION>.amazonaws.com/<ECR_REPOSITORY>:<DOCKER_TAG>`
	Révisez les espaces réservés `AWS_Account_ID` `AWS_REGION` ,`ECR_REPOSITORY` , et `DOCKER_TAG` avec vos informations.
		AWS DevOps

Déployez l' AWS CDK application

Tâche	Description	Compétences requises
Synthétisez la pile CDK avec des variables spécifiques à l'environnement.	Pour générer le CloudFormation modèle de votre infrastructure tel que défini dans votre code CDK, exécutez la commande suivante :	AWS DevOps

Tâche	Description	Compétences requises
	`ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk synth` Modifiez les espaces réservés suivants en fonction de vos informations : • `environment` — Remplacé par un nom d'environnement spécifique tel que `dev`, `staging`, ou `prod`. • `image_tag` — Remplacez par une balise spécifique pour une image Docker, telle que `v1.0.0` ou `latest`. • `ecr_repo_arn` — Remplacez par le nom de ressource Amazon (ARN) d'un référentiel Amazon ECR.	

Tâche	Description	Compétences requises
Déployez la pile CDK.	Pour déployer la pile CDK sur votre Compte AWS, exécutez la commande suivante. L'`--require-approval never`indicateur signifie que le CDK approuvera et exécutera automatiquement toutes les modifications. Cela inclut les modifications que le CDK signalerait normalement comme nécessitant une révision manuelle (telles que les modifications de la politique IAM ou la suppression de ressources). Assurez-vous que votre code CDK et votre pipeline CI/CD sont bien testés et sécurisés avant d'utiliser l'`--require-approval never`indicateur dans les environnements de production. `ENV=<environment> IMAGETAG=<image_tag> ECR_ARN=<ecr_repo_arn> cdk deploy --require-approval never`	AWS DevOps

Automatisez le CI/CD à l'aide GitHub des flux de travail Actions

Tâche	Description	Compétences requises

Créez une branche de fonctionnalités et ajoutez vos modifications.	Utilisez le référentiel cloné que vous avez créé précédemment, créez une branche de fonctionnalités, puis ajoutez vos modifications au code de l'application. Utilisez les commandes suivantes :
	`git checkout -b <feature_branch>`
	`git add .`
	`git commit -m “add your changes”`
	`git push origin <feature_branch>`
	Voici des exemples de modifications :
	• Modifications apportées à la logique de la fonction Lambda
	• Ajouter de nouvelles fonctionnalités ou fonctionnalités au code Lambda
	• Corriger des bogues ou optimiser le code existant dans la fonction Lambda
	GitHub Les actions utiliseront les flux de travail réutilisables et déclencheront les pipelines CI/CD.
		AWS DevOps

Tâche	Description	Compétences requises
Fusionnez vos modifications.	Créez une pull request et fusionnez vos modifications avec la commande principale.	AWS DevOps

Résolution des problèmes

Problème	Solution
`AccessDenied` des erreurs lors du déploiement de ressources entre Comptes AWS, par exemple,`AccessDenied: User not authorized to perform: “sts:AssumeRole" .`	Pour résoudre ce problème, procédez comme suit pour vérifier les autorisations entre comptes : • Assurez-vous que les rôles et politiques IAM nécessaires sont en place pour les déploiements entre comptes. • Vérifiez que les autorisations de `assume` rôle sont correctement configurées.
Problèmes de compatibilité dus à des incohérences de version, par exemple une `undefined: awscdkStack` erreur avec une version obsolète du CDK.	Pour résoudre ce problème, procédez comme suit pour vérifier que vous utilisez les versions requises de AWS CDK and Go : • Assurez-vous que vous utilisez des versions compatibles de AWS CDK et Go. • Vérifiez s'il existe des problèmes connus ou des modifications importantes dans les versions récentes.
Défaillances du pipeline CI/CD, par exemple, en `Error: No such file or directory` raison d'une configuration YAML incorrecte ou de branches protégées`Permission denied`.	Pour résoudre les problèmes liés à la configuration GitHub des actions, vérifiez que les flux de travail réutilisables sont correctement référencés et configurés.

Ressources connexes

Ressources AWS

- AWS Bonnes pratiques en matière de sécurité, d'identité et de conformité
- AWS CDK Atelier
- AWS Bibliothèque de kits de développement Cloud
- Création d'une fonction Lambda à l'aide d'une image de conteneur
- Identity and Access Management pour Amazon Elastic Container Registry
- Utilisation du kit AWS CDK dans Go

Autres ressources

- Configuration d'OpenID Connect dans Amazon Web Services (documentation) GitHub
- Documentation sur le Golang
- Démarrage rapide pour les GitHub actions (GitHub documentation)
- Réutilisation des flux de travail (GitHub documentation)

Effectuez des actions personnalisées à partir d' CodeCommit événements AWS

Créée par Abdullahi Olaoye (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Lorsque vous utilisez un CodeCommit référentiel AWS pour stocker du code, vous souhaiterez peut-être surveiller le référentiel et lancer un flux de travail d'actions lorsque des événements spécifiques se produisent. Par exemple, vous pouvez envoyer une notification par e-mail lorsqu'un utilisateur commente une ligne de code dans un commit, ou lancer une fonction AWS Lambda pour effectuer des analyses de sécurité sur le contenu du référentiel après un commit. Ce modèle décrit les étapes de configuration d'un CodeCommit référentiel pour des actions personnalisées. Le modèle utilise les règles de CodeCommit notification AWS pour capturer les événements intéressants, puis envoie ces événements à une cible configurée.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Connaissance des commandes Git.
- AWS CodeCommit, configurez. Pour obtenir des instructions, consultez Configuration pour AWS CodeCommit.
- (Recommandé) Interface de ligne de commande AWS (AWS CLI), installée et configurée. Pour obtenir des instructions, consultez Getting started with the AWS CLI.

Architecture

Outils

Services AWS

- AWS CodeCommit est un service de contrôle de source entièrement géré qui héberge des référentiels sécurisés basés sur Git. Il permet aux équipes de collaborer facilement sur le code dans un écosystème sécurisé et hautement évolutif. CodeCommit élimine le besoin d'exploiter votre propre système de contrôle de source ou de vous soucier de la mise à l'échelle de son infrastructure
- Amazon Simple Notification Service (Amazon SNS) est un service Web qui permet aux applications, aux utilisateurs finaux et aux appareils d'envoyer et de recevoir instantanément des notifications depuis le cloud. Amazon SNS propose des rubriques (canaux de communication) pour la messagerie push à haut débit. many-to-many À l'aide des rubriques Amazon SNS, les éditeurs peuvent distribuer des messages à un grand nombre d'abonnés pour un traitement parallèle, notamment les files d'attente Amazon Simple Queue Service (Amazon SQS), les fonctions AWS Lambda et les webhooks HTTP/S. Vous pouvez également utiliser Amazon SNS pour envoyer des notifications aux utilisateurs finaux par push mobile, SMS et e-mail.

Épopées

Configuration d'un CodeCommit référentiel

Tâche	Description	Compétences requises
Créez un CodeCommit référentiel.	Utilisez la CodeCommi t console ou la CLI AWS pour créer un CodeCommit référentiel. Pour obtenir des instructions, voir Création d'un CodeCommit référentiel.	DevOps ingénieur
Transférez le contenu vers le CodeCommit référentiel.	Après avoir créé un dépôt, ajoutez-y du contenu à l'aide des commandes Git. Vous pouvez migrer le contenu d'un dépôt Git existant ou du contenu local non versionné depuis votre ordinateur. Pour obtenir des instructions, consultez Ajouter des fichiers	DevOps ingénieur

Tâche	Description	Compétences requises
	à votre référentiel ou Migrer vers AWS CodeCommit.	

Configurer Amazon SNS

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Cette rubrique SNS reçoit les événements de CodeCommit. Pour obtenir des instructions, consultez la rubrique Création d'un Amazon SNS.	Architecte cloud, DevOps ingénieur
Créez une ressource pour une action personnalisée.	Pour que l'action personnalisée soit exécutée, vous devez créer la ressource correspondante. Par exemple, si votre action personnalisée consiste à exécuter du code Lambda et à envoyer des messages à une file d'attente SQS, vous devez créer la fonction Lambda et la file d'attente SQS. Les actions telles que les notifications par e-mail et par SMS ne nécessitent aucune ressource. Pour plus d'informations, consultez la documentation AWS relative au type de ressource que vous créez.	Architecte cloud, DevOps ingénieur
Abonnez la ressource d'action personnalisée à la rubrique SNS.	En fonction de l'action personnalisée, vous créez un abonnement pour le protocole	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	approprié. Par exemple, vous souscrivez une adresse e-mail pour recevoir des notifications par e-mail, une fonction Lambda pour exécuter du code personnalisé ou une file d'attente SQS pour envoyer des événements à Amazon SQS. Pour les protocoles d'abonnement tels que les e-mails et les SMS, vous devez confirmer l'abonnement à l'aide du lien envoyé à l'e-mail ou au numéro de téléphone, respectivement. Pour obtenir des instructions, consultez la section S'abonner à une rubrique Amazon SNS.	

Configuration des règles de notification

Tâche	Description	Compétences requises
Créez la règle de notification pour le CodeCommit référentiel.	Lorsque vous créez la règle de notification, vous sélectionnez les événements Git qui doivent lancer la notification, vous sélectionnez le sujet SNS comme type de cible, puis le sujet SNS que vous avez créé précédemment. Vous pouvez également configurer plusieurs cibles pour le référentiel. Pour obtenir des instructions,	DevOps ingénieur

Tâche	Description	Compétences requises
	voir Création d'une règle de notification.	
Testez les actions personnalisées.	Effectuez l'un des événements configurés pour lancer la notification. Par exemple, créez une pull request si vous avez sélectionné cet événement comme déclencheur. Vous devriez voir votre action personnalisée être exécutée. Par exemple, si vous avez souscrit une adresse e-mail à la rubrique SNS, vous devriez recevoir une notification par e-mail.	DevOps ingénieur

Ressources connexes

- CodeCommit Documentation AWS
- Documentation Amazon SNS
- Documentation Git

Provisionner AWS Service Catalog des produits basés sur AWS CloudFormation des modèles à l'aide d' GitHub actions

Créée par Ashish Bhatt (AWS) et Ruchika Modi (AWS)

Récapitulatif

Ce modèle fournit aux organisations une approche rationalisée utilisant des AWS Service Catalogproduits et des portefeuilles pour fournir des services standardisés et conformes à Services AWS toutes les équipes. AWS CloudFormationpermet de combiner les composants essentiels des produits et des portefeuilles Service Catalog pour le provisionnement de l'infrastructure réseau de base. AWS Cloud Ce modèle favorise également DevOps les pratiques en intégrant l'infrastructure en tant que code (IaC) dans les flux de travail de développement automatisés à l'aide d'GitHub actions.

AWS Service Catalog permet aux entreprises de créer et de gérer des services informatiques approuvés sur AWS, offrant des avantages tels que la standardisation, le contrôle centralisé, le provisionnement en libre-service et la gestion des coûts. En automatisant le déploiement des portefeuilles et des produits Service Catalog par le biais d' GitHub actions, les entreprises peuvent effectuer les opérations suivantes :

- Réalisez des déploiements cohérents et reproductibles.
- Utilisez le contrôle de version pour IaC.
- Intégrez la gestion des ressources cloud aux flux de développement existants.

Cette combinaison rationalise les opérations dans le cloud, renforce la conformité et accélère la fourniture de services approuvés tout en réduisant les erreurs manuelles et en améliorant l'efficacité globale.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Accès au GitHub référentiel
- Compréhension de base de AWS CloudFormation et AWS Service Catalog
- Un compartiment Amazon Simple Storage Service (Amazon S3) pour héberger des modèles CloudFormation

- Rôle AWS Identity and Access Management (IAM) nommé `github-actions` qui est utilisé pour la connectivité entre et GitHub AWS

Limites

- Le code réutilisable de ce modèle a été testé uniquement avec GitHub des actions.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

La solution de ce modèle a été créée à l'aide des actions GitHub Marketplace suivantes et de leurs versions respectives :

- `actions/checkout@v4`
- `aws-actions/configure-aws-credentials@v2`
- `aws-actions/aws-cloudformation-github-deploy@v1.2.0`

Architecture

Le schéma suivant montre l'architecture de cette solution.

1. Les administrateurs ou les ingénieurs de plateforme CloudFormation transfèrent les modèles standardisés vers un GitHub référentiel, où ils sont conservés. Le GitHub dépôt contient également des flux de travail qui automatisent le provisionnement à l' AWS Service Catalog aide GitHub d'actions.
2. GitHub Actions déclenche un flux de travail qui se connecte à l' AWS Cloud aide d'un fournisseur OpenID Connect (OIDC) pour approvisionner Service Catalog.
3. Service Catalog contient le portefeuille et les produits que les développeurs peuvent directement utiliser pour fournir AWS des ressources standardisées. Ce modèle regroupe AWS des ressources telles que les clouds privés virtuels (VPCs), les sous-réseaux, les passerelles NAT et Internet, ainsi que les tables de routage.

4. Une fois que le développeur a créé un produit Service Catalog, Service Catalog le convertit en AWS ressources préconfigurées et standardisées. Les développeurs gagnent ainsi du temps car ils n'ont pas besoin de provisionner des ressources individuelles et de les configurer manuellement.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS. Il s'agit d'un service d'infrastructure sous forme de code (IaC) qui peut être facilement utilisé comme l'un des types de produits AWS Service Catalog.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Service Catalogvous permet de gérer de manière centralisée le catalogue des services informatiques approuvés AWS. Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres

- GitHub Actions est une plateforme d'intégration et de livraison continues (CI/CD) étroitement intégrée aux GitHub référentiels. Vous pouvez utiliser GitHub les actions pour automatiser votre pipeline de création, de test et de déploiement.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub service-catalog-with-github-actions. Le dépôt contient les fichiers intéressants suivants :

- `github/workflows`:
  - `e2e-test.yaml`— Ce fichier appelle`workflow.yaml`, qui est le flux de travail réutilisable. Ce flux de travail est déclenché dès qu'il y a un commit et un push sur une branche.

  - `workflow.yaml`— Ce fichier contient le flux de travail réutilisable pour cette solution et est configuré avec `workflow_call` comme déclencheur. En tant que flux de travail réutilisable, il `workflow.yaml` peut être appelé depuis n'importe quel autre flux de travail.
- `templates`:
  - `servicecatalog-portfolio.yaml`— Ce CloudFormation modèle inclut des ressources qui fournissent le portefeuille Service Catalog et le produit Service Catalog. Le modèle contient un ensemble de paramètres utilisés lors du provisionnement du portefeuille et des produits Service Catalog. Un paramètre accepte l'URL d'un fichier Amazon S3 où le modèle `vpc.yaml` est chargé. Bien que ce modèle inclut le `vpc.yaml` fichier pour provisionner AWS les ressources, vous pouvez également utiliser le paramètre URL du fichier S3 pour la configuration.
  - `vpc.yaml`— Ce CloudFormation modèle contient AWS des ressources à ajouter au produit Service Catalog. AWS les ressources incluent les VPCs sous-réseaux, les passerelles Internet, les passerelles NAT et les tables de routage. Le `vpc.yaml` modèle est un exemple de la manière dont vous pouvez utiliser n'importe quel CloudFormation modèle avec un modèle de produit et de portefeuille Service Catalog.

Bonnes pratiques

- Consultez les meilleures pratiques de sécurité AWS Service Catalog dans la AWS Service Catalog documentation.
- Consultez la section Renforcement de la sécurité pour GitHub les actions dans la GitHub documentation.

Épopées

Configuration d'un poste de travail local

Tâche	Description	Compétences requises
Configurez Git sur votre poste de travail local.	Pour installer et configurer Git sur votre poste de travail local, utilisez les instructions Getting Started — Install Git de la documentation Git.	Développeur d’applications

Tâche	Description	Compétences requises
Clonez le dépôt GitHub du projet.	Pour cloner le dépôt GitHub du projet, procédez comme suit : 1. Ouvrez le GitHub dépôt pour ce modèle 2. Choisissez Code pour voir les options de clonage, puis copiez l'URL fournie dans l'onglet HTTPS. 3. Créez un dossier pour votre projet sur votre poste de travail. 4. Ouvrez un terminal et naviguez jusqu'à ce dossier 5. Pour cloner le GitHub dépôt, exécutez la commande suivante à l'aide de l'URL que vous avez copiée à l'étape 2 : `git clone https://github.com/aws-samples/service-catalog-with-github-actions.git` 6. Une fois le clonage terminé, pour accéder au dépôt cloné dans le dossier de votre projet, exécutez la commande suivante :	DevOps ingénieur

Tâche	Description	Compétences requises
	``` cd <folder-name>/service-catalog-with-github-actions ``` 7. Ouvrez le projet dans un environnement de développement intégré (IDE) de votre choix.	

Configurer le fournisseur OIDC

Tâche	Description	Compétences requises
Configurez un fournisseur OIDC.	Créez un fournisseur OpenID Connect (OIDC) qui permet aux flux de travail GitHub Actions d'accéder aux ressources AWS, sans avoir à stocker les informations d' AWS identification sous forme de secrets de longue durée. GitHub Pour obtenir des instructions, consultez la section Configuration d'OpenID Connect dans Amazon Web Services dans la GitHub documentation. Une fois qu'un fournisseur OIDC est configuré, la politique de confiance du rôle IAM`github-actions` , mentionnée plus haut dans	Administrateur AWS, AWS DevOps, AWS général

Tâche	Description	Compétences requises
	les conditions préalables, sera mise à jour.	

Pipeline Trigger GitHub Actions pour déployer le portefeuille et les produits Service Catalog

Tâche	Description	Compétences requises
Mettre à jour `e2e-test.yaml` .	Le `e2e-test.yaml` fichier déclenche le flux de travail réutilisable à l'adresse `workflow.yaml` . Mettez à jour et validez les valeurs des paramètres d'entrée suivants dans `e2e-test.yaml` : • `aws_account_id` — Spécifiez le bon Compte AWS. • `aws_region` — Spécifiez le bon Région AWS. • `s3BucketName` — Spécifiez le compartiment Amazon S3 qui doit contenir les CloudFormation modèles. • Le fichier de flux de travail nécessite deux rôles IAM en entrée : • `LaunchConstraintRole` - Le rôle IAM qui joue le AWS Service Catalog rôle lorsqu'un utilisateur final lance, met à jour ou met fin à un produit.	DevOps ingénieur

Tâche	Description	Compétences requises
	• `PrincipalArn` - Le nom de ressource Amazon (ARN) du principal (utilisateur, rôle ou groupe IAM) qui sera associé au portefeuille de services Catalog. Dans l'`Principal Type` affirmative`IAM`, la valeur prise en charge est un nom de ressource IAM Amazon (ARN) entièrement défini. Si tel `PrincipalType` est le cas`IAM_PATTERN`, la valeur prise `AccountID` en charge est un ARN IAM sans `arn:partition:iam::resource-type/resource-id`	

Valider le déploiement

Tâche	Description	Compétences requises
Validez les ressources du Service Catalog.	Pour valider les ressources du Service Catalog, procédez comme suit : 1. Connectez-vous au AWS Management Console Compte AWS, et vérifiez	AWS DevOps

Tâche	Description	Compétences requises
	que c' Région AWS est correct. 2. Accédez à un portefeuille AWS Service Cataloget validez qu'un portefeuille est présent sous Administration, Portefeuilles. 3. Choisissez le portefeuille et validez les informations dans les onglets Produits, Contraintes et Accès.	

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez la CloudFormation pile.	Pour supprimer la CloudFormation pile, procédez comme suit : 1. Ouvrez la AWS CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation. 2. Dans la barre de navigation en haut de l'écran, choisissez l' Région AWS emplacement de la pile. 3. Sur la page Stacks, choisissez la pile que vous souhaitez supprimer. La pile doit être en cours d’exécution.	DevOps ingénieur, administrateur AWS

Tâche	Description	Compétences requises
	4. Dans le volet des détails de la pile, choisissez Supprimer. 5. Sélectionnez Supprimer la pile lorsque vous y êtes invité. Pour plus d'informations, voir Supprimer une pile de la CloudFormation console dans la CloudFormation documentation	

Résolution des problèmes

Problème	Solution

`e2e-test`
 	
`Can't find 'action.yml', 'action.yaml' or 'Dockerfile' under '*/home/runner/work/service-catalog-with-github-actions/service-catalog-with-github-actions`
 	
`Did you forget to run actions/checkout before running your local action?`
	Pour vous assurer que les paramètres de référentiel corrects sont activés, procédez comme suit :
	1. Accédez au référentiel Github, onglet Paramètres.
	2. Choisissez Actions, Général dans le menu de gauche
	3. Accédez à la section Accès et sélectionnez l'option Accessible depuis les référentiels de l'organisation « XXX ».

Ressources connexes

AWS documentation

- Présentation du Service Catalog

Autres ressources

- À propos des événements qui déclenchent des flux de travail (GitHub documentation)
- Réutilisation des flux de travail (GitHub documentation)

Informations supplémentaires

Pour voir des captures d'écran liées aux Epics, rendez-vous dans le dossier Images du GitHub dépôt de ce modèle. Les captures d'écran suivantes sont disponibles :

- AWS Service Catalog portefeuille, section de l'administration
- AWS Service Catalog produit, section Administration
- AWS Service Catalog produit, section Utilisateur/Approvisionnement

Fournissez des rôles IAM avec le moindre privilège en déployant une solution de distribution automatique de rôles

Créée par Benjamin Morris (AWS), Aman Kaur Gandhi (AWS), Tchad Moon (AWS) et Nima Fotouhi (AWS)

Récapitulatif

Les autorisations de rôle AWS Identity and Access Management surdimensionnées (IAM) pour les pipelines peuvent présenter des risques inutiles pour une organisation. Les développeurs accordent parfois des autorisations étendues pendant le développement, mais négligent de limiter les autorisations après avoir résolu le problème avec leur code. Cela pose un problème lorsque des rôles puissants sont présents sans aucun besoin commercial et n'ont peut-être jamais été revus par un ingénieur en sécurité.

Ce modèle offre une solution à ce problème : le distributeur automatique de rôles (RVM). À l'aide d'un modèle de déploiement sécurisé et centralisé, le RVM montre comment fournir des rôles IAM avec le moindre privilège pour les pipelines de GitHub référentiels individuels avec un minimum d'efforts de la part des développeurs. Le RVM étant une solution centrale, vous pouvez configurer vos équipes de sécurité en tant que réviseurs requis pour approuver les modifications. Cette approche permet à la sécurité de rejeter les demandes de rôle de pipeline avec des autorisations excessives.

Le RVM prend le code Terraform en entrée et génère des rôles IAM prêts pour le pipeline en sortie. Les entrées requises sont l' Compte AWS ID, le nom du GitHub référentiel et la politique d'autorisation. Le RVM utilise ces entrées pour créer la politique de confiance et la politique d'autorisation du rôle. La politique de confiance qui en résulte permet au GitHub référentiel spécifié d'assumer le rôle et de l'utiliser pour les opérations de pipeline.

Le RVM utilise un rôle IAM (configuré lors du bootstrap). Ce rôle est autorisé à assumer un rôle role-provisioning-role dans chaque compte de l'organisation. Le rôle est configuré via AWS Control Tower Account Factory for Terraform (AFT) ou. AWS CloudFormation StackSets Ce role-provisioning-roles sont les rôles qui créent réellement les rôles de pipeline pour les développeurs.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.

- GitHub Organisation utilisée pour déployer une infrastructure sous forme de code (IaC) par le biais d' GitHub actions. (ne GitHub Enterprise/Premium/Ultimate sont pas obligatoires.)
- Un AWS environnement multi-comptes. Il n'est pas nécessaire d'en faire partie AWS Organizations.
- Mécanisme permettant de déployer un rôle IAM dans tous les domaines Comptes AWS (par exemple, AFT ou CloudFormation StackSets).
- Terraform version 1.3 ou ultérieure installée et configurée.
- Terraform AWS Provider version 4 ou ultérieure installée et configurée.

Limites

- Le code de ce modèle est spécifique à GitHub Actions et Terraform. Cependant, les concepts généraux du modèle peuvent être réutilisés dans d'autres cadres d'intégration et de livraison continues (CI/CD).
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant illustre le flux de travail pour ce modèle.

Le flux de travail pour l'utilisation typique du distributeur automatique de rôles comprend les étapes suivantes :

1. Un développeur envoie du code contenant du code Terraform pour un rôle IAM récemment demandé vers le référentiel RVM. GitHub Cette action déclenche le pipeline d' GitHub actions RVM.
2. Le pipeline utilise une politique de confiance OpenID Connect (OIDC) pour assumer le rôle d'hypothèse de rôle du RVM.
3. Au fur et à mesure que le pipeline RVM s'exécute, il assume le rôle de flux de travail RVM dans le compte dans lequel il fournit le nouveau rôle IAM du développeur. (Le rôle de flux de travail RVM a été fourni à l'aide d'AFT ou CloudFormation StackSets.)

4. Le RVM crée le rôle IAM du développeur avec les autorisations et la confiance appropriées, afin que le rôle puisse être assumé par d'autres pipelines d'applications.
5. Les développeurs d'applications peuvent configurer leurs pipelines d'applications pour assumer ce rôle fourni par RVM.

Le rôle créé inclut les autorisations demandées par le développeur et une `ReadOnlyAccess` politique. Le rôle n'est assumé que par les pipelines qui s'exécutent sur la `main` branche du référentiel spécifié par le développeur. Cette approche permet de garantir que la protection et les révisions des succursales peuvent être nécessaires pour utiliser le rôle.

Automatisation et mise à l'échelle

Les autorisations de moindre privilège nécessitent une attention particulière aux détails pour chaque rôle fourni. Ce modèle réduit la complexité requise pour créer ces rôles, permettant aux développeurs de créer les rôles dont ils ont besoin sans trop d'apprentissage ou d'efforts supplémentaires.

Outils

Services AWS

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

Autres outils

- Git est un système de contrôle de version distribué et open source. Cela inclut la possibilité de créer un compte d'organisation.
- GitHub Actions est une plateforme d'intégration et de livraison continues (CI/CD) étroitement intégrée aux GitHub référentiels. Vous pouvez utiliser GitHub les actions pour automatiser votre pipeline de création, de test et de déploiement.
- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub role-vending-machineréférentiel.

Bonnes pratiques

- Facilitez le bon chemin et compliquez le mauvais chemin — Faites en sorte qu'il soit facile de faire le bon choix. Si les développeurs rencontrent des difficultés avec le processus de provisionnement du RVM, ils peuvent tenter de créer des rôles par d'autres moyens, ce qui mine la nature centrale du RVM. Assurez-vous que votre équipe de sécurité fournit des conseils clairs sur la manière d'utiliser le RVM de manière sûre et efficace.

  Vous devez également empêcher les développeurs de faire le mauvais choix. Utilisez des politiques de contrôle des services (SCPs) ou des limites d'autorisation pour limiter les rôles qui peuvent créer d'autres rôles. Cette approche peut aider à limiter la création de rôles au seul RVM et à d'autres sources fiables.
- Donnez de bons exemples — Inévitablement, certains développeurs adapteront les rôles existants dans le référentiel RVM en tant que modèles informels pour accorder des autorisations à leurs nouveaux rôles. Si vous disposez d'exemples d'autorisations minimales à partir desquels ils peuvent copier, cela peut réduire le risque que les développeurs demandent des autorisations étendues et comportant de nombreux caractères génériques. Si vous commencez avec des rôles très autorisés contenant de nombreux jokers, ce problème peut se multiplier au fil du temps.
- Utilisez des conventions et conditions de dénomination : même si un développeur ne connaît pas tous les noms de ressources que son application va créer, il doit tout de même limiter les autorisations relatives aux rôles en utilisant une convention de dénomination. Par exemple, s'ils créent des compartiments Amazon S3, la valeur de leur clé de ressource peut sembler `arn:aws:s3:::myorg-myapp-dev-*` telle que leur rôle ne dispose pas d'autorisations autres que les compartiments portant ce nom. L'application de la convention de dénomination par le biais d'une politique IAM présente l'avantage supplémentaire d'améliorer le respect de la convention de dénomination. Cette amélioration est due au fait que la création de ressources non correspondantes ne sera pas autorisée.
- Exiger des révisions par pull request (PR) — L'avantage de la solution RVM réside dans le fait qu'elle crée un emplacement central où les nouveaux rôles du pipeline peuvent être examinés. Cependant, cette conception n'est utile que s'il existe des garde-fous qui permettent de garantir que le code sécurisé et de haute qualité est transmis au RVM. Protégez les branches utilisées pour déployer du code (par exemple,`main`) contre les envois directs et exigez des approbations pour toute demande de fusion qui les cible.
- Configurer les rôles en lecture seule : par défaut, le RVM fournit une `readonly` version de chaque rôle demandé. Ce rôle peut être utilisé dans les pipelines CI/CD qui n'écrivent pas de données,

tels qu'un flux de travail de `terraform plan` pipeline. Cette approche permet d'éviter les modifications indésirables en cas de mauvais comportement d'un flux de travail en lecture seule.

Par défaut, la `ReadOnlyAccess` politique AWS gérée est attachée à la fois aux rôles en lecture seule et aux rôles en lecture-écriture. Cette politique réduit le besoin d'itérations lors de la détermination des autorisations requises, mais elle peut être trop permissive pour certaines organisations. Si vous le souhaitez, vous pouvez supprimer la politique du code Terraform.

- Accorder des autorisations minimales — Suivez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Préparer l'environnement

Tâche	Description	Compétences requises
Copiez le référentiel d'échantillons dans votre GitHub organisation.	Clonez le référentiel de ce modèle ou associez-le à votre GitHub organisation afin de l'adapter à vos besoins. • Si vous choisissez de cloner ce dépôt, vous pouvez utiliser la commande suivante : `git clone https://github.com/aws-samples/role-vending-machine` • Si vous choisissez de transférer le référentiel à votre GitHub organisation, vous pouvez utiliser la commande suivante :	DevOps ingénieur

Tâche	Description	Compétences requises
	`gh repo fork aws-samples/role-vending-machine --org YOUR_ORGANIZATION_NAME`	
Déterminez le Compte AWS pour le RVM.	Déterminez le déploiement de l'infrastructure Compte AWS à utiliser pour le RVM. N'utilisez pas le compte de gestion ou le compte root.	Architecte du cloud

Tâche	Description	Compétences requises
(Facultatif) Autorisez la création des pipelines de l'organisation PRs.	**Note** Cette étape n'est nécessaire que si vous souhaitez autoriser la création du `generate_providers_and_account_vars` flux de travail PRs. Pour autoriser la création de pipelines de votre organisation PRs, procédez comme suit : 1. Accédez à `https://github.com/organizations/YOUR_ORG/settings/actions` . 2. Sélectionnez Autoriser GitHub les actions pour créer et approuver des pull requests. Pour plus d'informations, consultez la section Gestion GitHub des paramètres des actions pour un référentiel dans la GitHub documentation.	DevOps ingénieur

Tâche	Description	Compétences requises
Accordez des autorisations en lecture seule au compte RVM.	Créez une politique de délégation dans votre compte de gestion qui accorde à votre compte RVM des autorisations en lecture seule. Cela permet à vos GitHub flux de travail RVM d'extraire dynamique ment une liste des comptes de votre AWS organisat ion lorsque le `generate_ providers_and_acco unt_vars.py` script s'exécute. Utilisez le code suivant et remplacez-le `<YOUR RVM Account ID>` par l' Compte AWS ID que vous avez sélectionné à l'étape 2 : `{ "Version": "2012-10- 17", "Statement": [ { "Sid": "Statemen t", "Effect": "Allow", "Principal": { "AWS": "arn:aws: iam::<YOUR RVM Account ID>:root" }, "Action": [ "organiza tions:ListAccounts",`	Administrateur du cloud

Tâche	Description	Compétences requises
	"organizations:DescribeOrganization", "organizations:DescribeOrganizationalUnit", "organizations:ListRoots", "organizations:ListAWSServiceAccessForOrganization", "organizations:ListDelegatedAdministrators"], "Resource": "*" }] }	

Tâche	Description	Compétences requises
Mettez à jour les valeurs par défaut à partir de l'exemple de dépôt.	Pour configurer le RVM afin qu'il fonctionne dans votre environnement spécifiqu e Région AWS, procédez comme suit : 1. Fichiers de mise à jour `scripts/generate_p roviders_and_accou nt_vars.py` et autres (tels que le `bootstrap` dossier) correspondant à la région dans laquelle vous opérez. 2. Mettez à jour le `.github/w orkflows/.env` fichier avec l' Compte AWS ID, la région et toute autre variable que vous souhaitez spécifier.	DevOps ingénieur

Initialisation de l'infrastructure

Tâche	Description	Compétences requises
Démarrez le dépôt RVM.	Cette étape est nécessair e pour créer les rôles OIDC Trust et IAM utilisés par le pipeline RVM lui-même, afin qu'il puisse commencer à fonctionner et à vendre d'autres rôles.	DevOps ingénieur

Tâche	Description	Compétences requises
	Dans le contexte de votre compte RVM, exécutez manuellement une `terraform apply` commande depuis le `scripts/bootstrap` répertoire. Fournissez toutes les valeurs requises sur la base de la documentation des variables.	

Configuration des opérations

Tâche	Description	Compétences requises
Déployez les `github-workflow-rvm-readonly` rôles `github-workflow-rvm` et sur tous les comptes.	Choisissez une méthode de déploiement conforme aux pratiques de votre organisation, telle que AFT ou StackSets. Utilisez cette méthode pour déployer les deux rôles IAM du `scripts/assumed_role/main.tf` fichier (noms par défaut `github-workflow-rvm` et`github-workflow-rvm-readonly`) sur chaque compte sur lequel vous souhaitez que le RVM puisse créer des rôles de pipeline. Ces rôles IAM ont des politiques de confiance qui permettent au rôle d'acceptation de rôle du compte RVM	Administrateur AWS

Tâche	Description	Compétences requises
	(ou son `readonly` équivalent) de l'assumer. Les rôles sont également soumis à des politiques d'autorisation IAM qui leur permettent de lire et d'écrire (sauf en utilisant le `readonly` rôle) les rôles correspondants`github-workflow-role-*` .	
Exécutez le `generate_providers_and_account_vars` flux de travail.	Pour configurer votre RVM afin qu'elle soit prête à créer des rôles de pipeline, procédez comme suit : 1. Exécutez le `generate_providers_and_account_vars` flux de travail à l'aide de workflow_dispatch. 2. Fusionnez le PR créé par le flux de travail. Une fois le flux de travail terminé, le RVM est prêt à : • Acceptez les demandes de nouveaux rôles dans le pipeline. • Créez des rôles en lecture seule ou en lecture-écriture selon les besoins. • Déployez les rôles sur le site spécifié Comptes AWS.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
J'ai créé un rôle à l'aide du RVM, mais je ne suis GitHub pas en mesure de l'assumer.	Vérifiez que le nom du GitHub dépôt correspond au nom fourni au `github_workflow_roles` module. Les rôles sont définis de manière à ce qu'un seul référentiel puisse les assumer. De même, vérifiez que la branche utilisée dans le GitHub pipeline correspond au nom de la branche fournie au `github_workflow_roles` module. Généralement, les rôles créés par RVM dotés d'autorisations d'écriture ne peuvent être utilisés que par les flux de travail limités à la `main` branche (c'est-à-dire les déploiements provenant de). `main`
Mon rôle en lecture seule ne parvient pas à exécuter son pipeline car il n'est pas autorisé à lire une ressource spécifique.	Bien que la `ReadOnlyAccess` politique fournisse des autorisations étendues en lecture seule, elle ne comporte pas certaines actions de lecture (par exemple, certaines AWS Security Hub actions). Vous pouvez ajouter des autorisations d'action spécifiques en utilisant le `inline_policy_readonly` paramètre du `github-workflow-roles` module.

Ressources connexes

- Bonnes pratiques d'utilisation AWS CloudFormation StackSets
- Organisation de votre AWS environnement à l'aide de plusieurs comptes
- Présentation de AWS Control Tower Account Factory pour Terraform (AFT)
- Bonnes pratiques en matière de politiques

Informations supplémentaires

Utilisation d' GitHub environnements

GitHub les environnements constituent une approche alternative aux restrictions d'accès aux rôles basées sur les branches. Si vous préférez utiliser un GitHub environnement, voici un exemple de syntaxe pour une condition supplémentaire dans la politique de confiance IAM. Cette syntaxe indique que le rôle ne peut être utilisé que lorsque l' GitHub action est exécutée dans l'`Production`environnement.

```
"StringLike": {
    "token.actions.githubusercontent.com:sub": "repo:octo-org/octo-
repo:environment:Production"
}
```

L'exemple de syntaxe utilise les valeurs d'espace réservé suivantes :

- `octo-org`est le nom GitHub de l'organisation.
- `octo-repo`est le nom du dépôt.
- `Production`est le nom de GitHub l'environnement spécifique.

Publier CloudWatch les statistiques Amazon dans un fichier CSV

Créée par Abdullahi Olaoye (AWS)

Récapitulatif

Ce modèle utilise un script Python pour récupérer les CloudWatch métriques Amazon et pour convertir les informations des métriques dans un fichier de valeurs séparées par des virgules (CSV) pour une meilleure lisibilité. Le script utilise le service AWS dont les métriques doivent être récupérées comme argument obligatoire. Vous pouvez spécifier la région AWS et le profil d'identification AWS en tant qu'arguments facultatifs. Si vous ne spécifiez pas ces arguments, le script utilise la région et le profil par défaut configurés pour le poste de travail sur lequel le script est exécuté. Une fois le script exécuté, il génère et stocke un fichier CSV dans le même répertoire.

Consultez la section Pièces jointes pour le script et les fichiers associés fournis avec ce modèle.

Conditions préalables et limitations

Prérequis

- Python 3.x
- Interface de ligne de commande AWS (AWS CLI)

Limites

Le script prend actuellement en charge les services AWS suivants :

- AWS Lambda
- Amazon Elastic Compute Cloud (Amazon EC2)
  - Par défaut, le script ne collecte pas les métriques de volume Amazon Elastic Block Store (Amazon EBS). Pour collecter les métriques Amazon EBS, vous devez modifier le `metrics.yaml` fichier joint.
- Amazon Relational Database Service (Amazon RDS)
  - Toutefois, le script ne prend pas en charge Amazon Aurora.
- Application Load Balancer
- Network Load Balancer
- Amazon API Gateway

Outils

- Amazon CloudWatch est un service de surveillance conçu pour les DevOps ingénieurs, les développeurs, les ingénieurs de fiabilité des sites (SREs) et les responsables informatiques. CloudWatch fournit des données et des informations exploitables pour vous aider à surveiller vos applications, à répondre aux changements de performances à l'échelle du système, à optimiser l'utilisation des ressources et à obtenir une vue unifiée de l'état de fonctionnement. CloudWatch collecte des données opérationnelles et de surveillance sous forme de journaux, de mesures et d'événements, et fournit une vue unifiée des ressources, des applications et des services AWS exécutés sur AWS et sur des serveurs sur site.

Épopées

Installation et configuration des prérequis

Tâche	Description	Compétences requises
Installez les prérequis.	Exécutez la commande suivante : `$ pip3 install -r requirements.txt`	Developer
Configuration de l'AWS CLI.	Exécutez la commande suivante : `$ aws configure`	Developer

Configuration du script Python

Tâche	Description	Compétences requises
Ouvrez le script.	Pour modifier la configuration par défaut du script, ouvrez`metrics.yaml` .	Developer

Tâche	Description	Compétences requises
Définissez la période du script.	Il s'agit de la période à récupérer. La période par défaut est de 5 minutes (300 secondes). Vous pouvez modifier la période, mais tenez compte des limites suivantes : • Si la valeur des heures que vous spécifiez se situe entre 3 heures et 15 jours, utilisez un multiple de 60 secondes (1 minute) pour la période. • Si la valeur des heures que vous spécifiez se situe entre 15 heures et 63 jours, utilisez un multiple de 300 secondes (5 minutes) pour la période. • Si la valeur des heures que vous spécifiez est supérieure à 63 jours, utilisez un multiple de 3 600 secondes (1 heure) pour la période. Dans le cas contraire, l'opération d'API ne renverra aucun point de données.	Developer

Tâche	Description	Compétences requises
Définissez les heures du script.	Cette valeur indique le nombre d'heures de métriques que vous souhaitez récupérer . La valeur par défaut est 1 heure. Pour récupérer plusieurs jours de métriques, indiquez la valeur en heures. Par exemple, pour 2 jours, spécifiez 48.	Developer
Modifiez les valeurs statistiq ues du script.	(Facultatif) La valeur des statistiques globales est`Average`, qui est utilisée lors de l'extraction de métriques auxquelles aucune valeur statistique spécifique n'est attribuée. Le script prend en charge les valeurs statistiq ues `MaximumSampleCount` , et`Sum`.	Developer

Exécutez le script Python

Tâche	Description	Compétences requises
Exécutez le script.	Utilisez la commande suivante : `$ python3 cwreport.py <service>` Pour consulter la liste des valeurs de service, des options `region` et `profile`	Developer

Tâche	Description	Compétences requises
	des paramètres, exécutez la commande suivante : `$ python3 cwreport.py -h` Pour plus d'informations sur les paramètres facultatifs, consultez la section Informations supplémentaires.	

Ressources connexes

- Configuration de l'AWS CLI
- Utilisation des CloudWatch métriques Amazon
- CloudWatch Documentation Amazon
- EC2 CloudWatch Métriques
- Métriques AWS Lambda
- Métriques Amazon RDS
- Mesures relatives à l'Application Load Balancer
- Métriques du Network Load Balancer
- Métriques Amazon API Gateway

Informations supplémentaires

Utilisation des scripts

```
$ python3 cwreport.py -h
```

Exemple de syntaxe

```
python3 cwreport.py <service> <--region=Optional Region> <--profile=Optional credential
 profile>
```

Paramètres

- service (obligatoire) – Le service sur lequel vous souhaitez exécuter le script. Le script prend actuellement en charge les services suivants : AWS Lambda, Amazon, EC2 Amazon RDS, Application Load Balancer, Network Load Balancer et API Gateway.
- région (facultatif) – La région AWS à partir de laquelle récupérer les métriques. La région par défaut est`ap-southeast-1`.
- profil (facultatif) – Le profil nommé à utiliser dans l'interface de ligne de commande AWS. Si ce paramètre n'est pas spécifié, le profil d'identification configuré par défaut est utilisé.

Exemples

- Pour utiliser la région par défaut `ap-southeast-1` et les informations d'identification configurées par défaut pour récupérer EC2 les métriques Amazon : `$ python3 cwreport.py ec2`
- Pour spécifier une région et récupérer les métriques d'API Gateway, procédez comme suit : `$ python3 cwreport.py apigateway --region us-east-1`
- Pour spécifier un profil AWS et récupérer les EC2 métriques Amazon, procédez comme suit : `$ python3 cwreport.py ec2 --profile testprofile`
- Pour spécifier à la fois la région et le profil pour récupérer EC2 les métriques Amazon : `$ python3 cwreport.py ec2 --region us-east-1 --profile testprofile`

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Supprimez EC2 les entrées Amazon Comptes AWSAWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation

Créée par le Dr Rahul Sharad Gaikwad (AWS) et Tamilselvan (AWS)

Récapitulatif

Active Directory (AD) est un outil de script Microsoft qui gère les informations de domaine et les interactions des utilisateurs avec les services réseau. Il est largement utilisé par les fournisseurs de services gérés (MSPs) pour gérer les informations d'identification et les autorisations d'accès des employés. Étant donné que les attaquants publicitaires peuvent utiliser des comptes inactifs pour tenter de pirater une organisation, il est important de trouver les comptes inactifs et de les désactiver dans le cadre d'un programme de maintenance de routine. Avec AWS Directory Service for Microsoft Active Directory, vous pouvez exécuter Microsoft Active Directory en tant que service géré. Ce modèle peut vous aider à configurer AWS Lambda l'automatisation pour trouver et supprimer rapidement les comptes inactifs.

Si les scénarios suivants s'appliquent à votre organisation, ce modèle peut vous aider :

- Gestion centralisée d'AD : si votre organisation en possède plusieurs Comptes AWS, chacune avec son propre déploiement AD, il peut être difficile de gérer les comptes utilisateurs et les autorisations d'accès de manière cohérente sur tous les comptes. Avec une solution de nettoyage AD multicomptes, vous pouvez désactiver ou supprimer les comptes inactifs de toutes les instances AD de manière centralisée.
- Restructuration ou migration d'AD : si votre organisation prévoit de restructurer ou de migrer son déploiement AD, une solution de nettoyage AD multi-comptes peut vous aider à préparer l'environnement. La solution peut vous aider à supprimer les comptes inutiles ou inactifs, à simplifier le processus de migration et à réduire les conflits ou problèmes potentiels.

Lorsque vous utilisez ce modèle, vous pouvez bénéficier des avantages suivants :

- Améliorez les performances des bases de données et des serveurs, et corrigez les failles de sécurité liées aux comptes inactifs.
- Si votre serveur AD est hébergé dans le cloud, la suppression des comptes inactifs peut également réduire les coûts de stockage tout en améliorant les performances. Vos factures mensuelles peuvent diminuer car les frais de bande passante et de ressources informatiques peuvent tous deux diminuer.

- Gardez les attaquants potentiels à distance grâce à un Active Directory propre.

Conditions préalables et limitations

Prérequis

- Un parent actif Compte AWS et un ou plusieurs comptes enfants. Dans ce modèle, un compte parent est l'endroit où Active Directory est créé. Les comptes enfants hébergent des serveurs Windows et sont joints via le compte parent Active Directory.
- Git est installé et configuré sur un poste de travail local.
- Terraform installé et configuré sur un poste de travail local.
- AWS Managed Microsoft AD répertoire configuré dans le compte parent et partagé avec tous les comptes enfants. Pour plus de détails, voir Tutoriel : Partage de votre AWS Managed Microsoft AD répertoire pour une jonction de EC2 domaine fluide dans le Guide d'AWS Directory Service administration.
- Une connexion d'appairage au cloud privé virtuel (VPC) ou une AWS Transit Gateway connexion disponible entre le VPC de AWS Directory Service (compte parent) et le VPC des instances Amazon Elastic Compute Cloud (EC2Amazon) (comptes enfants). Pour plus de détails, consultez la section Configurer une connexion d'appairage VPC entre le propriétaire de l'annuaire et le compte du consommateur de l'annuaire dans le AWS Directory Service Guide d'administration.
- Une machine Windows configurée avec le `EC2WindowsUserdata` script sur tous les comptes parent et enfant. Le fichier de script est disponible à la racine du référentiel de code de ce modèle.
- Un rôle entre comptes AWS Identity and Access Management (IAM) disponible sur chaque compte enfant configuré avec une politique de confiance autorisant l'utilisation d'une AWS Lambda fonction du compte parent. Pour plus d'informations, consultez la section Envoi et réception d'événements entre Amazon Comptes AWS EventBridge dans le guide de EventBridge l'utilisateur Amazon.
- Les valeurs secrètes suivantes sont disponibles dans le AWS Systems Manager Parameter Store du compte parent :
  - `domainJoinUser`— Nom d'utilisateur du service d'annuaire
  - `domainJoinPassword`— Mot de passe du service d'annuaire

  Pour plus d'informations sur les secrets, voir Création d'un AWS Secrets Manager secret dans le Guide de AWS Secrets Manager l'utilisateur.

Limites

- La création d'une ressource dans un compte enfant n'est pas automatisée avec Terraform. Vous devez créer les ressources suivantes manuellement à l'aide de AWS Management Console :
  - EventBridge Règle Amazon pour envoyer les événements de EC2 résiliation d'Amazon au compte parent
  - Création de rôles EC2 entre comptes Amazon dans le compte enfant avec politique de confiance
  - Peering VPC ou connexion Transit Gateway
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Terraform version 1.1.9 ou ultérieure
- Terraform AWS Provider version 3.0 ou supérieure

Architecture

Le schéma suivant montre l'architecture de haut niveau de la solution.

Le schéma d'architecture illustre le processus suivant :

1. Dans les comptes enfants, la EventBridge règle collecte tous les événements de EC2 résiliation d'Amazon. La règle envoie les EventBridge événements présents dans le compte parent.
2. À partir du compte parent, EventBridge collecte tous les événements et contient la règle permettant de déclencher la fonction Lambda. `ADcleanup-Lambda`
3. Le compte parent reçoit tous les événements de résiliation du compte parent ou enfant et déclenche la fonction Lambda.
4. La fonction Lambda appelle les groupes Amazon EC2 Auto Scaling à l'aide du module Python boto et obtient l'ID d'instance aléatoire. L'ID d'instance est utilisé pour exécuter les commandes de Systems Manager.
5. La fonction Lambda effectue un autre appel à Amazon à EC2 l'aide du module boto. La fonction Lambda obtient les adresses IP privées des serveurs Windows en cours d'exécution et les stocke

dans une variable temporaire. Dans les étapes 5.1 et 5.2, les EC2 instances Windows en cours d'exécution sont collectées à partir de comptes enfants.

6. La fonction Lambda lance un nouvel appel à Systems Manager pour obtenir les informations de l'ordinateur auquel il est connecté. AWS Directory Service
7. Un AWS Systems Manager document permet d'exécuter la PowerShell commande sur les serveurs Amazon EC2 Windows pour obtenir les adresses IP privées des ordinateurs connectés à AD. (Le document Systems Manager utilise l'ID d'instance obtenu à l'étape 4.)
8. Le nom d'utilisateur et les mots de passe du domaine AD sont stockés dans le AWS Systems Manager Parameter Store. AWS Lambda et Systems Manager appellent Parameter Store et obtiennent les valeurs du nom d'utilisateur et du mot de passe à utiliser pour se connecter à AD.
9. À l'aide du document Systems Manager, le PowerShell script est exécuté sur le serveur Amazon EC2 Windows à l'aide de l'identifiant d'instance obtenu précédemment à l'étape 4.
10. Amazon EC2 se connecte AWS Directory Service à l'aide de PowerShell commandes et supprime les ordinateurs inutilisés ou inactifs.

Outils

AWS services

- AWS Directory Servicepropose plusieurs manières d'utiliser Microsoft Active Directory (AD) avec d'autres, Services AWS comme Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) pour SQL Server et FSx Amazon pour Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermet à vos charges de travail et à vos AWS ressources sensibles aux annuaires d'utiliser Microsoft Active Directory dans le. AWS Cloud
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, des AWS Lambda fonctions, des points de terminaison d'invocation HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser. Avec IAM, vous pouvez spécifier qui ou quoi peut accéder aux services et aux ressources AWS, gérer de manière

centralisée les autorisations détaillées et analyser les accès pour affiner les autorisations entre elles. AWS

- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.
- AWS Systems Manager les documents définissent les actions que Systems Manager exécute sur vos instances gérées. Systems Manager inclut plus d'une centaine de documents préconfigurés que vous pouvez utiliser en spécifiant des paramètres lors de l'exécution.
- AWS Systems Manager Parameter Store est une fonctionnalité AWS Systems Manager et fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub aws-lambda-ad-cleanup-terraform-samples.

Bonnes pratiques

- Joignez automatiquement des domaines.Lorsque vous lancez une instance Windows destinée à faire partie d'un AWS Directory Service domaine, rejoignez le domaine pendant le processus de création de l'instance au lieu de l'ajouter manuellement ultérieurement. Pour rejoindre automatiquement un domaine, sélectionnez le répertoire approprié dans la liste déroulante des répertoires de jointure de domaines lors du lancement d'une nouvelle instance. Pour plus

de détails, consultez la section Joindre sans difficulté une instance Amazon EC2 Windows à votre AWS Managed Microsoft AD Active Directory dans le guide d'AWS Directory Service administration.

- Supprimez les comptes inutilisés.Il est courant de trouver dans AD des comptes qui n'ont jamais été utilisés. Tout comme les comptes désactivés ou inactifs qui restent dans le système, les comptes non utilisés négligés peuvent ralentir votre système publicitaire ou rendre votre organisation vulnérable aux violations de données.
- Automatisez les nettoyages d'Active Directory.Pour atténuer les risques de sécurité et empêcher les comptes obsolètes d'affecter les performances d'AD, effectuez des nettoyages AD à intervalles réguliers. Vous pouvez effectuer la plupart des tâches de gestion et de nettoyage d'AD en écrivant des scripts. Les tâches incluent par exemple la suppression de comptes désactivés et inactifs, la suppression de groupes vides et inactifs et la localisation de comptes utilisateurs et de mots de passe expirés.

Épopées

Configurer des comptes pour enfants

Tâche	Description	Compétences requises
Créez un rôle multicompte dans le compte enfant.	Pour créer un rôle multicompte dans un compte enfant, procédez comme suit : 1. Pour chaque compte enfant, créez un rôle nommé à `ec2crossaccountrole` l'aide de la politique gérée nomméeAmazonEC2 `ReadOnlyAccess` . (Pour plus d'informations, consultez la section Création d'un rôle à l'aide de politiques de confiance	DevOps ingénieur

Tâche	Description	Compétences requises
	personnalisées dans la documentation IAM.) 2. Dans la section Politique de confiance personnalisée, ajoutez le code suivant : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "ec2.amazonaws.com" }, "Action": "sts:AssumeRole" }, { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::${Parentaccountid}:role/ADcleanuprole" }, "Action": "sts:AssumeRole" } ] }`	

Tâche	Description	Compétences requises
Créez une règle d'événement dans le compte enfant.	Pour créer une EventBridge règle pour chaque compte enfant, procédez comme suit : 1. Connectez-vous à l'enfant Compte AWS, puis ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/. 2. Dans le volet de navigation, choisissez Règles. 3. Choisissez Créer une règle. 4. Entrez un nom et, éventuellement, une description pour la règle. 5. Pour Event Bus, sélectionnez le bus d'événements par défaut AWS. 6. Pour Type de règle, choisissez Règle avec un modèle d'événement. 7. Choisissez Suivant. 8. Pour Modèle d'événement, collez le code suivant : `{ "source": ["aws.ec2"], "detail-type": ["EC2 Instance State-change Notification"], "detail": {`	DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>"state": ["terminated"]
	}
	}</pre>
	9. Choisissez Suivant.
	10. Pour le type de cible, choisissez Event bus dans un autre compte ou une autre région.Pour Event Bus comme cible, entrez le bus d'événements Amazon Resource Name (ARN) pour le compte parent.
	11. Pour Rôle d'exécution, choisissez Créer un nouveau rôle pour cette ressource spécifique.
	12. Choisissez Suivant pour consulter les détails de la nouvelle règle, puis choisissez Créer.
	
	Pour plus de détails, consultez la section Création de règles qui réagissent aux événements survenus sur Amazon EventBridge dans le guide de EventBridge l'utilisateur Amazon.	

Tâche	Description	Compétences requises
Créez une EC2 instance et rejoignez-la à AD.	Pour créer une EC2 instance pour Windows, procédez comme suit : 1. Utilisez le `EC2WindowsUserdata` script disponible dans le référentiel de code de ce modèle. 2. Dans le script de données utilisateur, modifiez le code suivant pour utiliser `Directory service addresses` les valeurs du compte parent : `set-DnsClientServerAddress -InterfaceIndex 6 -ServerAddresses $(Directory service addresses)`	DevOps ingénieur

Configuration du poste de travail local

Tâche	Description	Compétences requises
Créez un dossier de projet et ajoutez les fichiers.	Pour cloner le référentiel et créer un dossier de projet, procédez comme suit : 1. Ouvrez le GitHub référentiel de ce modèle. 2. Cliquez sur le bouton Code pour voir les options	DevOps ingénieur

Tâche	Description	Compétences requises

	de clonage dans la liste déroulante Cloner.
	3. Dans l'onglet HTTPS, copiez l'URL fournie dans Clone à l'aide de l'URL Web.
	4. Créez un dossier sur votre machine et nommez-le avec le nom de votre projet.
	5. Ouvrez un terminal sur votre ordinateur local et accédez à ce dossier.
	6. Pour cloner le dépôt git, utilisez la commande suivante.
	`git clone <repository-URL>.git`
	7. Une fois le dépôt cloné, utilisez la commande suivante pour accéder au répertoire cloné.
	`cd <directory name>/terraform-aws-lambda-ad-cleanup/multiple-account-cleanup`
	8. Dans le référentiel cloné, ouvrez ce projet dans un environnement de développement intégré (IDE) de votre choix.	

Tâche	Description	Compétences requises
Créez le `adcleanup.zip` fichier.	Pour compresser le `lambda_function.py` fichier, exécutez la commande suivante : `zip -r adcleanup.zip lambda_function.py`	DevOps ingénieur

Provisionner l'architecture cible à l'aide de la configuration Terraform

Tâche	Description	Compétences requises
Fournissez des valeurs pour les variables Terraform.	Pour le compte enfant, fournissez les valeurs des `arn` variables suivantes sous forme de chaînes dans le `terraform.tfvars` fichier : • `lambda_env_cross_role_arn` • `child_account_cross_role_arn`	DevOps ingénieur
Initialisez la configuration Terraform.	Pour initialiser votre répertoire de travail contenant les fichiers Terraform, exécutez la commande suivante : `terraform init`	DevOps ingénieur
Prévisualisez les modifications.	Vous pouvez prévisualiser les modifications que Terraform apportera à l'infrastructure avant que celle-ci ne soit déployée. Pour valider que	DevOps ingénieur

Tâche	Description	Compétences requises
	Terraform apportera les modifications nécessair es, exécutez la commande suivante : `terraform plan –– var-file=examples/ terraform.tfvars`	
Exécutez les actions proposées.	Pour vérifier que les résultats de la `terraform plan` commande sont conformes aux attentes, procédez comme suit : 1. Exécutez la commande suivante: `terraform apply` 2. Connectez-vous au et AWS Management Console vérifiez que les ressources sont présentes.	DevOps ingénieur

Vérification du déploiement

Tâche	Description	Compétences requises
Exécutez et testez la fonction Lambda.	Pour vérifier que le déploieme nt a bien eu lieu, procédez comme suit : 1. Connectez-vous à la console AWS Managemen t Console Lambda et ouvrez-la. Ouvrez	DevOps ingénieur

Tâche	Description	Compétences requises
	la page Fonctions et sélectionnez le nom de la fonction commençant par ADcleanup-Lambda-*. 2. Sur la page de présentation des fonctions, choisissez Test dans l'onglet Code de la section Source du code. 3. Pour enregistrer l'événement de test, donnez-lui un nom et choisissez Enregistrer. Pour tester l'événement, sélectionnez à nouveau Tester. Les résultats de l'exécution indiquent le résultat de la fonction.	

Tâche	Description	Compétences requises
Afficher les résultats de l'exécution des EventBridge règles depuis le compte parent.	Pour consulter les résultats de la EventBridge règle basée sur les événements de EC2 résiliation d'Amazon depuis le compte parent, procédez comme suit : 1. Mettez fin aux EC2 instances depuis le compte parent. 2. Ouvrez la console Lambda du compte parent. Ouvrez la page Fonctions et sélectionnez le nom de la fonction commençant par ADcleanup-Lambda-*. 3. Cliquez sur l'onglet Surveiller, puis sur Afficher CloudWatch les journaux. Dans la CloudWatch console, la page Log groups affiche les résultats de la fonction Lambda.	DevOps ingénieur

Tâche	Description	Compétences requises
Afficher les résultats de l'exécution des EventBrid ge règles depuis le compte enfant.	Pour consulter les résultats de la EventBridge règle basée sur les événements de EC2 résiliation d'Amazon liés au compte enfant, procédez comme suit : 1. Mettez fin aux EC2 instances depuis le compte enfant. 2. Ouvrez la console Lambda du compte parent. Ouvrez la page Fonctions et sélectionnez le nom de la fonction commençant par ADcleanup-Lambda-*. 3. Cliquez sur l'onglet Surveiller, puis sur Afficher CloudWatch les journaux. Dans la CloudWatch console, la page Log groups affiche les résultats de la fonction Lambda.	DevOps ingénieur

Nettoyer l'infrastructure après utilisation

Tâche	Description	Compétences requises
Nettoyez l'infrastructure.	Pour nettoyer l'infrastructure que vous avez créée, utilisez la commande suivante : `terraform destroy`	DevOps ingénieur

Tâche	Description	Compétences requises
	Pour confirmer la `destroy` commande, tapez`yes`.	
Vérifiez après le nettoyage.	Vérifiez que les ressources ont été correctement supprimées.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Problème de connexion entre AWS Directory Service (compte parent) et l' EC2 instance Amazon (compte enfant) : vous ne pouvez pas associer les ordinateurs du compte enfant à AD même si le peering VPC est disponible.	Ajoutez le routage dans le VPCs. Pour obtenir des instructions, consultez la section Configure r une connexion d'appairage VPC entre le propriétaire du répertoire et le compte du consommateur de l'annuaire dans la documentation. AWS Directory Service

Ressources connexes

AWS documentation

- Amazon EventBridge et AWS Identity and Access Management
- Configurer des autorisations d’instance requises pour Systems Manager
- Gestion des identités et des accès pour AWS Directory Service
- Politiques IAM basées sur l'identité pour Lambda
- Joindre manuellement une instance Amazon EC2 Windows à votre AWS Managed Microsoft AD Active Directory
- Supprimez EC2 les entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation

Autres ressources

- AWS Fournisseur (documentation Terraform)

- Configuration du backend (documentation Terraform)
- Installer Terraform (documentation Terraform)
- Module de démarrage Python (référentiel Python Package Index)
- Téléchargement du binaire Terraform (documentation Terraform)

Supprimez EC2 les entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation

Créée par le Dr Rahul Sharad Gaikwad (AWS) et Tamilselvan (AWS)

Récapitulatif

Active Directory (AD) est un outil de script Microsoft qui gère les informations de domaine et les interactions des utilisateurs avec les services réseau. Il est largement utilisé par les fournisseurs de services gérés (MSPs) pour gérer les informations d'identification et les autorisations d'accès des employés. Étant donné que les attaquants publicitaires peuvent utiliser des comptes inactifs pour tenter de pirater une organisation, il est important de trouver les comptes inactifs et de les désactiver dans le cadre d'un programme de maintenance de routine. Avec AWS Directory Service for Microsoft Active Directory, vous pouvez exécuter Microsoft Active Directory en tant que service géré.

Ce modèle peut vous aider à configurer AWS Lambda l'automatisation pour trouver et supprimer rapidement les comptes inactifs. Lorsque vous utilisez ce modèle, vous pouvez bénéficier des avantages suivants :

- Améliorez les performances des bases de données et des serveurs, et corrigez les failles de sécurité liées aux comptes inactifs.
- Si votre serveur AD est hébergé dans le cloud, la suppression des comptes inactifs peut également réduire les coûts de stockage tout en améliorant les performances. Vos factures mensuelles peuvent diminuer car les frais de bande passante et de ressources informatiques peuvent tous deux diminuer.
- Tenez les attaquants potentiels à distance grâce à un Active Directory propre.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Git est installé et configuré sur un poste de travail local.
- Terraform installé et configuré sur un poste de travail local.
- Ordinateur Windows doté de modules Active Directory (`ActiveDirectory`).
- Un répertoire AWS Managed Microsoft AD et des informations d'identification stockées dans un paramètre du AWS Systems Manager Parameter Store.

- AWS Identity and Access Management rôle (IAM) avec autorisations d'accès aux éléments Services AWS répertoriés dans Outils. Pour plus d'informations sur IAM, consultez la section Ressources connexes.

Limites

- Ce modèle ne prend pas en charge la configuration entre comptes.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Terraform version 1.1.9 ou ultérieure
- Terraform AWS Provider version 3.0 ou supérieure

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Amazon EventBridge déclenche la AWS Lambda fonction en fonction d'une expression cron. (Pour ce modèle, le calendrier des expressions cron est d'une fois par jour.)
2. Le rôle et la politique IAM requis sont créés et attachés AWS Lambda via Terraform.
3. La AWS Lambda fonction est exécutée et appelle Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling Groups à l'aide du module Python boto. La fonction Lambda obtient l'identifiant d'instance aléatoire. L'identifiant d'instance est utilisé pour exécuter AWS Systems Manager des commandes.
4. AWS Lambda effectue un autre appel à Amazon à l' EC2 aide du module boto et obtient les adresses IP privées des serveurs Windows en cours d'exécution et les stocke dans une variable temporaire.
5. AWS Lambda lance un nouvel appel à Systems Manager pour obtenir les informations de l'ordinateur auquel il est connecté AWS Directory Service.

6. Un AWS Systems Manager document permet d'exécuter le PowerShell script sur les serveurs Amazon EC2 Windows pour obtenir les adresses IP privées des ordinateurs connectés à AD.
7. Le nom d'utilisateur et les mots de passe du domaine AD sont stockés dans le AWS Systems Manager Parameter Store. AWS Lambda et Systems Manager appellent Parameter Store et obtiennent les valeurs du nom d'utilisateur et du mot de passe à utiliser pour connecter AD.
8. À l'aide du document Systems Manager, le PowerShell script est exécuté sur le serveur Amazon EC2 Windows à l'aide de l'identifiant d'instance obtenu précédemment à l'étape 3.
9. Amazon EC2 se connecte AWS Directory Service à l'aide de PowerShell commandes et supprime les ordinateurs inutilisés ou inactifs.

Outils

Services AWS

- AWS Directory Servicepropose plusieurs manières d'utiliser Microsoft Active Directory (AD) avec d'autres, Services AWS comme Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) pour SQL Server et FSx Amazon pour Windows File Server.
- AWS Directory Service for Microsoft Active Directorypermet à vos charges de travail et à vos AWS ressources sensibles aux annuaires d'utiliser Microsoft Active Directory dans le. AWS Cloud
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, AWS Lambda des fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser. Avec IAM, vous pouvez spécifier qui ou quoi peut accéder aux services et aux ressources AWS, gérer de manière centralisée les autorisations détaillées et analyser les accès pour affiner les autorisations entre elles. AWS
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.
- AWS Systems Manager les documents définissent les actions que Systems Manager exécute sur vos instances gérées. Systems Manager inclut plus d'une centaine de documents préconfigurés que vous pouvez utiliser en spécifiant des paramètres lors de l'exécution.
- AWS Systems Manager Parameter Store est une fonctionnalité AWS Systems Manager et fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure open source sous forme de code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code C

Le code de ce modèle est disponible dans le référentiel de solutions GitHub Custom AD Cleanup Automation.

Bonnes pratiques

- Joignez automatiquement des domaines.Lorsque vous lancez une instance Windows destinée à faire partie d'un AWS Directory Service domaine, rejoignez le domaine pendant le processus de création de l'instance au lieu de l'ajouter manuellement ultérieurement. Pour rejoindre automatiquement un domaine, sélectionnez le répertoire approprié dans la liste déroulante des répertoires de jointure de domaines lors du lancement d'une nouvelle instance. Pour plus de détails, consultez la section Joindre sans difficulté une instance Amazon EC2 Windows à votre AWS Managed Microsoft AD Active Directory dans le guide d'AWS Directory Service administration.
- Supprimez les comptes inutilisés.Il est courant de trouver dans AD des comptes qui n'ont jamais été utilisés. Tout comme les comptes désactivés ou inactifs qui restent dans le système,

les comptes non utilisés négligés peuvent ralentir votre système publicitaire ou rendre votre organisation vulnérable aux violations de données.

- Automatisez les nettoyages d'Active Directory.Pour atténuer les risques de sécurité et empêcher les comptes obsolètes d'affecter les performances d'AD, effectuez des nettoyages AD à intervalles réguliers. Vous pouvez accomplir la plupart des tâches de gestion et de nettoyage d'AD en écrivant des scripts. Les tâches incluent par exemple la suppression de comptes désactivés et inactifs, la suppression de groupes vides et inactifs et la localisation de comptes utilisateurs et de mots de passe expirés.

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises
Créez un dossier de projet et ajoutez les fichiers.	Pour cloner le référentiel et créer un dossier de projet, procédez comme suit : 1. Ouvrez le GitHub référentiel de ce modèle. 2. Cliquez sur le bouton Code pour voir les options de clonage dans la liste déroulante Cloner. 3. Dans l'onglet HTTPS, copiez l'URL fournie dans Clone à l'aide de l'URL Web. 4. Créez un dossier sur votre machine et nommez-le avec le nom de votre projet. 5. Ouvrez un terminal sur votre ordinateur local et accédez à ce dossier.	DevOps ingénieur

Tâche	Description	Compétences requises

	6. Pour cloner le dépôt git, utilisez la commande suivante.
	
	`git clone <repository-URL>.git`
	7. Une fois le dépôt cloné, utilisez la commande suivante pour accéder au répertoire cloné.
	
	`cd <directory name>`
	8. Dans le référentiel cloné, ouvrez ce projet dans un environnement de développement intégré (IDE) de votre choix.	

Provisionner l'architecture cible à l'aide de la configuration Terraform

Tâche	Description	Compétences requises
Initialisez la configuration Terraform.	Pour initialiser votre répertoire de travail contenant les fichiers Terraform, exécutez la commande suivante. `terraform init`	DevOps ingénieur
Prévisualisez les modifications.	Vous pouvez prévisualiser les modifications que Terraform apportera à l'infrastructure avant que celle-ci ne soit déployée. Pour valider que Terraform apportera les	DevOps ingénieur

Tâche	Description	Compétences requises
	modifications nécessair es, exécutez la commande suivante. `terraform plan`	
Exécutez les actions proposées.	Pour vérifier que les résultats de la `terraform plan` commande sont conformes aux attentes, procédez comme suit : 1. Exécutez la commande suivante. `terraform apply` 2. Connectez-vous au et AWS Management Console vérifiez que les ressources sont présentes.	DevOps ingénieur
Nettoyez l'infrastructure.	Pour nettoyer l'infrastructure que vous avez créée, utilisez la commande suivante. `terraform destroy` Pour confirmer la commande de destruction, tapez`yes`.	DevOps ingénieur

Vérification du déploiement

Tâche	Description	Compétences requises
Exécutez et testez la fonction Lambda.	Pour vérifier que le déploiement a bien eu lieu, procédez comme suit : 1. Connectez-vous à la console AWS Management Console et ouvrez-la. Ouvrez la page Fonctions et sélectionnez le nom de la fonction commençant par ADcleanup-Lambda-*. 2. Sur la page de présentation des fonctions, choisissez Test dans l'onglet Code de la section Source du code. 3. Pour enregistrer l'événement de test, donnez-lui un nom et choisissez Enregistrer. Ensuite, pour tester l'événement, sélectionnez à nouveau Tester. Les résultats de l'exécution indiquent le résultat de la fonction.	DevOps ingénieur
Affichez les résultats de la fonction Lambda.	Dans ce modèle, une EventBridge règle exécute la fonction Lambda une fois par jour. Pour afficher les résultats de la fonction Lambda, procédez comme suit :	DevOps ingénieur

Tâche	Description	Compétences requises
	1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la. Ouvrez la page Fonctions et sélectionnez le nom de la fonction commençant par ADcleanup-Lambda-*. 2. Cliquez sur l'onglet Surveiller, puis sur Afficher CloudWatch les journaux. Dans la CloudWatch console, la page Log groups affiche les résultats de la fonction Lambda.	

Nettoyer l'infrastructure après utilisation

Tâche	Description	Compétences requises
Nettoyez les infrastructures.	Pour nettoyer l'infrastructure que vous avez créée, utilisez la commande suivante. `terraform destroy` Pour confirmer la commande de destruction, tapez`yes`.	DevOps ingénieur
Vérifiez après le nettoyage.	Vérifiez que les ressources ont été correctement supprimées.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Si vous essayez de supprimer l'ordinateur AD, le message « Accès refusé » s'affiche. L'ordinateur AD ne peut pas être supprimé car, par défaut, l'action tente de supprimer deux adresses IP privées connectées dans le cadre des services AD.	Pour éviter cette erreur, utilisez l'opération Python suivante pour ignorer les deux premiers ordinateurs lorsque vous listez les différences entre la sortie d'un ordinateur AD et la sortie de votre machine exécutant Windows. `Difference = Difference[2:]`
Lorsque Lambda exécute un PowerShell script sur un serveur Windows, il s'attend à ce que les modules Active Directory soient disponibl es par défaut. Si les modules ne sont pas disponibles, une fonction Lambda crée une erreur indiquant « Get- n'AdComputer est pas installé sur l'instance ».	Pour éviter cette erreur, installez les modules requis en utilisant les données utilisateur des EC2 instances. Utilisez le EC2Window sUserdatascript qui se trouve dans le GitHub dépôt de ce modèle.

Ressources connexes

AWS documentation

- Amazon EventBridge et AWS Identity and Access Management
- Configurer des autorisations d’instance requises pour Systems Manager
- Gestion des identités et des accès pour AWS Directory Service
- Joindre manuellement une instance Amazon EC2 Windows à votre AWS Managed Microsoft AD Active Directory
- Utilisation de politiques IAM basées sur l'identité dans AWS Lambda

Autres ressources

- AWS Fournisseur (documentation Terraform)
- Configuration du backend (documentation Terraform)

- Installer Terraform (documentation Terraform)
- Module de démarrage Python (référentiel Python Package Index)
- Téléchargement du binaire Terraform (documentation Terraform)

Exécutez des tests unitaires pour les tâches ETL Python en AWS Glue utilisant le framework pytest

Créée par Praveen Kumar Jeyarajan (AWS) et Vaidy Sankaran (AWS)

Récapitulatif

Vous pouvez exécuter des tests unitaires pour des tâches d'extraction, de transformation et de chargement (ETL) en Python AWS Glue dans un environnement de développement local, mais la réplication de ces tests dans un DevOps pipeline peut s'avérer difficile et chronophage. Les tests unitaires peuvent être particulièrement difficiles lorsque vous modernisez le processus ETL du mainframe sur des piles AWS technologiques. Ce modèle vous montre comment simplifier les tests unitaires, tout en préservant les fonctionnalités existantes, en évitant d'interrompre les fonctionnalités clés de l'application lorsque vous publiez de nouvelles fonctionnalités et en maintenant des logiciels de haute qualité. Vous pouvez utiliser les étapes et les exemples de code de ce modèle pour exécuter des tests unitaires pour les tâches ETL Python en AWS Glue utilisant le framework pytest dans AWS CodePipeline. Vous pouvez également utiliser ce modèle pour tester et déployer plusieurs AWS Glue tâches.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une URI d'image Amazon Elastic Container Registry (Amazon ECR) pour AWS Glue votre bibliothèque, téléchargée depuis la galerie publique Amazon ECR
- terminal Bash (sur n'importe quel système d'exploitation) avec un profil pour la cible Compte AWS et Région AWS
- Python 3.10 ou version ultérieure
- Pytest
- bibliothèque Moto Python pour les tests Services AWS

Architecture

Le schéma suivant décrit comment intégrer les tests unitaires pour les processus AWS Glue ETL basés sur Python dans un pipeline typique à l'échelle AWS DevOps d'une entreprise.

Le schéma suivant illustre le flux de travail suivant :

1. Au stade source, AWS CodePipeline utilise un bucket Amazon Simple Storage Service (Amazon S3) versionné pour stocker et gérer les actifs du code source. Ces ressources incluent un exemple de tâche ETL Python (`sample.py`), un fichier de test unitaire (`test_sample.py`) et un AWS CloudFormation modèle. CodePipeline Transfère ensuite le code le plus récent de la branche principale vers le AWS CodeBuild projet pour un traitement ultérieur.
2. Au cours de la phase de création et de publication, le code le plus récent de l'étape source précédente est testé à l'unité à l'aide d'une image Amazon ECR AWS Glue publique. Le rapport de test est ensuite publié dans les groupes de CodeBuild rapports. L'image du conteneur dans le référentiel public Amazon ECR pour les AWS Glue bibliothèques inclut tous les fichiers binaires nécessaires à l'exécution locale de tâches ETL PySparkbasées sur des tests unitaires. AWS Glue Le référentiel de conteneurs public comporte trois balises d'image, une pour chaque version prise en charge par AWS Glue. À des fins de démonstration, ce modèle utilise la balise `glue_libs_4.0.0_image_01` image. Pour utiliser cette image de conteneur comme image d'exécution CodeBuild, copiez l'URI de l'image qui correspond à la balise d'image que vous souhaitez utiliser, puis mettez à jour le `pipeline.yml` fichier dans le GitHub référentiel de la `TestBuild` ressource.
3. Lors de la phase de déploiement, le CodeBuild projet est lancé et le code est publié dans un compartiment Amazon S3 si tous les tests sont réussis.
4. L'utilisateur déploie la AWS Glue tâche à l'aide du CloudFormation modèle figurant dans le `deploy` dossier.

Outils

Services AWS

- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- AWS Glueest un service ETL entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets offrant une évolutivité, une disponibilité des données, une sécurité et des performances de pointe.

Autres outils

- Python est un langage de programmation de haut niveau interprété à usage général.
- Moto est une bibliothèque Python pour les tests Services AWS.
- Pytest est un framework permettant d'écrire de petits tests unitaires évolutifs pour prendre en charge des tests fonctionnels complexes pour les applications et les bibliothèques.
- La bibliothèque Python ETL for AWS Glue est un référentiel pour les bibliothèques Python utilisées dans le développement local de tâches PySpark par lots pour AWS Glue.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub aws-glue-jobs-unit-testing. Le référentiel inclut les ressources suivantes :

- Exemple de AWS Glue tâche basée sur Python dans le dossier `src`
- Cas de tests unitaires associés (créés à l'aide du framework pytest) dans le dossier `tests`
- Un CloudFormation modèle (écrit en YAML) dans le dossier `deploy`

Bonnes pratiques

Sécurité des CodePipeline ressources

Il est recommandé d'utiliser le chiffrement et l'authentification pour les référentiels sources qui se connectent à vos pipelines. CodePipeline Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité dans la CodePipeline documentation.

Surveillance et journalisation des CodePipeline ressources

Il est recommandé d'utiliser les fonctionnalités de AWS journalisation pour déterminer les actions que les utilisateurs effectuent sur votre compte et les ressources qu'ils utilisent. Les fichiers journaux contiennent les informations suivantes :

- Heure et date des actions
- Adresse IP source des actions

- Quelles actions ont échoué en raison d'autorisations inadéquates

Les fonctionnalités de journalisation sont disponibles dans AWS CloudTrail et Amazon CloudWatch Events. Vous pouvez l'utiliser CloudTrail pour enregistrer les appels d' AWS API et les événements connexes effectués par ou pour votre compte Compte AWS. Pour plus d'informations, consultez la section Journalisation des appels d' CodePipeline API AWS CloudTrail dans la CodePipeline documentation.

Vous pouvez utiliser CloudWatch les événements pour surveiller vos AWS Cloud ressources et vos applications en cours d'exécution AWS. Vous pouvez également créer des alertes dans CloudWatch Événements. Pour plus d'informations, consultez la section Surveillance CodePipeline des événements dans la CodePipeline documentation.

Épopées

Déployer le code source

Tâche	Description	Compétences requises

Préparez l'archive de code pour le déploiement.	1. `code.zip`Téléchargez-le depuis le dépôt GitHub aws-glue-jobs-unit-testing ou créez vous-même le fichier .zip à l'aide d'un outil de ligne de commande. Par exemple, vous pouvez créer le fichier .zip sous Linux ou Mac en exécutant les commandes suivantes dans le terminal :
	`git clone https://github.com/aws-samples/aws-glue-jobs-unit-testing.git`
	`cd aws-glue-jobs-unit-testing`
	`git checkout master`
		DevOps ingénieur

Tâche	Description	Compétences requises
	``` zip -r code.zip src/ tests/ deploy/ ``` 2. Connectez-vous au AWS Management Consoleet choisissez celui Région AWS de votre choix. 3. Créez un compartiment Amazon S3, puis chargez le package et le `code.zip` fichier .zip (téléchargés précédemment) dans le compartiment Amazon S3 que vous avez créé.	

Tâche	Description	Compétences requises
Créez la CloudFormation pile.	1. Connectez-vous à la CloudFormation console, AWS Management Console puis ouvrez-la. 2. Choisissez Créer une pile, puis sélectionnez Avec les ressources existantes (ressources d'importation). 3. Dans la section Spécifier le modèle de la page Créer une pile, choisisse z Télécharger un fichier modèle, puis choisisse z le modèle pipeline.yml (téléchargé depuis le référentiel). GitHub Ensuite, choisissez Suivant. 4. Pour Nom de pile glue-unit -testing-pipeline, entrez ou choisissez le nom de pile de votre choix. 5. Pour ApplicationStackNa me, utilisez le glue-code pipeline-appnom prérempli . Il s'agit du nom de la CloudFormation pile créée par le pipeline. 6. Pour BucketName, utilisez le nom de compartiment aws-glue-artifacts-us-east- 1 prérempli. Il s'agit du nom du compartiment Amazon S3 qui contient le fichier .zip	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	et qui est utilisé par le pipeline pour stocker les artefacts de code. 7. Pour CodeZipFile, utilisez la valeur code.zip prérempli e. Il s'agit du nom clé de l'exemple de code de l'objet Amazon S3. L'objet doit être un fichier .zip. 8. Pour TestReportGroupNam e, utilisez le glue-unittest-reportnom prérempli. Il s'agit du nom du groupe de rapports de CodeBuild test créé pour stocker les rapports de tests unitaires. 9. Choisissez Next, puis de nouveau Next sur la page Configurer les options de pile. 10. Sur la page de révision, sous Fonctionnalités, choisissez l'option Je reconnais que des ressources IAM CloudForm ation pourraient être créées avec des noms personnal isés. 11. Sélectionnez Envoyer. Une fois la création de la pile terminée, vous pouvez voir les ressources créées dans l'onglet Ressources. La	

Tâche	Description	Compétences requises
	création de la pile prend environ 5 à 7 minutes. La pile crée une CodePipel ine vue en utilisant Amazon S3 comme source. Dans les étapes ci-dessus, le pipeline est aws-glue-unit-test-pipeline.	

Exécutez les tests unitaires

Tâche	Description	Compétences requises
Exécutez les tests unitaires dans le pipeline.	1. Pour tester le pipeline déployé, connectez-vous à la CodePipeline console AWS Management Console, puis ouvrez-la. 2. Sélectionnez le pipeline créé par la CloudForm ation pile, puis choisisse z Release change. Le pipeline commence à s'exécuter (en utilisant le code le plus récent du compartiment Amazon S3). 3. Une fois la phase Test_and_build terminée, choisissez l'onglet Détails, puis examinez les journaux. 4. Choisissez l'onglet Rapports, puis sélection nez le rapport de test dans	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	l'historique des rapports pour afficher les résultats des tests unitaires. 5. Une fois la phase de déploiement terminée, exécutez et surveille z le AWS Glue travail déployé sur la AWS Glue console. Pour plus d'informations, consultez la section Surveillance AWS Glue dans la AWS Glue documentation.	

Nettoyez toutes les AWS ressources

Tâche	Description	Compétences requises
Nettoyez les ressources de votre environnement.	Pour éviter des coûts d'infrast ructure supplémentaires, assurez-vous de supprimer la pile après avoir testé les exemples fournis dans ce modèle. 1. Ouvrez la CloudFormation console, puis sélectionnez la pile que vous avez créée. 2. Sélectionnez Delete (Supprimer). Cela supprime toutes les ressources créées par votre pile, y compris les rôles AWS Identity and Access	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	Management (IAM), les politiques IAM et les projets. CodeBuild	

Résolution des problèmes

Problème	Solution
Le rôle CodePipeline de service ne peut pas accéder au compartiment Amazon S3.	• Pour la politique associée à votre rôle CodePipeline de service, `s3:ListBucket` ajoutez-la à la liste des actions de votre stratégie. Pour obtenir des instructions sur l'affichage de la politique de rôle de service, voir Afficher l'ARN du pipeline et l'ARN du rôle de service (console). Modifiez la déclaration de politique relative à votre rôle de service, comme indiqué dans Ajouter des autorisations au rôle CodePipeline de service. • Pour la politique basée sur les ressource s attachée au compartiment d'artefacts Amazon S3 pour votre pipeline, également appelée politique de compartiment d'artefac ts, ajoutez une déclaration qui autorise le rôle de CodePipeline service à utiliser l'autoris ation. `s3:ListBucket`
CodePipeline renvoie une erreur indiquant que le compartiment Amazon S3 n'est pas versionné.	CodePipeline nécessite que le compartiment Amazon S3 source soit versionné. Activez le versionnement sur votre compartiment Amazon S3. Pour obtenir des instructions, consultez la section Activation de la gestion des versions sur les buckets.

Ressources connexes

- AWS Glue
- Développer et tester des AWS Glue emplois au niveau local
- AWS CloudFormation pour AWS Glue

Informations supplémentaires

En outre, vous pouvez déployer les AWS CloudFormation modèles en utilisant le AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez la section Déploiement rapide de modèles avec transformations dans la CloudFormation documentation.

Configuration d'un référentiel de graphiques Helm v3 dans Amazon S3

Créée par Abhishek Sharma (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle vous aide à gérer efficacement les graphiques Helm v3 en intégrant le référentiel Helm v3 dans Amazon Simple Storage Service (Amazon S3) sur le cloud Amazon Web Services (AWS). Pour utiliser ce modèle, vous devez connaître Kubernetes et Helm, qui est un gestionnaire de packages Kubernetes. L'utilisation des référentiels Helm pour stocker les graphiques et les versions des cartes de contrôle peut améliorer le temps moyen de restauration (MTTR) en cas de panne.

Ce modèle utilise AWS CodeCommit pour la création du référentiel Helm, et il utilise un compartiment S3 comme référentiel de diagrammes Helm, afin que les graphiques puissent être gérés de manière centralisée et accessibles par les développeurs de l'entreprise.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Python version 2.7.12 ou ultérieure
- pip
- Un cloud privé virtuel (VPC) avec des sous-réseaux et une instance Amazon Elastic Compute Cloud (Amazon) EC2
- Git installé sur l' EC2 instance
- Accès à AWS Identity and Access Management (IAM) pour créer le compartiment S3
- Accès IAM (par programmation ou par rôle) à Amazon S3 depuis la machine cliente
- CodeCommit Référentiel AWS
- Interface de ligne de commande AWS (AWS CLI)

Versions du produit

- Casque v3

- Python version 2.7.12 ou ultérieure

Architecture

Pile technologique cible

- Amazon S3
- AWS CodeCommit
- Helm
- Kubectl
- Python et pip
- Git
- plug-in helm-s3

Architecture cible

Automatisation et mise à l'échelle

- Vous pouvez intégrer Helm à votre outil d'automatisation integration/continuous delivery (CI/CD (continu) existant pour automatiser le packaging et le contrôle des versions des graphiques Helm (hors de portée de ce modèle).
- GitVersion ou les numéros de version de Jenkins peuvent être utilisés pour automatiser le contrôle de version des graphiques.

Outils

- Helm — Helm est un gestionnaire de packages pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- plugin helm-s3 — Le plug-in helm-s3 prend en charge l'interaction avec Amazon S3. Il peut être utilisé avec Helm v2 ou Helm v3.

Épopées

Installez et validez Helm v3

Tâche	Description	Compétences requises
Installez le client Helm v3.	Pour télécharger et installer le client Helm sur votre système local, exécutez la commande suivante : `sudo curl https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3 | bash`	Administrateur cloud, DevOps ingénieur
Validez l'installation de Helm.	Pour valider le client Helm, exécutez la commande suivante : `helm version --short`	Administrateur cloud, DevOps ingénieur

Initialisation d'un compartiment S3 en tant que référentiel Helm

Tâche	Description	Compétences requises
Créez un compartiment S3 pour les cartes Helm.	Créez un compartiment S3 unique. Dans le compartiment, créez un dossier appelé `stable/myapp` . L'exemple de ce modèle utilise `s3://my-helm-charts/stable/myapp` comme référentiel graphique cible.	Administrateur cloud, DevOps ingénieur
Installez le plugin helm-s3 pour Amazon S3.	Pour installer le plugin helm-s3 sur votre machine cliente, exécutez la commande suivante : `helm plugin`	Administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	`install https://github.com/hypnoglow/helm-s3.git`	
Initialisez le référentiel Amazon S3 Helm.	Pour initialiser le dossier cible en tant que référentiel Helm, utilisez la commande suivante : `helm s3 init s3://my-helm-charts/stable/myapp` La commande crée un `index.yaml` fichier dans la cible pour suivre toutes les informations du graphique stockées à cet emplacement.	Administrateur cloud, DevOps ingénieur
Vérifiez le dépôt Helm nouvellement créé.	Pour vérifier que le `index.yaml` fichier a été créé, exécutez la commande suivante : `aws s3 ls s3://my-helm-charts/stable/myapp/`	Administrateur cloud, DevOps ingénieur
Ajoutez le référentiel Amazon S3 à Helm sur la machine cliente.	Pour ajouter l'alias du référentiel cible à la machine cliente Helm, utilisez la commande suivante : `helm repo add stable-myapp s3://my-helm-charts/stable/myapp/`	Administrateur cloud, DevOps ingénieur

Package et publication de graphiques dans le référentiel Amazon S3 Helm

Tâche	Description	Compétences requises
Clonez vos cartes Helm.	Si aucun graphique Helm local n'est présent dans votre CodeCommit dépôt, clonez-les depuis votre GitHub dépôt en exécutant la commande suivante : `git clone <url_of_your_helm_source_code>.git`	Administrateur cloud, DevOps ingénieur
Package de la carte Helm locale.	Pour empaqueter le graphique que vous avez créé ou cloné, utilisez la commande suivante : `helm package ./my-app` Par exemple, ce modèle utilise le `my-app` graphique. La commande regroupe tout le contenu du dossier `my-app` graphique dans un fichier d'archive, dont le nom est basé sur le numéro de version indiqué dans le `Chart.yaml` fichier.	Administrateur cloud, DevOps ingénieur
Stockez le package local dans le référentiel Amazon S3 Helm.	Pour télécharger le package local dans le référentiel Helm d'Amazon S3, exécutez la commande suivante : `helm s3 push ./my-app-0.1.0.tgz stable-my app`	Administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	Dans la commande, `my-app` figurent le nom du dossier de votre graphique, `0.1.0` la version du graphique mentionnée dans `Chart.yaml` et `stable-myapp` l'alias du référentiel cible.	
Recherchez le graphique Helm.	Pour vérifier que le graphique apparaît à la fois localement et dans le référentiel Amazon S3 Helm, exécutez la commande suivante : `helm search repo stable-myapp`	Administrateur cloud, DevOps ingénieur

Mettez à niveau votre référentiel Helm

Tâche	Description	Compétences requises
Modifiez et empaquetez le graphique.	Dans`values.yaml` , définissez la `replicaCount` valeur sur`1`, puis empaquetez le graphique, en changeant cette fois la version `Chart.yaml` en`0.1.1`. Le contrôle des versions est idéalement réalisé grâce à l'automatisation en utilisant des outils tels que GitVersion les numéros de build Jenkins dans un pipeline CI/CD. L'automatisation du numéro de version n'est pas couverte par ce modèle. Pour empaquete	Administrateur cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	r le graphique, exécutez la commande suivante : `helm package ./my-app/`	
Transférez la nouvelle version vers le référentiel Helm d'Amazon S3.	Pour transférer le nouveau package, version 0.1.1, vers le référentiel my-helm-c hartsHelm d'Amazon S3, exécutez la commande suivante : `helm s3 push ./ my-app-0.1.1.tgz stable-myapp`	Administrateur cloud, DevOps ingénieur

Vérifiez le graphique Helm mis à jour.	Pour vérifier que le graphique mis à jour apparaît à la fois localement et dans le référenti el Amazon S3 Helm, exécutez les commandes suivantes.
	`helm repo update`
	`helm search repo stable-myapp`
		Administrateur cloud, DevOps ingénieur

Recherchez et installez un graphique depuis le référentiel Amazon S3 Helm

Tâche	Description	Compétences requises
Recherchez toutes les versions du graphique my-app.	Pour afficher toutes les versions disponibles d'un graphique, exécutez la commande suivante avec l'`--versions` indicateur : `helm search repo my-app --versions`	DevOps Ingénieur

Tâche	Description	Compétences requises
	Sans le drapeau, Helm affiche par défaut la dernière version téléchargée d'un graphique.	
Installez un graphique depuis le référentiel Amazon S3 Helm.	L'installation automatique n'est pas couverte par ce modèle, mais vous pouvez l'installer manuellement. Les résultats de la recherche de la tâche précédente montrent les différentes versions du `my-app` graphique. Pour installer la nouvelle version (0.1.1) depuis le référentiel Amazon S3 Helm, utilisez la commande suivante : `helm upgrade --install my-app-release stable-myapp/my-app --version 0.1.1 --namespace dev`	DevOps Ingénieur

Revenir à une version précédente à l'aide de Helm

Tâche	Description	Compétences requises
Passez en revue les détails d'une révision spécifique.	La restauration automatique n'est pas couverte par ce modèle, mais vous pouvez revenir manuellement à une version antérieure. Avant de passer à une version fonctionnelle ou de revenir à une version fonctionnelle, et pour une couche de validation	DevOps Ingénieur

Tâche	Description	Compétences requises
	supplémentaire avant d'installer une révision, consultez les valeurs transmises à chacune des révisions à l'aide de la commande suivante : `helm get values --revision=2 my-app-release`	
Retournez à une version précédente.	La restauration automatique est hors de portée de ce modèle. Pour revenir manuellement à une version précédente, utilisez la commande suivante : `helm rollback my-app-release 1` Cet exemple revient à la révision numéro 1.	DevOps Ingénieur

Ressources connexes

- Documentation HELM
- plugin helm-s3 (licence MIT)
- Amazon S3

Configuration d'un pipeline CI/CD à l'aide d'AWS et d' CodePipeline AWS CDK

Créée par Konstantin Zarudaev (AWS), Cizer Pereira (AWS), Lars Kinder (AWS) et Yasha Dabas (AWS)

Accueil

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus Automatiser le processus de création et de publication de vos logiciels grâce à l'intégration et à la livraison continues (CI/CD) supports repeatable builds and rapid delivery of new features to your users. You can quickly and easily test each code change, and you can catch and fix bugs before releasing your software. By running each change through your staging and release process, you can verify the quality of your application or infrastructure code. CI/CDincarne une culture, un ensemble de principes de fonctionnement et un ensemble de pratiques qui aident les équipes de développement d'applications à apporter des modifications de code plus fréquemment et de manière plus fiable). L'implémentation est également connue sous le nom de pipeline CI/CD.

Ce modèle définit un pipeline d'intégration et de livraison continues (CI/CD) réutilisable sur Amazon Web Services (AWS) avec un référentiel AWS CodeCommit . Le CodePipeline pipeline AWS est écrit à l'aide d'AWS Cloud Development Kit (AWS CDK) v2.

Vous pouvez ainsi modéliser les différentes étapes du processus de publication de votre logiciel via l'interface AWS Management Console, l'AWS Command Line Interface (AWS CLI), CloudFormation AWS ou AWS SDKs. CodePipeline Ce modèle illustre la mise en œuvre d'AWS CDK CodePipeline et de ses composants à l'aide d'AWS CDK. Outre la création de bibliothèques, AWS CDK inclut une boîte à outils (la commande CLI`cdk`), qui est le principal outil pour interagir avec votre application AWS CDK. La boîte à outils permet notamment de convertir une ou plusieurs piles en CloudFormation modèles et de les déployer sur un compte AWS.

Le pipeline inclut des tests visant à valider la sécurité de vos bibliothèques tierces et contribue à garantir une publication accélérée et automatisée dans les environnements spécifiés. Vous pouvez améliorer la sécurité globale de vos applications en les soumettant à un processus de validation.

L'objectif de ce modèle est d'accélérer votre utilisation des pipelines CI/CD pour déployer votre code tout en garantissant que les ressources que vous déployez respectent les DevOps meilleures pratiques. Après avoir implémenté l'exemple de code, vous disposerez d'un AWS CodePipeline avec

des processus de linting, de test, de vérification de sécurité, de déploiement et de post-déploiement. Ce modèle inclut également des étapes pour Makefile. À l'aide d'un Makefile, les développeurs peuvent reproduire les étapes CI/CD localement et accélérer le processus de développement.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une compréhension de base dans les domaines suivants :
  - AWS CDK
  - AWS CloudFormation
  - AWS CodePipeline
  - TypeScript

Limites

Ce modèle utilise AWS CDK TypeScript uniquement pour. Il ne couvre pas les autres langues prises en charge par AWS CDK.

Versions du produit

Utilisez les dernières versions des outils suivants :

- Interface de ligne de commande AWS (AWS CLI)
- cfn_nag
- git-remote-codecommit
- Node.js

Architecture

Pile technologique cible

- AWS CDK
- AWS CloudFormation
- AWS CodeCommit
- AWS CodePipeline

Architecture cible

Le pipeline est déclenché par une modification du CodeCommit référentiel AWS (`SampleRepository`). Au début, CodePipeline crée des artefacts, se met à jour et lance le processus de déploiement. Le pipeline qui en résulte déploie une solution dans trois environnements indépendants :

- Dev — Vérification du code en trois étapes dans l'environnement de développement actif
- Test — Environnement de test d'intégration et de régression
- Prod — Environnement de production

Les trois étapes incluses dans la phase de développement sont le linting, la sécurité et les tests unitaires. Ces étapes s'exécutent en parallèle pour accélérer le processus. Pour garantir que le pipeline ne fournit que des artefacts fonctionnels, il sera arrêté de fonctionner chaque fois qu'une étape du processus échoue. Après un déploiement en phase de développement, le pipeline exécute des tests de validation pour vérifier les résultats. En cas de succès, le pipeline déploiera ensuite les artefacts dans l'environnement de test, qui contient une validation après le déploiement. La dernière étape consiste à déployer les artefacts dans l'environnement Prod.

Le schéma suivant montre le flux de travail entre le CodeCommit référentiel et les processus de création et de mise à jour exécutés par CodePipeline, les trois étapes de l'environnement de développement, ainsi que le déploiement et la validation ultérieurs dans chacun des trois environnements.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS. Dans ce modèle, les CloudFormation modèles peuvent être utilisés pour créer un CodeCommit référentiel et un pipeline CodePipeline CI/CD.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.

- AWS CodePipeline est un service CI/CD qui vous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

Autres outils

- cfn_nag est un outil open source qui recherche des modèles dans des CloudFormation modèles afin d'identifier les problèmes de sécurité potentiels.
- git-remote-codecommitest un utilitaire permettant de transférer et d'extraire du code depuis des CodeCommit référentiels en étendant Git.
- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.

Code

Le code de ce modèle est disponible dans le référentiel de pratiques GitHub AWS CodePipeline with CI/CD.

Bonnes pratiques

Passez en revue les ressources, telles que les politiques AWS Identity and Access Management (IAM), pour vérifier qu'elles sont conformes aux meilleures pratiques de votre organisation.

Épopées

Outils d'installation

Tâche	Description	Compétences requises
Installez des outils sur macOS ou Linux.	Si vous utilisez macOS ou Linux, vous pouvez installer les outils en exécutant la commande suivante dans votre terminal préféré ou	DevOps ingénieur

Tâche	Description	Compétences requises

	en utilisant Homebrew pour Linux.
	
	`brew install`
	`brew install git-remote-codecommit`
	`brew install ruby brew-gem`
	`brew-gem install cfn-nag`	

Configurez l'AWS CLI.	Pour configurer l'AWS CLI, suivez les instructions correspondant à votre système d'exploitation : • Windows : étapes de configuration pour les connexions HTTPS aux CodeCommit référentiels AWS sous Windows avec l'assistant d'identification de l'interface de ligne de commande AWS • Linux, macOS, Unix : étapes de configuration des connexions HTTPS aux CodeCommit référentiels AWS sous Linux, macOS ou Unix à l'aide de l'assistant d'identification de la CLI AWS	DevOps ingénieur

Configuration du déploiement initial

Tâche	Description	Compétences requises

Téléchargez ou clonez le code.	Pour obtenir le code utilisé par ce modèle, effectuez l'une des opérations suivantes :
	• Téléchargez le dernier code source des versions du GitHub dépôt et décompressez le fichier téléchargé dans un dossier.
	• Clonez le projet en exécutant la commande suivante.
	`git clone --depth 1 https://github.com/aws-samples/aws-codepipeline-cicd.git`
	Supprimez le `.git` répertoire du référentiel cloné.
	`cd ./aws-codepipeline-cicd`
	`rm -rf ./.git`
	Plus tard, vous utiliserez un CodeCommit dépôt AWS nouvellement créé comme origine distante.
		DevOps ingénieur

Connectez-vous au compte AWS.	Vous pouvez vous connecter à l'aide d'un jeton de sécurité temporaire ou d'une authentif	DevOps ingénieur

Tâche	Description	Compétences requises

	ication par zone d'atterrissage. Pour vérifier que vous utilisez le bon compte et la bonne région AWS, exécutez les commandes suivantes.
	
	`AWS_REGION="eu-west-1"`
	`ACCOUNT_NUMBER=$(aws sts get-caller-identity --query Account --output text)`
	`echo "${ACCOUNT_NUMBER}"`	

Tâche	Description	Compétences requises

Démarrez l'environnement.	Pour démarrer un environnement AWS CDK, exécutez les commandes suivantes.
	`npm install`
	`npm run cdk bootstrap "aws://${ACCOUNT_NUMBER}/${AWS_REGION}"`
	Une fois que vous avez réussi à démarrer l'environnement, le résultat suivant doit être affiché.
	`# Bootstrapping environment aws://{account}/{region}...`
	`# Environment aws://{account}/{region} bootstrapped`
	Pour plus d'informations sur le démarrage d'AWS CDK, consultez la documentation du CDK AWS.
		DevOps ingénieur

Tâche	Description	Compétences requises

Synthétisez un modèle.	Pour synthétiser une application AWS CDK, utilisez la `cdk synth` commande.
	`npm run cdk synth`
	Le résultat suivant doit s'afficher.
	`Successfully synthesized to <path-to-directory>/aws-codepipeline-cicd/cdk.out`
	`Supply a stack id (CodePipeline, Dev-MainStack) to display its template.`
		DevOps ingénieur

Tâche	Description	Compétences requises

Déployez la CodePipeline pile.	Maintenant que vous avez amorcé et synthétisé le CloudFormation modèle, vous pouvez le déployer. Le déploiement créera le CodePipeline pipeline et un CodeCommit référenti el, qui seront la source et le déclencheur du pipeline.
	`npm run cdk -- deploy CodePipeline --require-approval never`
	Après avoir exécuté la commande, vous devriez constater un déploiement réussi de la CodePipeline pile et des informations de sortie. Vous `CodePipeline.RepositoryName` donne le nom du CodeCommit référentiel dans le compte AWS.
	`CodePipeline: deploying... CodePipeline: creating CloudFormation changeset... # CodePipeline Outputs: CodePipeline.RepositoryName = SampleRepository Stack ARN:`
		DevOps ingénieur

Tâche	Description	Compétences requises
	`arn:aws:cloudformation:REGION:ACCOUNT-ID:stack/CodePipeline/STACK-ID`	

Tâche	Description	Compétences requises

Configurez le CodeCommit référentiel et la branche distants.	Une fois le déploiement réussi, CodePipeline lancera la première exécution du pipeline, que vous trouverez dans la CodePipeline console AWS. Comme AWS CDK CodeCommit n'initie pas de branche par défaut, cette exécution initiale du pipeline échouera et renverra le message d'erreur suivant.
	`The action failed because no branch named main was found in the selected AWS CodeCommit repository SampleRepository. Make sure you are using the correct branch name, and then try again. Error: null`
	Pour corriger cette erreur, configurez une origine distante en tant que `SampleRepository` et créez la `main` branche requise.
	`RepoName=$(aws cloudformation describe-stacks --stack-name CodePipeline --query "Stacks[0].Outputs[?OutputKey=='RepositoryName'].OutputValue" --output text)`
		DevOps ingénieur

Tâche	Description	Compétences requises

	`echo "${RepoName}"`
	`#`
	`git init`
	`git branch -m master main`
	`git remote add origin codecommit://${RepoName}`
	`git add .`
	`git commit -m "Initial commit"`
	`git push -u origin main`	

Testez le CodePipeline pipeline déployé

Tâche	Description	Compétences requises
Validez une modification pour activer le pipeline.	Après un déploiement initial réussi, vous devriez disposer d'un pipeline CI/CD complet avec une `main` branche pour `SampleRepository` en tant que branche source. Dès que vous validez les modifications apportées à la `main` branche, le pipeline lance et exécute la séquence d'actions suivante : 1. Récupérez votre code depuis le CodeCommit dépôt. 2. Créez votre code. 3. Mettez à jour le pipeline lui-même (`UpdatePipeline`).	DevOps ingénieur

Tâche	Description	Compétences requises
	4. Exécutez trois tâches parallèles pour le linting, la sécurité et les tests unitaires. 5. En cas de succès, le pipeline déploiera la `Main` pile depuis `./lib/main-stack.ts` l'environnement de développement. 6. Exécutez une vérification des ressources déployées après le déploiement. Vous pouvez suivre toutes les CodePipeline étapes et les résultats dans la CodePipeline console. 7. En cas de succès, le pipeline répétera le déploiement et la validation pour les environnements de test et de production.	

Testez localement en utilisant un Makefile

Tâche	Description	Compétences requises
Lancez le processus de développement à l'aide d'un Makefile.	Vous pouvez exécuter l'ensemble du pipeline localement à l'aide de la `make` commande, ou vous pouvez exécuter une étape individuelle (par exemple,`make linting`).	Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises
	Pour tester l'utilisation`make`, effectuez les actions suivantes : • Implémentez le pipeline local : `make` • Exécutez uniquement des tests unitaires : `make unittest` • Déployer sur le compte courant : `make deploy` • Nettoyez l'environnement : `make clean`	

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez les ressources de l'application AWS CDK.	Pour nettoyer votre applicati on AWS CDK, exécutez la commande suivante. `cdk destroy --all` Sachez que les compartim ents Amazon Simple Storage Service (Amazon S3) créés lors du démarrage ne sont pas automatiquement supprimés . Ils ont besoin d'une politique de rétention autorisant leur suppression, ou vous devez les supprimer manuellement dans votre compte AWS.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Le modèle ne fonctionne pas comme prévu.	Si quelque chose ne va pas et que le modèle ne fonctionne pas, assurez-vous que vous disposez des éléments suivants : • Les versions appropriées des outils. • Accès au compte AWS cible (connectivité réseau). • Autorisations suffisantes pour le compte AWS cible.

Ressources connexes

- Démarrez avec les tâches courantes dans IAM Identity Center
- CodePipeline Documentation AWS
- Kit de développement logiciel AWS

Configurez une journalisation centralisée à l'échelle de l'entreprise à l'aide de Terraform

Créée par Aarti Rajput (AWS), Yashwant Patel (AWS) et Nishtha Yadav (AWS)

Récapitulatif

La journalisation centralisée est vitale pour l'infrastructure cloud d'une entreprise, car elle fournit une visibilité sur ses opérations, sa sécurité et sa conformité. Au fur et à mesure que votre entreprise adapte son AWS environnement à plusieurs comptes, une stratégie structurée de gestion des journaux devient fondamentale pour exécuter les opérations de sécurité, répondre aux exigences d'audit et atteindre l'excellence opérationnelle.

Ce modèle fournit un cadre évolutif et sécurisé pour centraliser les journaux provenant de multiples services, afin de permettre la gestion Comptes AWS des journaux à l'échelle de l'entreprise dans le cadre de déploiements complexes. AWS La solution est automatisée à l'aide de Terraform, un outil d'infrastructure en tant que code (IaC) HashiCorp qui garantit des déploiements cohérents et répétables et minimise la configuration manuelle. En combinant Amazon CloudWatch Logs, Amazon Data Firehose et Amazon Simple Storage Service (Amazon S3), vous pouvez mettre en œuvre un pipeline robuste d'agrégation et d'analyse des journaux qui fournit :

- Gestion centralisée des journaux au sein de votre organisation dans AWS Organizations
- Collecte de journaux automatisée avec contrôles de sécurité intégrés
- Traitement évolutif des journaux et stockage durable
- Rapports de conformité et pistes d'audit simplifiés
- Informations opérationnelles et surveillance en temps réel

La solution collecte les journaux à partir des AWS Lambda conteneurs, des fonctions et des instances de base de données Amazon Elastic Kubernetes Service (Amazon EKS) via Logs. CloudWatch Il transmet automatiquement ces journaux vers un compte de journalisation dédié à l'aide de filtres CloudWatch d'abonnement. Firehose gère le pipeline de streaming de journaux à haut débit vers Amazon S3 pour un stockage à long terme. Amazon Simple Queue Service (Amazon SQS) est configuré pour recevoir des notifications d'événements Amazon S3 lors de la création d'un objet. Cela permet l'intégration avec les services d'analyse, notamment :

- Amazon OpenSearch Service pour la recherche dans les journaux, la visualisation et les analyses en temps réel

- Amazon Athena pour les requêtes basées sur SQL
- Amazon EMR pour le traitement à grande échelle
- Lambda pour une transformation personnalisée
- Amazon QuickSight pour les tableaux de bord

Toutes les données sont cryptées à l'aide de AWS Key Management Service (AWS KMS), et l'ensemble de l'infrastructure est déployée à l'aide de Terraform pour une configuration cohérente dans tous les environnements.

Cette approche de journalisation centralisée permet aux entreprises d'améliorer leur niveau de sécurité, de respecter les exigences de conformité et d'optimiser l'efficacité opérationnelle de leur AWS infrastructure.

Conditions préalables et limitations

Prérequis

- Une zone de landing zone pour votre organisation créée en utilisant AWS Control Tower
- Account Factory pour Terraform (AFT), déployé et configuré avec les comptes requis
- Terraform pour le provisionnement de l'infrastructure
- AWS Identity and Access Management Rôles et politiques (IAM) pour l'accès entre comptes

Pour obtenir des instructions sur la configuration AWS Control Tower des comptes AFT et Application, consultez la section Epics.

Comptes obligatoires

Votre organisation AWS Organizations doit inclure les comptes suivants :

- Compte d'application : un ou plusieurs comptes sources sur lesquels Services AWS (Amazon EKS, Lambda et Amazon RDS) s'exécutent et génèrent des journaux
- Compte Log Archive : un compte dédié pour le stockage et la gestion centralisés des journaux

Versions du produit

- AWS Control Tower version 3.1 ou ultérieure
- Terraform version 0.15.0 ou ultérieure

Architecture

Le schéma suivant illustre une architecture de journalisation AWS centralisée qui fournit une solution évolutive pour collecter, traiter et stocker les journaux de plusieurs comptes d'applications dans un compte Log Archive dédié. Cette architecture gère efficacement les journaux provenant Services AWS notamment d'Amazon RDS, Amazon EKS et Lambda, et les achemine via un processus rationalisé vers les compartiments S3 régionaux du compte Log Archive.

Le flux de travail comprend cinq processus :

1. Processus de journalisation
   - Le processus de flux de journaux commence dans les comptes de l'application, où sont Services AWS générés différents types de journaux, tels que les journaux généraux, les journaux d'erreurs, les journaux d'audit, les journaux de requêtes lentes d'Amazon RDS, les journaux du plan de contrôle d'Amazon EKS et les journaux d'exécution et d'erreur de Lambda.
   - CloudWatch sert de point de collecte initial. Il rassemble ces journaux au niveau du groupe de journaux au sein de chaque compte d'application.
   - Dans CloudWatch, les filtres d'abonnement déterminent quels journaux doivent être transférés au compte central. Ces filtres vous permettent de contrôler de manière précise le transfert des journaux, afin que vous puissiez spécifier des modèles de journal exacts ou des flux de journaux complets à des fins de centralisation.
2. Transfert de journaux entre comptes
   - Les journaux sont transférés vers le compte Log Archive. CloudWatch les filtres d'abonnement facilitent le transfert entre comptes et préservent le contexte régional.
   - L'architecture établit plusieurs flux parallèles pour gérer efficacement différentes sources de journaux, afin de garantir des performances et une évolutivité optimales.
3. Traitement des journaux dans le compte Log Archive
   - Dans le compte Log Archive, Firehose traite les flux de journaux entrants.
   - Chaque région gère des flux de diffusion Firehose dédiés qui peuvent transformer, convertir ou enrichir les logs selon les besoins.
   - Ces flux Firehose fournissent les journaux traités aux compartiments S3 du compte Log Archive, qui se trouve dans la même région que les comptes de l'application source (région A dans le schéma) afin de respecter les exigences de souveraineté des données.
4. Notifications et flux de travail supplémentaires

- Lorsque les logs atteignent leurs compartiments S3 de destination, l'architecture implémente un système de notification à l'aide d'Amazon SQS.
- Les files d'attente SQS régionales permettent un traitement asynchrone et peuvent déclencher des flux de travail, des analyses ou des systèmes d'alerte supplémentaires en fonction des journaux stockés.

5. AWS KMS pour la sécurité

   L'architecture intègre des éléments AWS KMS de sécurité. AWS KMS fournit des clés de chiffrement pour les compartiments S3. Cela garantit que tous les journaux stockés maintiennent le chiffrement au repos tout en conservant le chiffrement régional pour répondre aux exigences de résidence des données.

Outils

Services AWS

- Amazon CloudWatch est un service de surveillance et d'observabilité qui collecte des données opérationnelles et de surveillance sous forme de journaux, de mesures et d'événements. Il fournit une vue unifiée des AWS ressources, des applications et des services qui s'exécutent sur AWS et sur des serveurs sur site.
- CloudWatch Les filtres d'abonnement aux journaux sont des expressions qui correspondent à un modèle des événements de journal entrants et fournissent les événements de journal correspondants à la AWS ressource spécifiée pour un traitement ou une analyse ultérieurs.
- AWS Control Tower Account Factory For Terraform (AFT) met en place un pipeline Terraform pour vous aider à approvisionner et à personnaliser des comptes dans. AWS Control Tower AFT fournit un provisionnement de comptes basé sur Terraform tout en vous permettant de gérer vos comptes avec. AWS Control Tower
- Amazon Data Firehose fournit des données de streaming en temps réel vers des destinations telles qu'Amazon S3, Amazon Redshift et Amazon Service. OpenSearch Il s'adapte automatiquement au débit de vos données et ne nécessite aucune administration continue.
- Amazon Elastic Kubernetes Service (Amazon EKS) est un service d'orchestration de conteneurs géré qui facilite le déploiement, la gestion et le dimensionnement d'applications conteneurisées à l'aide de Kubernetes. Il gère automatiquement la disponibilité et l'évolutivité des nœuds du plan de contrôle Kubernetes.

- AWS Key Management Service (AWS KMS) crée et contrôle les clés de chiffrement pour chiffrer vos données. AWS KMS s'intègre Services AWS à d'autres services pour vous aider à protéger les données que vous stockez avec ces services.
- AWS Lambdaest un service de calcul sans serveur qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. Il adapte automatiquement vos applications en exécutant du code en réponse à chaque déclencheur, et ne facture que le temps de calcul que vous utilisez.
- Amazon Relational Database Service (Amazon RDS) est un service de base de données relationnelle géré qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud. Il fournit une capacité rentable et redimensionnable tout en automatisant les tâches d'administration fastidieuses.
- Amazon Simple Queue Service (Amazon SQS) est un service de mise en file d'attente de messages qui vous permet de découpler et de dimensionner les microservices, les systèmes distribués et les applications sans serveur. Il élimine la complexité de la gestion et de l'exploitation d'un intergiciel orienté message.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui offre évolutivité, disponibilité des données, sécurité et performances. Il peut stocker et récupérer n'importe quelle quantité de données n'importe où sur le Web.

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Code

Le code de ce modèle est disponible dans le référentiel de journalisation GitHub centralisé.

Bonnes pratiques

- Utilisez plusieurs Comptes AWS au sein d'une même organisation dans AWS Organizations. Cette pratique permet une gestion centralisée et une journalisation standardisée entre les comptes.
- Configurez les compartiments S3 avec le versionnement, les politiques de cycle de vie et la réplication entre régions. Mettez en œuvre le chiffrement et la journalisation des accès pour des raisons de sécurité et de conformité.

- Mettez en œuvre des normes de journalisation communes en utilisant le format JSON avec des horodatages et des champs standard. Utilisez une structure de préfixes et une corrélation cohérentes IDs pour faciliter le suivi et l'analyse.
- Activez les contrôles de sécurité grâce au AWS KMS chiffrement et à l'accès avec le moindre privilège. Maintenez une AWS CloudTrail surveillance et une rotation régulière des clés pour une sécurité renforcée.
- Configurez CloudWatch des métriques et des alertes pour le suivi des livraisons. Surveillez les coûts et les performances grâce à des notifications automatisées.
- Configurez les politiques de rétention Amazon S3 pour répondre aux exigences de conformité et activez la journalisation des accès au serveur Amazon S3 pour suivre toutes les demandes adressées à vos compartiments S3. Tenez à jour la documentation relative aux politiques relatives aux compartiments S3 et aux règles de cycle de vie. Révisez régulièrement les journaux d'accès, les autorisations des compartiments et les configurations de stockage afin de garantir la conformité et les meilleures pratiques en matière de sécurité.

Épopées

Comptes de configuration AWS Control Tower, AFT et d'application

Tâche	Description	Compétences requises
Configurez un AWS Control Tower environnement avec AFT.	1. Déployez AWS Control Tower en suivant les instructions de la AWS Control Tower documentation. 2. Déployez AFT en suivant les instructions de la AWS Control Tower documentation.	Administrateur AWS
Activez le partage des ressources pour l'organisation.	1. Configurez AWS Command Line Interface (AWS CLI) avec les informations d'identification du compte de gestion, qui fournissent	Administrateur AWS

Tâche	Description	Compétences requises
	les autorisations administratives nécessaires à la gestion AWS Control Tower. 2. Exécutez la AWS CLI commande suivante dans n'importe laquelle Région AWS : `aws ram enable-sharing-with-aws-organization` Cela permet le partage des ressources au sein de votre organisation dans toutes les AWS Organizations régions qui prennent en charge AWS Resource Access Manager (AWS RAM).	
Vérifiez ou approvisionnez les comptes de l'application.	Pour configurer de nouveaux comptes d'application pour votre cas d'utilisation, créez-les via AFT. Pour plus d'informations, voir Provisionner un nouveau compte avec AFT dans la AWS Control Tower documentation.	Administrateur AWS

Configuration des fichiers de configuration pour les comptes d'applications

Tâche	Description	Compétences requises
Copiez `Application_account` le contenu du dossier dans le `aft-account-customizations` référentiel.	1. Créez un dossier nommé `Application_account` dans le chemin racine du `aft-account-customizations` référentiel. Ce dépôt est créé automatiquement lorsque vous configurez AFT (voir l'épopée précédente). 2. Accédez au répertoire racine du scale-using-terraform référentiel centralised-logging-at-enterprise-, copiez le contenu du `aft/account` répertoire, puis collez-le dans le `Application_account` répertoire que vous avez créé à l'étape 1 du `aft-account-customizations` référentiel. 3. À partir du répertoire racine du `centralised-logging-at-enterprise-scale-using-terraform` référentiel, copiez le contenu du `Application_account` répertoire dans le `Application_account/terraform` répertoir	DevOps ingénieur

Tâche	Description	Compétences requises
	e du `aft-account-customizations` référentiel. 4. Dans le `aft-account-customizations/Application_account/terraform.tfvars` fichier, vérifiez que tous les paramètres sont transmis en tant qu'arguments dans les fichiers de configuration Terraform correspondants.	

Tâche	Description	Compétences requises
Vérifiez et modifiez les paramètres d'entrée pour configurer le compte de l'application.	Au cours de cette étape, vous configurez le fichier de configuration pour créer des ressources dans les comptes d'applications, notamment les groupes de CloudWatch journaux, les filtres CloudWatch d'abonnement, les rôles et politiques IAM, ainsi que les détails de configuration pour les fonctions Amazon RDS, Amazon EKS et Lambda. Dans votre `aft-account-customizations` référentiel, dans le `Application_account` dossier, configurez les paramètres d'entrée du `terraform.tfvars` fichier en fonction des exigences de votre organisation : • `environment` : nom de l'environnement (par exemple,, `proddev`,`staging`) dans lequel les ressources seront déployées. • `account_name` : nom de l'Compte AWS endroit où les ressources seront créées. • `log_archive_account_id` : Compte AWS ID	DevOps ingénieur

Tâche	Description	Compétences requises
	dans lequel les journaux seront archivés. • `admin_role_name` : nom du rôle administratif qui sera utilisé pour gérer les ressources. • `tags`: carte de paires clé-valeur représentant des balises communes à appliquer à toutes les ressources. • `rds_config` : objet contenant les détails de configuration des instances Amazon RDS. • `allowed_cidr_blocks` : liste des blocs CIDR autorisés à accéder aux ressources. • `destination_name:` Variable utilisée pour créer le nom de ressource Amazon (ARN) de la CloudWatch destination où les journaux seront diffusés. • `rds_parameters:` Objet contenant les paramètres du groupe de paramètres Amazon RDS. • `vpc_config` : objet contenant les détails de configuration du VPC.	

Tâche	Description	Compétences requises
	• `eks_config` : objet contenant les détails de configuration des clusters Amazon EKS. • `lambda_config` : objet contenant les détails de configuration des fonctions Lambda. • `restrictive_cidr_range` : liste de plages CIDR restrictives pour les règles des groupes de sécurité. • `target_account_id` : Compte AWS ID du compte Log Archive cible sur lequel les ressources seront déployées.	

Configuration des fichiers de configuration pour le compte Log Archive

Tâche	Description	Compétences requises
Copiez `Log_archive_account` le contenu du dossier dans le `aft-account-customizations` référentiel.	1. Créez un dossier nommé `Log_archive_account` dans le chemin racine du `aft-account-customizations` dépôt. Ce dépôt est créé automatiquement lorsque vous configurez AFT. 2. Accédez au répertoire racine du `centralised-logging-at-ente`	DevOps ingénieur

Tâche	Description	Compétences requises
	`rprise-scale-using-terraform` référentiel, copiez le contenu du `aft/account` répertoire, puis collez-le dans le `Log_archive_account` répertoire que vous avez créé à l'étape précédente dans le `aft-account-customizations` référentiel. 3. À partir du répertoire racine du `centralised-logging-at-enterprise-scale-using-terraform` référentiel, copiez le contenu du `Log_archive_account` répertoire dans le `Log_archive_account/terraform` répertoire du `aft-account-customizations` référentiel. 4. Dans le `aft-account-customizations/Log_archive_account/terraform.tfvars` fichier, vérifiez que tous les paramètres sont transmis en tant qu'arguments dans les fichiers de configuration Terraform correspondants.	

Tâche	Description	Compétences requises
Vérifiez et modifiez les paramètres d'entrée pour configurer le compte Log Archive.	Au cours de cette étape, vous configurez le fichier de configuration pour créer des ressources dans le compte Log Archive, notamment les flux de diffusion Firehose, les compartiments S3, les files d'attente SQS, ainsi que les rôles et politiques IAM. Dans le `Log_archive_account` dossier de votre `aft-account-customizations` référentiel, configurez les paramètres d'entrée dans le `terraform.tfvars` fichier en fonction des exigences de votre organisation : • `environment` : nom de l'environnement (par exemple,, `proddev`,`staging`) dans lequel les ressources seront déployées. • `destination_name` : variable utilisée pour créer l'ARN de la CloudWatch destination où les journaux seront diffusés. • `source_account_ids` : une liste de ceux Compte AWS IDs qui sont autorisés à placer des	DevOps ingénieur

Tâche	Description	Compétences requises
	filtres d'abonnement sur la destination du journal. Vous pouvez saisir autant de comptes IDs que vous souhaitez activer pour une journalisation centralisée.	

Exécutez des commandes Terraform pour provisionner des ressources

Tâche	Description	Compétences requises

Option 1 - Déployez les fichiers de configuration Terraform depuis AFT.	Dans AFT, le pipeline AFT est déclenché une fois que vous avez envoyé le code contenant les modifications de configuration dans le GitHub `aft-account-customizations` référentiel. AFT détecte automatiquement les modifications et lance le processus de personnalisation du compte.
	
	Après avoir apporté des modifications à vos fichiers Terraform (`terraform.tfvars`), validez et transférez vos modifications dans votre référentiel : `aft-account-customizations`
	
	`$ git add *`
	`$ git commit -m "update message"`
		DevOps ingénieur

Tâche	Description	Compétences requises
	`$ git push origin main` **Note** Si vous utilisez une autre branche (par exemple`dev`), remplacez-la `main` par le nom de votre succursale.	

Tâche	Description	Compétences requises

Option 2 - Déployez le fichier de configuration Terraform manuellement.	Si vous n'utilisez pas AFT ou si vous souhaitez déployer la solution manuellement, vous pouvez utiliser les commandes Terraform suivantes à partir des dossiers `Application_account` et `Log_archive_account` :
	1. Clonez le GitHub référentiel et configurez les paramètres d'entrée dans le `terraform.tfvars` fichier.
	2. Exécutez la commande suivante :
	`$ terraform init`
	3. Aperçu des modifications :
	`$ terraform plan`
	Cette commande évalue la configuration Terraform pour déterminer l'état souhaité des ressources et le compare à l'état actuel de votre infrastructure.
	4. Appliquer les modifications :
	`$ terraform apply`
		DevOps ingénieur

Tâche	Description	Compétences requises
	5. Passez en revue les modifications prévues et tapez « oui » à l'invite pour poursuivre le traitement de la demande.	

Valider les ressources

Tâche	Description	Compétences requises
Vérifiez les filtres d'abonnement.	Pour vérifier que les filtres d'abonnement transfèrent correctement les journaux des groupes de journaux du compte de l'application vers le compte Log Archive : 1. Dans le compte de l'application, ouvrez la CloudWatch console. 2. Dans le volet de navigation de gauche, choisissez Groupes de journaux. 3. Sélectionnez chaque groupe de journaux (`/aws/rds`,`/aws/eks`,`/aws/lambda`) et choisissez l'onglet Filtres d'abonnement. Vous devriez voir des filtres d'abonnement actifs pointant vers l'ARN de destination, en fonction du	DevOps ingénieur

Tâche	Description	Compétences requises
	nom que vous avez spécifié dans le fichier de configuration Terraform. 4. Choisissez n'importe quel filtre d'abonnement pour vérifier sa configuration et son statut.	
Vérifiez les streams Firehose.	Pour vérifier que les streams Firehose contenus dans le compte Log Archive traitent correctement les journaux de l'application : 1. Dans le compte Log Archive, ouvrez la console Firehose. 2. Dans le volet de navigation de gauche, choisissez Firehose streams. 3. Choisissez n'importe quel stream Firehose et vérifiez les points suivants : • La destination indique le compartiment S3 approprié. • L'onglet Surveillance affiche les indicateurs de livraison réussis. • L'horodatage de livraison récent est à jour.	DevOps ingénieur

Tâche	Description	Compétences requises
Validez les compartiments S3 centralisés.	Pour vérifier que les compartiments S3 centralisés reçoivent et organisent correctement les journaux : 1. Dans le compte Log Archive, ouvrez la console Amazon S3. 2. Sélectionnez chaque compartiment de journalisation central. 3. Naviguez dans la structure des dossiers : AWSLogs/AccountID/Region/Service. Vous devriez voir les fichiers journaux organisés par timestamp () YYYY/MM/DD/HH. 4. Choisissez n'importe quel fichier journal récent et vérifiez son format et l'intégrité des données.	DevOps ingénieur

Tâche	Description	Compétences requises
Validez les files d'attente SQS.	Pour vérifier que les files d'attente SQS reçoivent des notifications pour les nouveaux fichiers journaux : 1. Dans le compte Log Archive, ouvrez la console Amazon SQS. 2. Dans le volet de navigation de gauche, choisissez Files d'attente. 3. Sélectionnez chaque file d'attente configurée et choisissez Envoyer et recevoir des messages. Vous devriez voir des messages contenant des notifications d'événements S3 pour les nouveaux fichiers journaux. 4. Choisissez un message pour vérifier qu'il contient les informations correctes sur l'objet S3.	DevOps ingénieur

Nettoyage des ressources

Tâche	Description	Compétences requises
Option 1 - Désaffecter le fichier de configuration Terraform d'AFT.	Lorsque vous supprimez les fichiers de configuration Terraform et que vous appliquez les modifications,	DevOps ingénieur

Tâche	Description	Compétences requises

	AFT lance automatiquement le processus de suppression des ressources.
	
	1. Accédez au `aft-account-customizations` référentiel.
	2. Accédez au répertoire `terraform` .
	3. Supprimez les fichiers suivants :
	• `modules`annuaire
	• `iam.tf`
	• `versions.tf`
	• `variables.tf`
	• `outputs.tf`
	• `terraform.tfvars`
	4. Effacez le contenu du `main.tf` fichier.
	5. Transférez vos modifications au dépôt :
	
	`# Stage all changes`
	`$ git add *`
	
	`# Commit cleanup changes`
	`$ git commit -m "Remove AFT customizations"`
	
	`# Push to repository`
	`$ git push origin main`	

Tâche	Description	Compétences requises
	Note Si vous utilisez une autre branche (par exemple`dev`), remplacez-la `main` par le nom de votre succursale.	

Tâche	Description	Compétences requises

Option 2 — Nettoyez les ressources Terraform manuellement.	Si vous n'utilisez pas AFT ou si vous souhaitez nettoyer les ressources manuellement, utilisez les commandes Terraform suivantes à partir des dossiers `Application_account` et `Log_archive_account` :
	1. Initialisez la configuration Terraform :
	`$ terraform init`
	Cette commande initialise Terraform et garantit l'accès à l'état actuel.
	2. Prévisualisez les modifications apportées lors du nettoyage :
	`$ terraform destroy`
	Cette commande évalue les ressources qui seront détruites et compare l'état souhaité avec l'état actuel de votre infrastructure.
	3. Exécutez le nettoyage. Lorsque vous y êtes invité, tapez oui pour confirmer et exécuter le plan de destruction.
		DevOps ingénieur

Résolution des problèmes

Problème	Solution
La destination CloudWatch Logs n'a pas été créée ou est inactive.	Validez les éléments suivants : 1. Dans le compte Log Archive, vérifiez que la politique de destination inclut : • Le principal du compte source correct. • L'action correcte (`logs:PutSubscriptionFilter`). • Un ARN de destination valide. 2. Vérifiez que le stream Firehose existe et qu'il est actif. 3. Vérifiez que le rôle IAM associé à la destination dispose d'autorisations pour Firehose.
Le filtre d'abonnement a échoué ou est bloqué en attente.	Vérifiez les éléments suivants : 1. Dans le compte d'application, vérifiez que le rôle IAM possède : • Autorisations d'appel`PutSubscriptionFilter`. • Une relation de confiance avec CloudWatch Logs. 2. Vérifiez que l'ARN de destination est correct. 3. Consultez les CloudWatch journaux pour voir s'il existe des messages d'erreur spécifiques.
Le flux de livraison Firehose n'affiche aucun enregistrement entrant.	Vérifiez les paramètres suivants : 1. Vérifiez que le rôle Firehose IAM possède les caractéristiques suivantes : • Autorisations pour écrire sur Amazon S3. • Accès à la AWS KMS clé si le chiffrement est activé.

Problème	Solution
	2. Passez en revue CloudWatch les métriques pour : • `IncomingRecords` • `DeliveryToS3.Records` 3. Vérifiez les paramètres de la mémoire tampon et les configurations de livraison.

Ressources connexes

- Configuration de l'infrastructure Terraform (documentation Terraform)
- Déployer AWS Control Tower Account Factory pour Terraform (AFT) (AWS Control Tower documentation)
- Tutoriel IAM : Déléguer l'accès à l' Comptes AWS aide de rôles IAM () IAMdocumentation

Configurer le end-to-end chiffrement des applications sur Amazon EKS à l'aide du gestionnaire de certificats et de Let's Encrypt

Créée par Mahendra nasiddappa (AWS) et Vasanth Jeyaraj (AWS)

Récapitulatif

La mise en œuvre du end-to-end chiffrement peut être complexe et vous devez gérer les certificats pour chaque actif de votre architecture de microservices. Bien que vous puissiez mettre fin à la connexion TLS (Transport Layer Security) à la périphérie du réseau Amazon Web Services (AWS) à l'aide d'un Network Load Balancer ou d'Amazon API Gateway, certaines organisations end-to-end exigent le chiffrement.

Ce modèle utilise le contrôleur d'entrée NGINX pour l'entrée. En effet, lorsque vous créez une entrée Kubernetes, la ressource d'entrée utilise un Network Load Balancer. Le Network Load Balancer n'autorise pas le téléchargement de certificats clients. Par conséquent, vous ne pouvez pas obtenir un TLS mutuel avec Kubernetes Ingress.

Ce modèle est destiné aux organisations qui ont besoin d'une authentification mutuelle entre tous les microservices de leurs applications. Le protocole TLS mutuel réduit le fardeau lié à la gestion des noms d'utilisateur ou des mots de passe et peut également utiliser le cadre de sécurité clé en main. L'approche de ce modèle est compatible si votre entreprise possède un grand nombre d'appareils connectés ou doit se conformer à des directives de sécurité strictes.

Ce modèle permet d'améliorer le niveau de sécurité de votre entreprise en implémentant le end-to-end chiffrement pour les applications exécutées sur Amazon Elastic Kubernetes Service (Amazon EKS). Ce modèle fournit un exemple d'application et de code dans le référentiel de GitHub End-to-end chiffrement sur Amazon EKS pour montrer comment un microservice fonctionne avec le end-to-end chiffrement sur Amazon EKS. L'approche du modèle utilise cert-manager, un module complémentaire de Kubernetes, avec Let's Encrypt comme autorité de certification (CA). Let's Encrypt est une solution rentable pour gérer les certificats et fournit des certificats gratuits valables pendant 90 jours. Cert-Manager automatise le provisionnement à la demande et la rotation des certificats lorsqu'un nouveau microservice est déployé sur Amazon EKS.

Public visé

Ce modèle est recommandé aux utilisateurs qui ont de l'expérience avec Kubernetes, TLS, Amazon Route 53 et le système de noms de domaine (DNS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un cluster Amazon EKS existant.
- Interface de ligne de commande AWS (AWS CLI) version 1.7 ou ultérieure, installée et configurée sur macOS, Linux ou Windows.
- L'utilitaire de ligne de `kubectl` commande, installé et configuré pour accéder au cluster Amazon EKS. Pour plus d'informations à ce sujet, consultez la section Installation de kubectl dans la documentation Amazon EKS.
- Nom DNS existant pour tester l'application. Pour plus d'informations à ce sujet, consultez la section Enregistrement de noms de domaine à l'aide d'Amazon Route 53 dans la documentation Amazon Route 53.
- La dernière version de Helm, installée sur votre machine locale. Pour plus d'informations à ce sujet, consultez la section Utilisation de Helm avec Amazon EKS dans la documentation Amazon EKS et dans le référentiel GitHub Helm.
- Le GitHub End-to-end chiffrement sur le référentiel Amazon EKS, cloné sur votre machine locale.
- Remplacez les valeurs suivantes dans les `trustpolicy.json` fichiers `policy.json` et du référentiel de GitHub End-to-end chiffrement cloné sur Amazon EKS :
  - `<account number>`— Remplacez-le par l'ID de compte AWS du compte dans lequel vous souhaitez déployer la solution.
  - `<zone id>`— Remplacez par l'ID de zone Route 53 du nom de domaine.
  - `<node_group_role>`— Remplacez par le nom du rôle AWS Identity and Access Management (IAM) associé aux nœuds Amazon EKS.
  - `<namespace>`— Remplacez par l'espace de noms Kubernetes dans lequel vous déployez le NGINX Ingress Controller et l'exemple d'application.
  - `<application-domain-name>`— Remplacez par le nom de domaine DNS de Route 53.

Limites

- Ce modèle ne décrit pas comment alterner les certificats et montre uniquement comment utiliser les certificats avec des microservices sur Amazon EKS.

Architecture

Le schéma suivant montre les composants du flux de travail et de l'architecture de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Un client envoie une demande d'accès à l'application au nom DNS.
2. L'enregistrement Route 53 est un CNAME pour le Network Load Balancer.
3. Le Network Load Balancer transmet la demande au NGINX Ingress Controller configuré avec un écouteur TLS. La communication entre le NGINX Ingress Controller et le Network Load Balancer suit le protocole HTTPS.
4. Le NGINX Ingress Controller effectue un routage basé sur le chemin en fonction de la demande du client au service d'application.
5. Le service d'application transmet la demande au module d'application. L'application est conçue pour utiliser le même certificat en appelant des secrets.
6. Les pods exécutent l'exemple d'application à l'aide des certificats cert-manager. La communication entre le NGINX Ingress Controller et les pods utilise le protocole HTTPS.

> **Note**
>
> CERT-Manager s'exécute dans son propre espace de noms. Il utilise un rôle de cluster Kubernetes pour fournir des certificats sous forme de secrets dans des espaces de noms spécifiques. Vous pouvez associer ces espaces de noms aux modules d'application et au NGINX Ingress Controller.

Outils

Services AWS

- Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré que vous pouvez utiliser pour exécuter Kubernetes sur AWS sans avoir à installer, exploiter et gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles, conteneurs et adresses IP.

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.

Autres outils

- cert-manager est un module complémentaire de Kubernetes qui demande des certificats, les distribue aux conteneurs Kubernetes et automatise le renouvellement des certificats.
- NGINX Ingress Controller est une solution de gestion du trafic pour les applications cloud natives dans Kubernetes et les environnements conteneurisés.

Épopées

Création et configuration d'une zone hébergée publique avec Route 53

Tâche	Description	Compétences requises
Créez une zone hébergée publique sur Route 53.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon Route 53, choisissez Hosted zones, puis Create hosted zone. Créez une zone hébergée publique et enregistrez l'ID de zone. Pour plus d'informations à ce sujet, consultez la section Création d'une zone hébergée publique dans la documenta tion Amazon Route 53. **Note** ACME DNS01 utilise le fournisseur DNS pour demander au gestionnaire de certificats de délivrer	AWS DevOps

Tâche	Description	Compétences requises
	le certificat. Ce défi vous demande de prouver que vous contrôlez le DNS de votre nom de domaine en saisissant une valeur spécifique dans un enregistrement TXT sous ce nom de domaine. Une fois que Let's Encrypt a fourni un jeton à votre client ACME, celui-ci crée un enregistrement TXT dérivé de ce jeton et de votre clé de compte, et place cet enregistrement à. `_acme-challenge.<YOURDOMAIN>` Let's Encrypt interroge ensuite le DNS pour cet enregistrement. S'il trouve une correspondance, vous pouvez procéder à l'émission d'un certificat.	

Configurer un rôle IAM pour autoriser le gestionnaire de certificats à accéder à la zone hébergée publique

Tâche	Description	Compétences requises
Créez la politique IAM pour cert-manager.	Une politique IAM est requise pour fournir à cert-manager l'autorisation de valider que vous êtes propriétaire du domaine Route 53. L'`policy.json` exemple de politique IAM est fourni dans le `1-IAMRole` répertoire du référentiel de GitHub End-to-end chiffrement cloné sur Amazon EKS. Entrez la commande suivante dans l'AWS CLI pour créer la politique IAM. `aws iam create-policy \ --policy-name PolicyForCertManager \ --policy-document file://policy.json`	AWS DevOps
Créez le rôle IAM pour cert-manager.	Après avoir créé la politique IAM, vous devez créer un rôle IAM. L'`trustpolicy.json` exemple de rôle IAM est fourni dans le `1-IAMRole` répertoire. Entrez la commande suivante dans l'interface de ligne de	AWS DevOps

Tâche	Description	Compétences requises
	commande AWS pour créer le rôle IAM. `aws iam create-role \ --role-name RoleForCertManager \ --assume-role-policy-document file://trustpolicy.json`	
Attachez la stratégie au rôle.	Entrez la commande suivante dans l'AWS CLI pour associer la politique IAM au rôle IAM. `AWS_ACCOUNT_ID` Remplacez-le par l'ID de votre compte AWS. `aws iam attach-role-policy \ --policy-arn arn:aws:iam::AWS_ACCOUNT_ID:policy/PolicyForCertManager \ --role-name RoleForCertManager`	AWS DevOps

Configurer le NGINX Ingress Controller dans Amazon EKS

Tâche	Description	Compétences requises
Déployez le NGINX Ingress Controller.	Installez la version la plus récente d'`nginx-ingress` utilisation de Helm. Vous pouvez modifier la `nginx-ingress` configuration en fonction de vos	AWS DevOps

Tâche	Description	Compétences requises
	besoins avant de la déployer. Ce modèle utilise un Network Load Balancer annoté et orienté vers l'interne, disponible dans le répertoire. `5-Nginx-Ingress-Controller` Installez le NGINX Ingress Controller en exécutant la commande Helm suivante depuis le répertoire. `5-Nginx-Ingress-Controller` `helm install test-nginx nginx-stable/nginx-ingress -f 5-Nginx-Ingress-Controller/values_internal_nlb.yaml`	
Vérifiez que le NGINX Ingress Controller est installé.	Entrez la commande `helm list`. La sortie doit indiquer que le NGINX Ingress Controller est installé.	AWS DevOps

Tâche	Description	Compétences requises
Créez un enregistrement Route 53 A.	L'enregistrement A pointe vers le Network Load Balancer créé par NGINX Ingress Controller. 1. Obtenez le nom DNS du Network Load Balancer. Pour obtenir des instructions, voir Obtenir le nom DNS d'un équilibreur de charge ELB. 2. Sur la console Amazon Route 53, choisissez Hosted Zones. 3. Sélectionnez la zone hébergée publique dans laquelle vous souhaitez créer l'enregistrement, puis choisissez Créer un enregistrement. 4. Entrez un nom pour l'enregistrement. 5. Dans Type d'enregistrement, choisissez A - Route le trafic vers IPv4 et certaines ressources AWS. 6. Activez Alias. 7. Dans Acheminer le trafic vers, procédez comme suit : a. Choisissez Alias to Network Load Balancer. b. Choisissez la région AWS dans laquelle le	AWS DevOps

Tâche	Description	Compétences requises
	Network Load Balancer est déployé. c. Entrez le nom DNS du Network Load Balancer. 8. Choisissez Créer des enregistrements.	

Configurer NGINX VirtualServer sur Amazon EKS

Tâche	Description	Compétences requises
Déployez NGINX VirtualServer.	La VirtualServer ressource NGINX est une configuration d'équilibrage de charge qui constitue une alternative à la ressource d'entrée. La configuration permettant de créer la VirtualServer ressource NGINX est disponible dans le `nginx_virtualserver.yaml` fichier du répertoire. `6-Nginx-Virtual-Server` Entrez la commande suivante `kubectl` pour créer la ressource NGINX VirtualServer . `kubectl apply -f nginx_virtualserver.yaml`	AWS DevOps

Tâche	Description	Compétences requises
	Important Assurez-vous de mettre à jour le nom de domaine de l'application, le secret du certificat et le nom du service de l'application dans le `nginx_virtualserver.yaml` fichier.	
Vérifiez que NGINX VirtualServer est créé.	Entrez la commande suivante `kubectl` pour vérifier que la VirtualServer ressource NGINX a été créée avec succès. `kubectl get virtualserver` **Note** Vérifiez que la `Host` colonne correspond au nom de domaine de votre application.	AWS DevOps

Tâche	Description	Compétences requises
Déployez le serveur Web NGINX avec le protocole TLS activé.	Ce modèle utilise un serveur Web NGINX avec TLS activé comme application pour tester le chiffrement. end-to-end Les fichiers de configuration requis pour déployer l'application de test sont disponibles dans le `demo-webserver` répertoire. Entrez la commande suivante `kubectl` pour déployer l'application de test. `kubectl apply -f nginx-tls-ap.yaml`	AWS DevOps

Tâche	Description	Compétences requises
Vérifiez que les ressources de l'application de test sont créées.	Entrez les commandes suivantes `kubectl` pour vérifier que les ressources requises sont créées pour l'application de test : • `kubectl get deployments` **Note** Validez la `Ready` colonne et `Available` la colonne. • `kubectl get pods | grep -i example-deploy` **Note** Les capsules doivent être en bon `running` état. • `kubectl get configmap` • `kubectl get svc`	AWS DevOps

Tâche	Description	Compétences requises
Validez l'application.	1. Entrez la commande suivante en `<application-domain-name>` remplaçant le par le nom DNS Route53 que vous avez créé précédemment. `curl --verbose https://<application-domain-name>` 2. Vérifiez que vous pouvez accéder à l'application.	AWS DevOps

Ressources connexes

Ressources AWS

- Création d'enregistrements à l'aide de la console Amazon Route 53 (documentation Amazon Route 53)
- Utilisation d'un Network Load Balancer avec le contrôleur d'entrée NGINX sur Amazon EKS (article de blog AWS)

Autres ressources

- Route 53 (documentation du gestionnaire de certificats)
- Configuration du fournisseur de défis DNS01 (documentation du gestionnaire de certificats)
- Défi DNS Let's Encrypt (documentation Let's Encrypt)

Simplifiez le déploiement d'applications multi-locataires Amazon EKS à l'aide de Flux

Créée par Nadeem Rahaman (AWS), Aditya Ambati (AWS), Aniket Dekate (AWS) et Shrikant Patil (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

De nombreuses entreprises qui proposent des produits et services sont des secteurs réglementés par les données qui sont tenus de maintenir des barrières entre leurs fonctions commerciales internes. Ce modèle décrit comment vous pouvez utiliser la fonctionnalité multi-tenant d'Amazon Elastic Kubernetes Service (Amazon EKS) pour créer une plate-forme de données qui assure une isolation logique et physique entre les locataires ou les utilisateurs qui partagent un seul cluster Amazon EKS. Le modèle fournit une isolation par le biais des approches suivantes :

- Isolation de l'espace de noms Kubernetes
- Contrôle d’accès basé sur les rôles (RBAC)
- Stratégies réseau
- Quotas de ressources
- AWS Identity and Access Management Rôles (IAM) pour les comptes de service (IRSA)

En outre, cette solution utilise Flux pour maintenir la configuration du locataire immuable lorsque vous déployez des applications. Vous pouvez déployer vos applications mutualisées en spécifiant le référentiel client qui contient le `kustomization.yaml` fichier Flux dans votre configuration.

Ce modèle implémente les éléments suivants :

- Un AWS CodeCommit référentiel, AWS CodeBuild des projets et un AWS CodePipeline pipeline, créés en déployant manuellement des scripts Terraform.
- Composants réseau et informatiques nécessaires à l'hébergement des locataires. Ils sont créés CodeBuild par CodePipeline et à l'aide de Terraform.
- Les espaces de noms des locataires, les politiques réseau et les quotas de ressources, qui sont configurés via un diagramme de Helm.
- Applications appartenant à différents locataires, déployées à l'aide de Flux.

Nous vous recommandons de planifier et de créer avec soin votre propre architecture pour la mutualisation en fonction de vos exigences uniques et de vos considérations de sécurité. Ce modèle constitue un point de départ pour votre mise en œuvre.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- AWS Command Line Interface (AWS CLI) version 2.11.4 ou ultérieure, installée et configurée
- Terraform version 0.12 ou ultérieure installée sur votre machine locale
- Terraform AWS Provider version 3.0.0 ou ultérieure
- Kubernetes Provider version 2.10 ou ultérieure
- Helm Provider version 2.8.0 ou ultérieure
- Kubectl Provider version 1.14 ou ultérieure

Limites

- Dépendance à l'égard des déploiements manuels de Terraform : La configuration initiale du flux de travail, y compris la création de CodeCommit référentiels, de CodeBuild projets et de CodePipeline pipelines, repose sur des déploiements manuels de Terraform. Cela introduit une limite potentielle en termes d'automatisation et d'évolutivité, car cela nécessite une intervention manuelle pour les modifications de l'infrastructure.
- CodeCommit dépendance aux référentiels : le flux de travail repose sur CodeCommit les référentiels en tant que solution de gestion du code source et est étroitement associé Services AWSà.

Architecture

Architectures cibles

Ce modèle déploie trois modules pour créer le pipeline, le réseau et l'infrastructure de calcul d'une plate-forme de données, comme illustré dans les diagrammes suivants.

Architecture du pipeline :

Architecture réseau :

Architecture de calcul :

Outils

Services AWS

- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous permet d'exécuter AWS Kubernetes sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Transit Gatewayest un hub central qui connecte des clouds privés virtuels (VPCs) et des réseaux sur site.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Autres outils

- Les politiques réseau de Cilium prennent en charge les politiques réseau Kubernetes L3 et L4. Ils peuvent être étendus avec des politiques L7 afin de fournir une sécurité au niveau de l'API pour HTTP, Kafka et gRPC, ainsi que pour d'autres protocoles similaires.
- Flux est un outil de diffusion continue (CD) basé sur Git qui automatise les déploiements d'applications sur Kubernetes.
- Helm est un gestionnaire de packages open source pour Kubernetes qui vous aide à installer et à gérer des applications sur votre cluster Kubernetes.
- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub EKS Multi-Tenancy Terraform Solution.

Bonnes pratiques

Pour les directives et les meilleures pratiques relatives à l'utilisation de cette implémentation, consultez les rubriques suivantes :

- Bonnes pratiques en matière de location multiple Amazon EKS
- Documentation sur les flux

Épopées

Créez des pipelines pour les étapes de construction, de test et de déploiement de Terraform

Tâche	Description	Compétences requises
Clonez le référentiel du projet.	Clonez le référentiel GitHub EKS Multi-Tenancy Terraform Solution en exécutant la commande suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/aws-eks-multitenancy-deployment.git`	AWS DevOps
Démarrez le compartiment Terraform S3 et Amazon DynamoDB.	1. Dans le `bootstrap` dossier, ouvrez le `bootstrap.sh` fichier et mettez à jour les valeurs des variables pour le nom du compartiment S3, le nom de la table DynamoDB et : Région AWS	AWS DevOps

Tâche	Description	Compétences requises

	<pre>S3_BUCKET_NAME="<S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME="<DYNAMODB_NAME>" REGION="<AWS_REGION>"</pre>
	2. Exécutez le script `bootstrap.sh` . Le script nécessite le AWS CLI, que vous avez installé dans le cadre des prérequis.
	<pre>cd bootstrap
	./bootstrap.sh</pre>	

Tâche	Description	Compétences requises

Mettez à jour les `locals.tf` fichiers `run.sh` et.	1. Une fois le processus d'amorçage terminé avec succès, copiez le nom du compartiment S3 et de la table DynamoDB depuis `variables` la section du script : `bootstrap.sh`
	`# Variables S3_BUCKET_NAME="< S3_BUCKET_NAME>" DYNAMODB_TABLE_NAME ="<DYNAMODB_NAME"`
	2. Collez ces valeurs dans le `run.sh` script, qui se trouve dans le répertoire racine du projet :
	`BACKEND_BUCKET_ID= "<SAME_NAME_AS_S3_ BUCKET_NAME>" DYNAMODB_ID=" <SAME_NAME_AS_DYNA MODB_NAME>"`
	3. Téléchargez le code du projet dans un CodeCommi t référentiel. Vous pouvez créer automatiquement ce référentiel via Terraform en définissant la variable suivante sur `true` dans le `demo/pipeline/loca ls.tf` fichier :
		AWS DevOps

Tâche	Description	Compétences requises
	`create_new_repo = true` 4. Mettez à jour le `locals.tf` fichier en fonction de vos besoins pour créer des ressources de pipeline.	

Déployez le module de pipeline.	Pour créer des ressources de pipeline, exécutez manuellement les commandes Terraform suivantes. Il n'existe aucune orchestration pour exécuter ces commandes automatiquement.
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t init`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t plan`
	`./run.sh -m pipeline -e demo -r <AWS_REGION> -t apply`
		AWS DevOps

Création de l'infrastructure réseau

Tâche	Description	Compétences requises
Démarrez le pipeline.	1. Dans le `templates` dossier, assurez-vous que la variable suivante est définie sur les `buildspec` fichiers `network` :	AWS DevOps

Tâche	Description	Compétences requises
	`TF_MODULE_TO_BUILD: "network"` 2. Sur la CodePipeline console, sur la page des détails du pipeline, démarrez le pipeline en choisissant Libérer le changement. Après cette première exécution, le pipeline démarre automatiquement chaque fois que vous validez une modification dans la branche principale du CodeCommit référentiel. Le pipeline comprend les étapes suivantes : • `validate`initialise Terraform, exécute les scans de sécurité Terraform à l'aide des outils checkov et tfsec, et télécharge les rapports d'analyse dans le compartiment S3. • `plan` affiche le plan Terraform et télécharge le plan dans le compartiment S3. • `apply`applique la sortie du plan Terraform à partir du	

Tâche	Description	Compétences requises
	compartiment S3 et crée AWS des ressources. • `destroy`supprime les AWS ressources créées au cours de l'`apply`étape. Pour activer cette étape facultative, définissez la variable suivante sur `true` dans le `demo/pipeline/locals.tf` fichier : `enable_destroy_stage = true`	

Tâche	Description	Compétences requises
Validez les ressources créées via le module réseau.	Vérifiez que les AWS ressources suivantes ont été créées après le déploiement réussi du pipeline : • Un VPC de sortie avec trois sous-réseaux publics et trois sous-réseaux privés, une passerelle Internet et une passerelle NAT. • Un VPC Amazon EKS avec trois sous-réseaux privés. • Locataire 1 et locataire 2 VPCs avec trois sous-réseaux privés chacun. • Une passerelle de transit avec toutes les pièces jointes VPC et les itinéraires vers chaque sous-réseau privé. • Route de passerelle de transit statique pour le VPC de sortie Amazon EKS avec un bloc CIDR de destination de. `0.0.0.0/0` Cela est nécessaire pour permettre VPCs à tous d'avoir un accès Internet sortant via le VPC de sortie Amazon EKS.	AWS DevOps

Création de l'infrastructure informatique

Tâche	Description	Compétences requises

Mise `locals.tf` à jour pour permettre l'accès du CodeBuild projet au VPC.	Pour déployer les modules complémentaires pour le cluster privé Amazon EKS, le CodeBuild projet doit être attaché au VPC Amazon EKS.
	1. Dans le `demo/pipeline` dossier, ouvrez le `locals.tf` fichier et définissez la `vpc_enabled` variable sur`true`.
	2. Exécutez le `run.sh` script pour appliquer les modifications au module de pipeline :
	`demo/pipeline/locals.tf`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd init`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd plan`
	`./run.sh -m pipeline -env demo -region <AWS_REGION> -tfcmd apply`
		AWS DevOps

Mettez à jour les `buildspec` fichiers pour créer le module de calcul.	Dans le `templates` dossier, dans tous les fichiers `buildspec` YAML, définissez la valeur de la `TF_MODULE`	AWS DevOps

Tâche	Description	Compétences requises
	_TO_BUILD variable de network à compute : `TF_MODULE_TO_BUILD: "compute"`	

Tâche	Description	Compétences requises

Mettez à jour le `values` fichier du diagramme Helm de gestion des locataires.	1. Ouvrez le `values.yaml` fichier à l'emplacement suivant :
	`cd cfg-terraform/demo/compute/cfg-tenant-mgmt`
	Le fichier ressemble à ceci :
	`---`
	`global:`
	`  clusterRoles:`
	`  operator: platform-tenant`
	`  flux: flux-tenant-applier`
	`  flux:`
	`  tenantCloneBaseUrl: ${TEANT_BASE_URL}`
	`  repoSecret: ${TENANT_REPO_SECRET}`
	`tenants:`
	`  tenant-1:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 1Gi`
	`  flux:`
	`  path: overlays/tenant-1`
	`  tenant-2:`
	`  quotas:`
	`  limits:`
	`  cpu: 1`
	`  memory: 2Gi`
	`  flux:`
		AWS DevOps

Tâche	Description	Compétences requises

	<pre>path: overlays/
	tenant-2</pre>
	2. Dans les `tenants` sections `global` et, mettez à jour la configuration en fonction de vos besoins :
	• `tenantCloneBaseUrl` — Chemin vers le dépôt qui héberge le code pour tous les locataires (nous utilisons le même dépôt Git pour tous les locataires)
	• `repoSecret` — Le secret de Kubernetes qui contient les clés SSH et les hôtes connus pour s'authentifier auprès du référentiel Git du locataire global
	• `quotas`— Quotas de ressources Kubernetes que vous souhaitez appliquer à chaque locataire
	• `flux path`— Chemin d'accès aux fichiers YAML de l'application locataire dans le référentiel global des locataires	

Tâche	Description	Compétences requises
Validez les ressources de calcul.	Après avoir mis à jour les fichiers au cours des étapes précédentes, CodePipeline démarre automatiquement. Vérifiez qu'il a créé les AWS ressources suivantes pour l'infrastructure de calcul : • Cluster Amazon EKS avec point de terminaison privé • Nœuds de travail Amazon EKS • Modules complémentaires Amazon EKS : secrets externes`aws-loadb alancer-controller` , et `metrics-server` • GitOps module, graphique Flux Helm, graphique Cilium Helm et tableau Helm de gestion des locataires	AWS DevOps

Vérifiez la gestion des locataires et les autres ressources

Tâche	Description	Compétences requises
Validez les ressources de gestion des locataires dans Kubernetes.	Exécutez les commandes suivantes pour vérifier que les ressources de gestion des locataires ont été créées avec succès à l'aide de Helm. 1. Les espaces de noms des locataires ont été	AWS DevOps

Tâche	Description	Compétences requises

	créés, comme indiqué dans `values.yaml` :
	`kubectl get ns -A`
	2. Des quotas sont attribués à chaque espace de noms de locataires, comme indiqué dans `values.yaml` :
	`kubectl get quota --namespace=<tenant_namespace>`
	3. Les détails des quotas sont corrects pour chaque espace de noms de locataires :
	`kubectl describe quota cpu-memory-resource-quota-limit -n <tenant_namespace>`
	4. Les politiques du réseau Cilium ont été appliquées à chaque espace de noms de locataires :
	`kubectl get CiliumNetworkPolicy -A`	

Tâche	Description	Compétences requises

Vérifiez les déploiements d'applications clientes.	Exécutez les commandes suivantes pour vérifier que les applications clientes ont été déployées.
	
	1. Flux est capable de se connecter au CodeCommi t référentiel spécifié dans le GitOps module :
	
	`kubectl get gitreposi tories -A`
	
	2. Le contrôleur de personnal isation Flux a déployé les fichiers YAML dans le référentiel : CodeCommit
	
	`kubectl get kustomiza tions -A`
	
	3. Toutes les ressources de l'application sont déployées dans leurs espaces de noms de locataires :
	
	`kubectl get all -n <tenant_namespace>`
	
	4. Une entrée a été créée pour chaque locataire :
	
	`kubectl get ingress -n <tenant_namespace>`	

Résolution des problèmes

Problème	Solution

Vous recevez un message d'erreur similaire au suivant :
 	
`Failed to checkout and determine revision: unable to clone unknown error: You have successfully authenticated over SSH. You can use Git to interact with AWS CodeCommit.`
	Pour résoudre le problème, procédez comme suit :
	
	1. Vérifiez le référentiel de l'application locataire : un référentiel vide ou mal configuré est peut-être à l'origine de l'erreur. Assurez-vous que le référentiel d'applica tions client contient le code requis.
	2. Redéployer le `tenant_mgmt` module : dans le fichier de configuration du `tenant_mgmt` module, localisez le `app` bloc, puis définissez le `deploy` paramètre comme suit : `0`
	
	`deploy = 0`
	
	Après avoir exécuté la `apply` commande Terraform, redéfinissez la valeur du `deploy` paramètre en : 1
	
	`deploy = 1`
	
	3. Revérifiez le statut : après avoir exécuté les étapes précédentes, utilisez la commande suivante pour vérifier si le problème persiste :
	
	`kubectl get gitrepositories -A`
	
	Si cela persiste, pensez à approfondir les journaux de Flux pour plus de détails ou consultez le guide de dépannage général de Flux.

Ressources connexes

- Blueprints Amazon EKS pour Terraform
- Guides des meilleures pratiques Amazon EKS, section sur l'hébergement mutualisé
- Site web de Flux
- Site web de Helm

Informations supplémentaires

Voici un exemple de structure de référentiel pour le déploiement d'applications clientes :

```
applications
sample_tenant_app
### README.md
### base
#   ### configmap.yaml
#   ### deployment.yaml
#   ### ingress.yaml
#   ### kustomization.yaml
#   ### service.yaml
### overlays
    ### tenant-1
    #   ### configmap.yaml
    #   ### deployment.yaml
    #   ### kustomization.yaml
    ### tenant-2
        ### configmap.yaml
        ### kustomization.yaml
```

Abonnement de plusieurs points de terminaison de messagerie à une rubrique SNS à l'aide d'une ressource personnalisée

Créée par Ricardo Morais (AWS)

Récapitulatif

Remarque, août 2022 : AWS prend CloudFormation désormais en charge l'abonnement à plusieurs ressources via l'AWS::SNS::Topicobjet et son attribut Subscription.

Ce modèle décrit comment abonner plusieurs adresses e-mail pour recevoir des notifications provenant d'une rubrique Amazon Simple Notification Service (Amazon SNS). Il utilise une fonction AWS Lambda comme ressource personnalisée dans un modèle AWS CloudFormation . La fonction Lambda est associée à un paramètre d'entrée qui spécifie les points de terminaison de messagerie pour la rubrique SNS.

Actuellement, vous pouvez utiliser les objets du CloudFormation modèle AWS AWS::SNS::Topicet abonner des points AWS::SNS::Subscriptionde terminaison uniques à des rubriques SNS. Pour abonner plusieurs points de terminaison, vous devez invoquer l'objet plusieurs fois. En utilisant la fonction Lambda comme ressource personnalisée, vous pouvez abonner plusieurs points de terminaison via un paramètre d'entrée. Vous pouvez utiliser cette fonction Lambda comme ressource personnalisée dans n'importe quel modèle AWS CloudFormation .

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un profil AWS configuré dans votre environnement local avec une clé d'accès et une clé secrète.
- Autorisations pour les éléments suivants :
  - Rôle et politique d'AWS Identity and Access Management (IAM)
  - Fonction AWS Lambda
  - Amazon Simple Storage Service (Amazon S3) pour le téléchargement de la fonction Lambda
  - Rubrique et politique Amazon SNS
  - CloudFormation piles AWS

Limites

- Le code prend en charge les postes de travail Linux et macOS.

Versions du produit

- Interface de ligne de commande AWS (AWS CLI) version 2 ou ultérieure.

Architecture

Pile technologique cible

- AWS CloudFormation
- Amazon SNS
- AWS Lambda

Outils

Outils

- Version 2 de l'interface de ligne de commande AWS

Code

La pièce jointe inclut les fichiers suivants :

- Fonction Lambda : `lambda_function.py`
- CloudFormation Modèle AWS : `template.yaml`
- Deux fichiers de paramètres pour gérer les abonnements multiples ou uniques à des terminaux de messagerie : `parameters-multiple-values.json` (utilisés par défaut) et `parameters-one-value.json`

Pour déployer la pile, vous pouvez utiliser l'un ou l'autre des fichiers de paramètres. Pour spécifier plusieurs points de terminaison de messagerie :

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>
```

Pour spécifier un point de terminaison de messagerie unique :

```
./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json
```

Épopées

Option 1 - Déployer une rubrique SNS avec un seul abonnement par e-mail

Tâche	Description	Compétences requises
Configurez le point de terminaison de messagerie pour les abonnements aux rubriques SNS.	Modifiez le fichier `parameters-one-value.json` (joint) et modifiez la valeur du `pSNSNotificationsEmail` paramètre pour qu'il reflète l'adresse e-mail que vous souhaitez utiliser, par exemple `someone@example.com` .	
Déployez la CloudFormation pile AWS qui crée les ressources et l'abonnement.	Exécutez la commande deploy.sh avec le nom de votre profil AWS, votre région AWS et le `parameters-one-value.json` fichier. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION> -f parameters-one-value.json`	Rôle IAM avec les autorisations appropriées

Option 2 - Déployer une rubrique SNS avec deux abonnements e-mail ou plus

Tâche	Description	Compétences requises
Configurez les points de terminaison de messagerie pour les abonnements aux rubriques SNS.	Modifiez le fichier `parameters-multiple-values.json` (joint) et modifiez la valeur du `pSNSNotificationsEmail` paramètre pour refléter les adresses e-mail que vous souhaitez utiliser, séparées par des virgules, comme suit :`someone1@example.com, someone2@example.com` .	
Déployez la CloudFormation pile AWS qui crée les ressources et l'abonnement.	Exécutez la commande deploy.sh avec le nom de votre profil AWS et votre région AWS. Il n'est pas nécessaire de spécifier le `parameters-multiple-values.json` fichier car il est utilisé par défaut. `./deploy.sh -p <YOUR_AWS_PROFILE_NAME> -r <YOUR_AWS_PROFILE_REGION>`	Rôle IAM avec les autorisations appropriées

Option 3 - Déployer une rubrique SNS via un modèle AWS CloudFormation

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Créez une rubrique SNS via un CloudFormation modèle	Rôle IAM avec les autorisations appropriées

Tâche	Description	Compétences requises
	AWS, sans spécifier les points de terminaison d'abonnement dans l'objet du `AWS::SNS::Topic` modèle. Vous pouvez l'utiliser `template.yaml` dans la pièce jointe comme point de départ.	
Créez une politique de rubrique SNS.	Créez une politique de rubrique SNS dans le CloudFormation modèle AWS.	Rôle IAM avec les autorisations appropriées
Abonnez la liste des points de terminaison de messagerie à la rubrique SNS.	Sur la base de la liste des points de terminaison de messagerie (un ou plusieurs), abonnez les points de terminaison à la rubrique SNS que vous avez créée.	Rôle IAM avec les autorisations appropriées

Ressources connexes

Références

- Ressources CloudFormation personnalisées AWS (documentation AWS)
- Création de ressources CloudFormation personnalisées AWS avec Python, AWS Lambda et crhelper (article de blog)

Outils nécessaires

- Version 2 de l'interface de ligne de commande AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Coordonnez la dépendance des ressources et l'exécution des tâches à l'aide de la structure AWS Fargate WaitCondition hook

Créée par Stan Fan (AWS)

Récapitulatif

Ce modèle décrit le package WaitCondition hook (`waitcondition-hook-for-aws-fargate-task`) npm, qui est une solution native pour le cloud conçue pour orchestrer les tâches AWS Fargatedans les clusters Amazon Elastic Container Service (Amazon ECS).

Le WaitCondition crochet est une AWS Cloud Development Kit (AWS CDK) construction spécialement conçue pour être intégrée à AWS CloudFormation. Le WaitCondition hook fournit les fonctionnalités clés suivantes :

- Agit comme un mécanisme d'attente, interrompant l'exécution de la CloudFormation pile jusqu'à ce qu'une tâche Fargate spécifiée soit terminée, ce qui facilite les déploiements ordonnés et le provisionnement des ressources.
- Supports TypeScript et Python, ce qui le rend idéal pour les AWS CDK projets.
- Permet aux développeurs et aux architectes d'orchestrer les déploiements en coordonnant l'exécution des tâches et la gestion des ressources pour les applications conteneurisées sur. AWS
- Permet d'exécuter des tâches Fargate avec un ou plusieurs conteneurs intégrés dans CloudFormation un cycle de vie, de gérer les échecs de tâches et de rétablir la pile après un échec de tâche. CloudFormation
- Offre la flexibilité nécessaire pour ajouter des dépendances entre les ressources et les résultats d'exécution des tâches Fargate, en activant des tâches personnalisées ou en invoquant d'autres points de terminaison. Par exemple, vous pouvez suspendre une CloudFormation pile et attendre une migration de base de données (effectuée par une tâche Fargate) et allouer d'autres ressources qui peuvent dépendre du succès de la migration de base de données.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.

- AWS Cloud Development Kit (AWS CDK) Interface de ligne de commande (CLI) installée sur un poste de travail local. Pour plus d'informations, consultez la référence de la AWS CDK CLI dans la AWS CDK documentation.
- Gestionnaire de packages de nœuds (npm), installé sur un poste de travail local et configuré pour l'entrée AWS CDK . TypeScript Pour plus d'informations, consultez la section Téléchargement et installation de Node.js et de npm dans la documentation de npm.
- Yarn installé sur un poste de travail local. Pour plus d'informations, consultez la section Installation dans la documentation de Yarn.

Limites

- Cette solution est déployée sur un seul Compte AWS.
- Le code de retour attendu du conteneur est un gage `0` de réussite. Tout autre code de retour indique un échec et la CloudFormation pile sera annulée.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant montre l'architecture de construction.

Le diagramme montre le flux de travail de `waitcondition-hook-for-aws-fargate-task` :

1. `WaitCondition`et `WaitConditionHandler` sont prévus pour écouter la réponse des AWS Lambda fonctions.
2. En fonction du résultat de la tâche, le `CallbackFunction` ou le `ErrorHandlerFunction` est déclenché à la fin de la tâche Fargate.
3. La fonction Lambda envoie un signal SUCCEED ou FAILURE à. `WaitConditionHandler`
4. `WaitConditionHandler`continue à approvisionner les ressources si le résultat de l'exécution de la tâche Fargate aboutit, ou annule la pile en cas d'échec de la tâche.

Le schéma suivant montre un exemple de flux de travail pour effectuer une migration de base de données.

L'exemple de flux de travail utilise `waitcondition-hook-for-aws-fargate-task` cette structure pour effectuer une migration de base de données, comme suit :

1. Une instance Amazon Relational Database Service (Amazon RDS) est mise en service.
2. La `waitcondition-hook-for-aws-fargate-task` construction exécute la tâche de migration de base de données et suspend la pile en tant qu'instance Amazon Elastic Compute Cloud (Amazon EC2).
3. Si la tâche de migration se termine correctement, elle envoie un signal de réussite à CloudFormation. Dans le cas contraire, il envoie un signal d'échec à la pile CloudFormation et l'annule.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir l'infrastructure cloud dans le code et à la mettre en service AWS CloudFormation.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie à travers Comptes AWS et Régions AWS.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.
- AWS Fargatevous permet d'exécuter des conteneurs sans avoir à gérer de serveurs ou d' EC2 instances Amazon. Il est utilisé conjointement avec Amazon ECS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages de l'utilisation de l'infrastructure évolutive de AWS.

Autres outils

- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.
- Yarn est un gestionnaire de paquets open source que vous pouvez utiliser pour gérer les dépendances dans les JavaScript projets. Yarn peut vous aider à installer, mettre à jour, configurer et supprimer les dépendances des packages.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub waitcondition-hook-for-aws-fargate-task.

Bonnes pratiques

- Lorsque vous créez votre AWS CDK application, suivez les meilleures pratiques pour le développement et le déploiement d'une infrastructure cloud AWS CDK dans la documentation de AWS CDK la version 2.
- Pour AWS Fargate cette tâche, suivez les meilleures pratiques relatives aux images de conteneurs Amazon ECS dans la documentation Amazon ECS.

Épopées

Configurez le AWS CDK

Tâche	Description	Compétences requises
Installez le AWS CDK.	Pour installer le AWS CDK sur votre machine locale	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	ou dans un autre environnement, exécutez la commande suivante : `npm install -g aws-cdk@latest`	
Bootstrap le. AWS CDK	Le bootstrapping est le processus de préparation d'un environnement pour le déploiement. Pour démarrer votre AWS CDK boîte à outils pour la cible Compte AWS Région AWS, exécutez la commande suivante : `cdk bootstrap aws://ACCOUNT-NUMBER-1/REGION-1` Cette commande crée une CloudFormation pile nomméeCDKToolkit .	Architecte du cloud

Exécutez le WaitCondition crochet pour créer AWS Fargate des tâches

Tâche	Description	Compétences requises
Créez le projet CDK.	Créez un projet CDK dans le langage de votre choix. Ce modèle utilise TypeScript. Pour créer un projet CDK à l'aide de TypeScript, exécutez la commande suivante :	Architecte du cloud

Tâche	Description	Compétences requises
	`cdk init app –language typescript`	
Installez le package .	Exécutez `npm install` sur le chemin racine de votre projet CDK. Une fois la bibliothèque CDK installée , exécutez la commande suivante pour l'installer `waitcondition-hook-for-aws-fargate-task` : `yarn add waitcondition-hook-for-aws-fargate-task`	Architecte du cloud

Tâche	Description	Compétences requises
Créez votre application CDK et les composants Amazon ECS.	Créez votre projet CDK. Une ressource de définitio n de tâche Amazon ECS est requise. Pour plus d'informations sur la création d'une définition de tâche, consultez les définitions de tâches Amazon ECS dans la documentation Amazon ECS. L'exemple suivant utilise cette construction : `import * as cdk from 'aws-cdk-lib'; import { Vpc } from 'aws-cdk-lib/aws-ec2'; import * as ecr from 'aws-cdk-lib/aws-ecr'; import * as ecs from 'aws-cdk-lib/aws-ecs'; import { Construct } from 'constructs'; import { FargateRunner } from 'waitcondition-hook-for-aws-fargate-task'; import { Queue } from 'aws-cdk-lib/aws-sqs';`  `export class FargateRunnerStack extends cdk.Stack { constructor(scope: Construct, id: string,`	Architecte du cloud

Tâche	Description	Compétences requises

	props?: cdk.StackProps) {
	super(scope, id, props);
	// Define the VPC
	const vpc = new Vpc(this, 'MyVpc')
	// Define the Fargate Task
	const taskDefinition = new ecs.FargateTaskDefinition(this, 'MyTask', {});
	// Import exiting ecr repo
	const repo = ecr.Repository.fromRepositoryName(this, 'MyRepo', 'RepoName');
	// Add a container to the task
	taskDefinition.addContainer('MyContainer', {
	image: ecs.ContainerImage.fromEcrRepository(repo),
	});
	// Create the Fargate runner
	const myFargateRunner = new FargateRunner(this, 'MyRunner', {
	fargateTaskDef: taskDefinition,
	timeout: `${60 * 5}`,
	vpc: vpc,
	});	

Tâche	Description	Compétences requises
	`// Create the SQS queue const myQueue = new Queue(this, 'MyQueue', {}); // Add dependency myQueue.node.addDependency(myFargateRunner); } }`	
Synthétisez et lancez l'application CDK.	1. Pour générer les ressources et le CloudFormation modèle, exécutez la commande suivante dans le chemin racine de votre CDK : `cdk synth` 2. Une fois la `synth` commande réussie, exécutez la commande suivante pour déployer les ressources : `cdk deploy` La `waitcondition-hook-for-aws-fargate-task` construction exécute la tâche Fargate.	Architecte du cloud

Nettoyage

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour nettoyer les ressources mises en service à partir de l'étape précédente, exécutez la commande suivante : `cdk destroy`	Architecte du cloud

Résolution des problèmes

Problème	Solution
Défaillance générale de la CloudFormation pile	Pour aider à résoudre les défaillances générales du CloudFormation stack, ajoutez l'`--no-rollback` indicateur comme indiqué dans l'exemple suivant : `cdk deploy --no-rollback` Cette commande interrompt la restauration de la CloudFormation pile, ce qui vous donne les ressources nécessaires pour résoudre les problèmes. Pour plus d'informations, consultez la section Choisir le mode de gestion des défaillances lors du provisionnement des ressources dans la AWS CloudFormation documentation.
AWS Step Functions échec	Une machine à AWS Step Functions états peut ne pas s'exécuter pour différentes raisons. Une `–disable-rollback` fois configuré, procédez comme suit pour résoudre les problèmes :

Problème	Solution
	1. Connectez-vous au AWS Management Console, saisissez Step Functions dans le champ de recherche, puis choisissez le service Step Functions. 2. Dans le volet de navigation de gauche, choisissez State machines, puis sélection nez la machine d'état provisionnée par la CloudFormation pile. 3. Dans Exécutions, choisissez le nom de l'exécution qui a échoué de façon inattendu e. 4. Dans la vue Evénements, choisissez l'étape qui a échoué. Pour plus d'informations, consultez les sections Résolution des problèmes dans Step Functions et Affichage des détails d'exécution dans la console Step Functions de la AWS Step Functions documentation.

Problème	Solution
AWS Lambda échec de fonction	Cette construction fournit deux fonctions Lambda : `CallbackFunction` et. `ErrorhandlerFunction` Ils peuvent échouer pour diverses raisons, telles que des exceptions non gérées. Pour résoudre les problèmes, procédez comme suit : 1. Connectez-vous au AWS Management Console, entrez CloudWatchdans le champ Rechercher, puis choisissez le CloudWatch service. 2. Dans le volet de navigation de gauche, choisissez Groupes de journaux. 3. Dans le champ Rechercher, entrez le nom de la fonction Lambda. 4. Choisissez le nom du groupe de journaux associé à la fonction Lambda. 5. Pour accéder au résultat de l'exécution de la fonction Lambda, choisissez le dernier flux de log. Pour plus d'informations, consultez la section Résolution des problèmes liés à Lambda dans la AWS Lambda documentation.

Ressources connexes

AWS documentation

- AWS CDK Référence d'API Construct
- Commencer à utiliser le AWS CDK
- Découvrez comment créer et utiliser les ressources Amazon ECS
- Découvrez comment démarrer avec Step Functions

- Qu'est-ce que c'est AWS CDK ?

Autres ressources

- Waitcondition Hook pour la AWS Fargate tâche (npm)
- waitcondition-hook-for-aws-fargate-task 1.0.6 (pypi.org)

Utiliser des référentiels sources Git tiers dans AWS CodePipeline

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle décrit comment utiliser AWS CodePipeline avec des référentiels sources Git tiers.

AWS CodePipeline est un service de livraison continue qui automatise les tâches de création, de test et de déploiement de vos logiciels. Le service prend actuellement en charge les référentiels Git gérés par GitHub AWS CodeCommit et Atlassian Bitbucket. Toutefois, certaines entreprises utilisent des référentiels Git tiers intégrés à leur service d'authentification unique (SSO) et à Microsoft Active Directory pour l'authentification. Vous pouvez utiliser ces référentiels Git tiers comme sources en CodePipeline créant des actions personnalisées et des webhooks.

Un webhook est une notification HTTP qui détecte des événements dans un autre outil, tel qu'un GitHub référentiel, et connecte ces événements externes à un pipeline. Lorsque vous créez un webhook dans CodePipeline, le service renvoie une URL que vous pouvez utiliser dans le webhook de votre dépôt Git. Si vous envoyez du code à une branche spécifique du référentiel Git, le webhook Git initie le CodePipeline webhook via cette URL et définit le stage source du pipeline sur In Progress. Lorsque le pipeline est dans cet état, un assistant interroge CodePipeline la tâche personnalisée, exécute la tâche et envoie un statut de réussite ou d'échec à CodePipeline. Dans ce cas, étant donné que le pipeline est au stade source, le job worker récupère le contenu du référentiel Git, le compresse et le télécharge dans le bucket Amazon Simple Storage Service (Amazon S3) où sont stockés les artefacts du pipeline, à l'aide de la clé d'objet fournie par le job interrogé. Vous pouvez également associer une transition pour l'action personnalisée à un événement sur Amazon CloudWatch et lancer le job worker en fonction de cet événement. Cette configuration vous permet d'utiliser des référentiels Git tiers que le service ne prend pas en charge de manière native en tant que sources. CodePipeline

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un référentiel Git qui prend en charge les webhooks et peut se connecter à l'URL d'un CodePipeline webhook via Internet

- Interface de ligne de commande AWS (AWS CLI) (AWS CLI) installée et configurée pour fonctionner avec le compte AWS

Architecture

Le modèle comprend les étapes suivantes :

1. L'utilisateur valide le code dans un dépôt Git.
2. Le webhook Git est appelé.
3. Le CodePipeline webhook s'appelle.
4. Le pipeline est défini sur En cours et le stage source sur l'état En cours.
5. L'action de l'étape source initie une règle CloudWatch Events, indiquant qu'elle a été démarrée.
6. L' CloudWatch événement initie une fonction Lambda.
7. La fonction Lambda obtient les détails de la tâche d'action personnalisée.
8. La fonction Lambda lance CodeBuild AWS et lui transmet toutes les informations relatives au travail.
9. CodeBuild obtient la clé SSH publique ou les informations d'identification utilisateur pour l'accès HTTPS à Git à partir de Secrets Manager.
10. CodeBuild clone le dépôt Git pour une branche spécifique.
11. CodeBuild compresse l'archive et la télécharge dans le compartiment S3 qui sert de magasin d' CodePipeline artefacts.

Outils

- AWS CodePipeline — AWS CodePipeline est un service de livraison continue entièrement géré qui vous aide à automatiser vos pipelines de publication pour des mises à jour rapides et fiables des applications et de l'infrastructure. CodePipeline automatise les phases de création, de test et de déploiement de votre processus de publication pour chaque modification de code, en fonction du modèle de version que vous définissez. Cela vous permet de fournir des fonctionnalités et des mises à jour de manière rapide et fiable. Vous pouvez intégrer AWS CodePipeline à des services tiers tels que GitHub ou avec votre propre plugin personnalisé.

- AWS Lambda — AWS Lambda vous permet d'exécuter du code sans provisionner ni gérer de serveurs. Avec Lambda, vous pouvez exécuter du code pour pratiquement n'importe quel type d'application ou de service principal sans qu'aucune administration ne soit nécessaire. Vous téléchargez votre code et Lambda s'occupe de tout ce qui est nécessaire pour exécuter et dimensionner votre code avec une haute disponibilité. Vous pouvez configurer votre code pour qu'il soit lancé automatiquement à partir d'autres services AWS ou l'appeler directement depuis n'importe quelle application Web ou mobile.
- AWS CodeBuild — AWS CodeBuild est un service d'intégration continue entièrement géré qui compile le code source, exécute des tests et produit des packages logiciels prêts à être déployés. Grâce à CodeBuild cela, vous n'avez pas besoin de provisionner, de gérer et de dimensionner vos propres serveurs de construction. CodeBuild évolue en continu et traite plusieurs versions simultanément, afin que vos versions ne soient pas laissées en attente dans une file d'attente. Vous pouvez démarrer rapidement en utilisant des environnements de génération prépackagés, ou bien, vous pouvez créer vos propres environnements de génération personnalisés, que vous utiliserez avec vos outils de génération.
- AWS Secrets Manager — AWS Secrets Manager vous aide à protéger les secrets nécessaires pour accéder à vos applications, services et ressources informatiques. Le service vous permet de faire pivoter, de gérer et de récupérer les informations d'identification de base de données, les clés d'API et d'autres secrets tout au long de leur cycle de vie. Les utilisateurs et les applications récupèrent les secrets en appelant Secrets Manager APIs, sans avoir à coder en dur les informations sensibles en texte brut. Secrets Manager propose une rotation secrète avec intégration intégrée à Amazon Relational Database Service (Amazon RDS), Amazon Redshift et Amazon DocumentDB. Le service peut être étendu pour prendre en charge d'autres types de secrets, notamment les clés API et les OAuth jetons. En outre, Secrets Manager vous permet de contrôler l'accès aux secrets à l'aide d'autorisations précises et d'auditer la rotation des secrets de manière centralisée pour les ressources du cloud AWS, des services tiers et des environnements sur site.
- Amazon CloudWatch — Amazon CloudWatch est un service de surveillance et d'observation conçu pour les DevOps ingénieurs, les développeurs, les ingénieurs de fiabilité des sites (SREs) et les responsables informatiques. CloudWatch vous fournit des données et des informations exploitables pour surveiller vos applications, répondre aux changements de performances à l'échelle du système, optimiser l'utilisation des ressources et obtenir une vue unifiée de l'état de fonctionnement. CloudWatch collecte des données opérationnelles et de surveillance sous forme de journaux, de mesures et d'événements, afin de vous fournir une vue unifiée des ressources, des applications et des services AWS exécutés sur AWS et sur des serveurs sur site. Vous pouvez l'utiliser CloudWatch pour détecter les comportements anormaux dans vos environnements,

définir des alarmes, visualiser les journaux et les indicateurs côte à côte, prendre des mesures automatisées, résoudre les problèmes et découvrir des informations permettant de garantir le bon fonctionnement de vos applications.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui vous permet de stocker et de protéger n'importe quel volume de données pour de nombreux cas d'utilisation, tels que les sites Web, les applications mobiles, la sauvegarde et la restauration, l'archivage, les applications d'entreprise, les appareils IoT et l'analyse des mégadonnées. Amazon S3 fournit easy-to-use des fonctionnalités de gestion qui vous aident à organiser vos données et à configurer des contrôles d'accès précis pour répondre à vos exigences commerciales, organisationnelles et de conformité spécifiques.

Épopées

Créez une action personnalisée dans CodePipeline

Tâche	Description	Compétences requises
Créez une action personnalisée à l'aide de l'AWS CLI ou d'AWS CloudFormation.	Cette étape implique la création d'une action source personnalisée qui peut être utilisée dans l'étape source d'un pipeline dans votre compte AWS dans une région donnée. Vous devez utiliser l'interface de ligne de commande AWS ou AWS CloudFormation (et non la console) pour créer l'action source personnalisée. Pour plus d'informations sur les commandes et les étapes décrites dans cette épopée et dans d'autres, consultez la section « Ressources connexes » à la fin de ce modèle. Dans l'AWS CLI,	AWS général

Tâche	Description	Compétences requises
	utilisez la create-custom-acti on-type commande. Utilisez -- configuration-properties pour fournir tous les paramètres que le travailleur doit traiter lorsqu'il interroge CodePipel ine une tâche. Assurez-vous de noter les valeurs fournies aux options --provider et -- action-version, afin de pouvoir utiliser les mêmes valeurs lors de la création du pipeline avec cette étape source personnal isée. Vous pouvez également créer l'action source personnal isée dans AWS en CloudForm ation utilisant le type de ressource AWS::Code Pipeline::CustomActionType.	

Configurer l'authentification

Tâche	Description	Compétences requises
Créez une paire de clés SSH.	Créez une paire de clés Secure Shell (SSH). Pour obtenir des instructi ons, consultez la GitHub documentation.	Ingénieur systèmes/systèmes DevOps
Créez un secret dans AWS Secrets Manager.	Copiez le contenu de la clé privée depuis la paire de clés SSH et créez un secret dans AWS Secrets Manager. Ce secret est utilisé pour l'authent	AWS général

Tâche	Description	Compétences requises
	ification lors de l'accès au dépôt Git.	
Ajoutez la clé publique au dépôt Git.	Ajoutez la clé publique de la paire de clés SSH aux paramètres du compte du référentiel Git, pour l'authent ification par le biais de la clé privée.	Ingénieur systèmes/systèmes DevOps

Création d'un pipeline et d'un webhook

Tâche	Description	Compétences requises
Créez un pipeline qui inclut l'action source personnalisée.	Créez un pipeline dans CodePipeline. Lorsque vous configurez le stage source, choisissez l'action source personnalisée que vous avez créée précédemment. Vous pouvez le faire dans la CodePipeline console AWS ou dans l'interface de ligne de commande AWS. CodePipel ine vous invite à saisir les propriétés de configuration que vous avez définies pour l'action personnalisée. Ces informations sont requises pour que le travailleur puisse traiter le travail pour l'action personnalisée. Suivez l'assista nt et créez l'étape suivante pour le pipeline.	AWS général

Tâche	Description	Compétences requises
Créez un CodePipeline webhook.	Créez un webhook pour le pipeline que vous avez créé à l'aide de l'action source personnalisée. Vous devez utiliser l'AWS CLI ou AWS CloudFormation (et non la console) pour créer le webhook. Dans l'AWS CLI, exécutez la commande put-webhook et fournissez les valeurs appropriées pour les options du webhook. Notez l'URL du webhook renvoyée par la commande. Si vous utilisez AWS CloudFormation pour créer le webhook, utilisez le type AWS::CodePipeline: :Webhook de ressource. Assurez-vous de sortir l'URL du webhook à partir de la ressource créée et notez-la.	AWS général

Tâche	Description	Compétences requises
Créez une fonction et CodeBuild un projet Lambda.	Au cours de cette étape, vous utilisez Lambda CodeBuild pour créer un job worker qui interrogera les demandes de travail CodePipeline pour l'action personnal isée, exécutera le travail et renverra le résultat du statut à. CodePipeline Créez une fonction Lambda initiée par une règle Amazon CloudWatch Events lorsque l'étape d'action sur la source personnalisée du pipeline passe à « En cours ». Lorsque la fonction Lambda est lancée, elle doit obtenir les détails des tâches d'action personnalisées en interroge ant les tâches. Vous pouvez utiliser l' PollForJobs API pour renvoyer ces informati ons. Une fois les informati ons de travail interrogées obtenues, la fonction Lambda doit renvoyer un accusé de réception, puis traiter les informations avec les données qu'elle obtient à partir des propriétés de configuration pour l'action personnalisée. Lorsque le travailleur est prêt à communiquer avec le dépôt Git, vous pouvez lancer un	AWS général, développeur de code

Tâche	Description	Compétences requises
	CodeBuild projet, car il est pratique de gérer les tâches Git à l'aide du client SSH.	

Créez un événement dans CloudWatch

Tâche	Description	Compétences requises
Créez une règle d' CloudWatch événements.	Créez une règle d' CloudWatch événements qui lance la fonction Lambda en tant que cible chaque fois que l'étape d'action personnalisée du pipeline passe à « En cours ».	AWS général

Ressources connexes

Création d'une action personnalisée dans CodePipeline

- Créez et ajoutez une action personnalisée dans CodePipeline
- AWS::CodePipeline::CustomActionType ressource

Configuration de l'authentification

- Création et gestion de secrets avec AWS Secrets Manager

Création d'un pipeline et d'un webhook

- Créez un pipeline dans CodePipeline
- référence de commande put-webhook
- AWS::CodePipeline::Webhook ressource
- PollForJobs Référence d'API
- Créez et ajoutez une action personnalisée dans CodePipeline

- Création d'un projet de génération dans AWS CodeBuild

Création d'un événement

- Détectez et réagissez aux changements d'état du pipeline avec Amazon CloudWatch Events

Références supplémentaires

- Travailler avec des pipelines dans CodePipeline
- Guide du développeur AWS Lambda

Créez un pipeline CI/CD pour valider les configurations Terraform à l'aide d'AWS CodePipeline

Créée par Aromal Raj Jayarajan (AWS) et Vijesh Vijayakumaran Nair (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle montre comment tester les configurations HashiCorp Terraform à l'aide d'un pipeline d'intégration continue et de livraison continue (CI/CD) déployé par AWS. CodePipeline

Terraform est une application d'interface en ligne de commande qui vous aide à utiliser du code pour provisionner et gérer l'infrastructure et les ressources du cloud. La solution fournie dans ce modèle crée un pipeline CI/CD qui vous aide à valider l'intégrité de vos configurations Terraform en exécutant cinq étapes : CodePipeline

1. `“checkout”`extrait la configuration Terraform que vous testez à partir d'un référentiel AWS CodeCommit .
2. `“validate”`exécute des outils de validation de l'infrastructure en tant que code (IaC) TFLint, notamment tfsec et checkov. Le stage exécute également les commandes de validation Terraform IaC suivantes : `terraform validate` et. `terraform fmt`
3. `“plan”`indique quelles modifications seront appliquées à l'infrastructure si la configuration Terraform est appliquée.
4. `“apply”`utilise le plan généré pour fournir l'infrastructure requise dans un environnement de test.
5. `“destroy”`supprime l'infrastructure de test créée au cours de l'`“apply”`étape.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI), installée et configurée
- Git, installé et configuré sur votre machine locale
- Terraform, installé et configuré sur votre machine locale

Limites

- L'approche de ce modèle déploie AWS CodePipeline sur un seul compte AWS et dans une seule région AWS. Des modifications de configuration sont nécessaires pour les déploiements multicomptes et multirégions.
- Le rôle AWS Identity and Access Management (IAM) fourni par ce modèle (codepipeline_iam_role) suit le principe du moindre privilège. Les autorisations de ce rôle IAM doivent être mises à jour en fonction des ressources spécifiques que votre pipeline doit créer.

Versions du produit

- AWS CLI version 2.9.15 ou ultérieure
- Terraform version 1.3.7 ou ultérieure

Architecture

Pile technologique cible

- AWS CodePipeline
- AWS CodeBuild
- AWS CodeCommit
- AWS IAM
- Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS)
- Terraform

Architecture cible

Le schéma suivant montre un exemple de flux de pipeline CI/CD pour tester les configurations Terraform dans. CodePipeline

Le schéma suivant illustre le flux de travail suivant :

1. Dans CodePipeline, un utilisateur AWS lance les actions proposées dans un plan Terraform en exécutant la `terraform apply` commande dans l'AWS CLI.

2. AWS CodePipeline assume un rôle de service IAM qui inclut les politiques requises pour accéder CodeCommit à AWS KMS et à Amazon S3. CodeBuild
3. CodePipeline exécute l'étape du `“checkout”` pipeline pour extraire la configuration Terraform d'un CodeCommit référentiel AWS à des fins de test.
4. CodePipeline exécute l'`“validate”`étape pour tester la configuration de Terraform en exécutant les outils de validation IaC et en exécutant les commandes de validation Terraform iAc dans un projet. CodeBuild
5. CodePipeline exécute l'`“plan”`étape pour créer un plan dans le CodeBuild projet basé sur la configuration Terraform. L'utilisateur AWS peut consulter ce plan avant que les modifications ne soient appliquées à l'environnement de test.
6. Code Pipeline exécute l'`“apply”`étape de mise en œuvre du plan en utilisant le CodeBuild projet pour fournir l'infrastructure requise dans l'environnement de test.
7. CodePipeline exécute la `“destroy”` phase, qui permet CodeBuild de supprimer l'infrastructure de test créée pendant la `“apply”` phase.
8. Un compartiment Amazon S3 stocke les artefacts du pipeline, qui sont chiffrés et déchiffrés à l'aide d'une clé gérée par le client AWS KMS.

Outils

Outils

Services AWS

- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres services

- HashiCorp Terraform est une application d'interface en ligne de commande qui vous aide à utiliser du code pour provisionner et gérer l'infrastructure et les ressources du cloud.

Code

Le code de ce modèle est disponible dans le GitHub aws-codepipeline-terraform-cicdsamplesréférentiel. Le référentiel contient les configurations Terraform requises pour créer l'architecture cible décrite dans ce modèle.

Épopées

Fournir les composants de la solution

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Clonez le GitHub aws-codepipeline-terraform-cicdsamplesdépôt en exécutant la commande suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/aws-codepipeline-terraform-cicd-samples.git` Pour plus d'informations, consultez la section Clonage d'un dépôt dans la GitHub documentation.	DevOps ingénieur
Créez un fichier de définitions de variables Terraform.	Créez un `terraform.tfvars` fichier en fonction	DevOps ingénieur

Tâche	Description	Compétences requises
	des exigences de votre cas d'utilisation. Vous pouvez mettre à jour les variables dans le `examples/terraform.tfvars` fichier qui se trouve dans le dépôt cloné. Pour plus d'informations, consultez Affecter des valeurs aux variables du module racine dans la documentation Terraform. **Note** Le `Readme.md` fichier du référentiel contient plus d'informations sur les variables requises.	
Configurez AWS en tant que fournisseur Terraform.	1. Dans un éditeur de code, ouvrez le `main.tf` fichier du dépôt cloné. 2. Ajoutez les configurations nécessaires pour établir la connectivité au compte AWS cible. Pour plus d'informations, consultez le fournisseur AWS dans la documentation Terraform.	DevOps ingénieur

Tâche	Description	Compétences requises
Mettez à jour la configuration du fournisseur Terraform pour créer le compartiment de réplication Amazon S3.	1. Ouvrez le `S3` répertoire du dépôt en exécutant la commande suivante : `cd ./modules/s3` 2. Mettez à jour la configuration du fournisseur Terraform pour créer le compartiment de réplication Amazon S3 en mettant à jour la `region` valeur dans le `tf` fichier. Assurez-vous de saisir la région dans laquelle vous souhaitez qu'Amazon S3 réplique les objets. 3. (Facultatif) Par défaut, Terraform utilise des fichiers d'état locaux pour la gestion des états. Si vous souhaitez ajouter Amazon S3 en tant que backend distant, vous devez mettre à jour la configuration de Terraform. Pour plus d'informations, consultez la section Configuration du backend dans la documentation Terraform.	DevOps ingénieur

Tâche	Description	Compétences requises
	Note La réplication active la copie automatique et asynchrone des objets dans les compartim ents Amazon S3.	
Initialisez la configuration Terraform.	Pour initialiser votre répertoir e de travail qui contient les fichiers de configura tion Terraform, exécutez la commande suivante dans le dossier racine du référentiel cloné : `terraform init`	DevOps ingénieur

Tâche	Description	Compétences requises
Créez le plan Terraform.	Pour créer un plan Terraform , exécutez la commande suivante dans le dossier racine du référentiel cloné : `terraform plan --var-file=terraform.tfvars -out=tfplan` **Note** Terraform évalue les fichiers de configuration pour déterminer l'état cible des ressources déclarées . Il compare ensuite l'état cible à l'état actuel et crée un plan.	DevOps ingénieur
Vérifiez le plan Terraform.	Passez en revue le plan Terraform et confirmez qu'il configure l'architecture requise dans votre compte AWS cible.	DevOps ingénieur

Tâche	Description	Compétences requises
Déployez la solution.	1. Pour appliquer le plan Terraform, exécutez la commande suivante dans le dossier racine du référentiel cloné : `terraform apply "tfplan"` 2. Entrez Oui pour confirmer que vous souhaitez déployer les ressources. **Note** Terraform crée, met à jour ou détruit l'infrast ructure pour atteindre l'état cible déclaré dans les fichiers de configuration.	DevOps ingénieur

Validez les configurations Terraform en exécutant le pipeline

Tâche	Description	Compétences requises
Configurez le référentiel de code source.	1. À partir de la sortie Terraform, obtenez les détails du référentiel source pour le référentiel contenant les configurations Terraform que vous souhaitez valider.	DevOps ingénieur

Tâche	Description	Compétences requises
	2. Connectez-vous à l'AWS Management Console. Ouvrez ensuite la CodeCommit console. 3. Créez une nouvelle branche dans le référentiel source nommé`main`. Pour obtenir des instructions, consultez la section Créer une branche dans AWS CodeCommit dans la CodeCommit documentation. 4. Clonez la `main` branche du référentiel source sur votre poste de travail local. Pour obtenir des instructions, consultez les étapes de configuration des connexions HTTPS aux CodeCommit référentiels AWS sous Windows avec l'assistant d'identification de l'interface de ligne de commande AWS dans la documentation. CodeCommit 5. Copiez le **`templates`** dossier depuis le GitHub aws-codepipeline-terraform-cicdsamplesréférentiel en exécutant la commande suivante :	

Tâche	Description	Compétences requises
	`cp -r templates $YOUR_CODECOMMIT_REPO_ROOT` **Note** Le `templates` dossier contient les fichiers de spécification de construction et le script de validation pour le répertoire racine du référentiel source. 6. Ajoutez les configurations Terraform iAc requises dans le dossier racine du référentiel source. 7. Ajoutez les détails du backend distant dans la configuration Terraform de votre projet. Pour plus d'informations, consultez S3 dans la documentation Terraform. 8. (Facultatif) Mettez à jour les variables du `templates` dossier pour activer ou désactiver les scans préconfigurés, les versions de changement d'outil et pour spécifier votre répertoire dans des fichiers de script	

Tâche	Description	Compétences requises
	personnalisés. Pour plus d'informations, consultez la section Informations supplémentaires de ce modèle. 9. Transférez les modificat ions à la `main` branche du référentiel source.	

Tâche	Description	Compétences requises
Validez les étapes du pipeline.	1. Connectez-vous à AWS Management Console et ouvrez la console CodePipeline . 2. Dans le résultat généré à partir de la `terraform apply "tfplan"` commande de la section Epic précédente, trouvez le nom de la commande générée CodePipeline. 3. Ouvrez le pipeline dans la CodePipeline console et choisissez Release change. 4. Passez en revue chaque étape du pipeline et confirmez qu'elle fonctionne comme prévu. Pour plus d'informations, consultez Afficher les détails et l'historique du pipeline (console) dans le guide de CodePipeline l'utilisateur AWS. ⚠ Important Lorsqu'une modification est validée dans la branche principale du référentiel source, le pipeline de test	DevOps ingénieur

Tâche	Description	Compétences requises
	est automatiquement activé.	
Vérifiez le résultat du rapport.	1. Sur la CodePipeline console, dans le volet de navigation de gauche, choisissez Build. Choisissez ensuite l'historique des rapports. 2. Passez en revue les rapports d'analyse tfsec et checkov générés par le pipeline. Ces rapports peuvent vous aider à identifier les problèmes par le biais de visualisations et de représentations graphiques. **Note** Le `<project_name>-validate` CodeBuild projet génère des rapports de vulnérabilité pour votre code au cours de l'`“validate”` étape.	DevOps ingénieur

Nettoyage de vos ressources

Tâche	Description	Compétences requises
Nettoyez le pipeline et les ressources associées.	Pour supprimer les ressources de test de votre compte AWS, exécutez la commande suivante dans le dossier racine du référentiel cloné : `terraform destroy --var-file=terraform.tfvars`	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Vous recevez un AccessDenied message d'erreur au cours de l'“`apply`”étape.	1. Consultez les journaux d'exécution du CodeBuild projet associés à l'“`apply`”étape pour identifier les autorisations IAM manquantes. Pour plus d'informations, consultez la section Afficher les détails de la version dans AWS CodeBuild dans le guide de CodeBuild l'utilisateur AWS. 2. Dans un éditeur de code, ouvrez le `modules` dossier du dépôt cloné. Accédez ensuite au `iam-role` dossier et ouvrez le `main.tf` fichier qui s'y trouve. 3. Dans le `codepipeline_policy` relevé, ajoutez les politiques IAM requises pour le provisionnement des ressources de votre compte AWS.

Ressources connexes

- Blocs de modules (documentation Terraform)
- Comment utiliser le CI/CD pour déployer et configurer les services de sécurité AWS avec Terraform (article de blog AWS)
- Utilisation de rôles liés à un service (documentation IAM)
- create-pipeline (documentation de la CLI AWS)
- Configurer le chiffrement côté serveur pour les artefacts stockés dans Amazon S3 pour (documentation CodePipeline AWS CodePipeline)
- Quotas pour AWS CodeBuild (CodeBuild documentation AWS)
- Protection des données dans AWS CodePipeline (CodePipeline documentation AWS)

Informations supplémentaires

Modules Terraform personnalisés

Voici une liste des modules Terraform personnalisés utilisés dans ce modèle :

- `codebuild_terraform`crée les CodeBuild projets qui constituent chaque étape du pipeline.
- `codecommit_infrastructure_source_repo`capture et crée le CodeCommit référentiel source.
- `codepipeline_iam_role`crée les rôles IAM requis pour le pipeline.
- `codepipeline_kms`crée la clé AWS KMS requise pour le chiffrement et le déchiffrement des objets Amazon S3.
- `codepipeline_terraform`crée le pipeline de test pour le CodeCommit référentiel source.
- `s3_artifacts_bucket`crée un compartiment Amazon S3 pour gérer les artefacts du pipeline.

Fichiers de spécifications de construction

Voici une liste des fichiers de spécification de construction (buildspec) que ce modèle utilise pour exécuter chaque étape du pipeline :

- `buildspec_validate.yml`dirige la “`validate`” scène.
- `buildspec_plan.yml`dirige la “`plan`” scène.
- `buildspec_apply.yml`dirige la “`apply`” scène.

- `buildspec_destroy.yml`dirige la “`destroy`” scène.

Variables du fichier de spécifications de construction

Chaque fichier buildspec utilise les variables suivantes pour activer différents paramètres spécifiques à la version :

Variable	Valeur par défaut	Description
`CODE_SRC_DIR`	"."	Définit le CodeCommit répertoire source
`TF_VERSION`	« 1,3,7 »	Définit la version Terraform pour l'environnement de construction

Le `buildspec_validate.yml` fichier prend également en charge les variables suivantes pour activer différents paramètres spécifiques à la version :

Variable	Valeur par défaut	Description
`SCRIPT_DIR`	«. /modèles/scripts »	Définit le répertoire des scripts
`ENVIRONMENT`	« développeur »	Définit le nom de l'environ nement
`SKIPVALIDATIONFAIL URE`	« Y »	Ignore la validation en cas d'échec
`ENABLE_TFVALIDATE`	« Y »	Active la validation Terraform
`ENABLE_TFFORMAT`	« Y »	Active le format Terraform
`ENABLE_TFCHECKOV`	« Y »	Active le scan de vérification
`ENABLE_TFSEC`	« Y »	Active le scan TFSEC
`TFSEC_VERSION`	« v1.28.1 »	Définit la version tfsec

Plus de modèles

- Accédez à des applications de conteneur en privé sur Amazon EKS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Associer un AWS CodeCommit référentiel dans un compte Compte AWS à Amazon SageMaker AI Studio Classic dans un autre compte
- Automatisez la création de comptes à l'aide de l'accélérateur Landing Zone sur AWS
- Automatisez l'ajout ou la mise à jour d'entrées de registre Windows à l'aide d'AWS Systems Manager
- Automatisez les sauvegardes pour les instances de base de données Amazon RDS for PostgreSQL à l'aide d'AWS Batch
- Automatisez le déploiement d'applications imbriquées à l'aide d'AWS SAM
- Automatisez le déploiement du gestionnaire de terminaison de nœuds dans Amazon EKS à l'aide d'un pipeline CI/CD
- Automatisez la configuration de RabbitMQ dans Amazon MQ
- Automatisez la réplication des instances Amazon RDS sur Comptes AWS
- Automatically build and deploy a Java application to Amazon EKS using a CI/CD pipeline
- Générez automatiquement un modèle PynamoDB et des fonctions CRUD pour Amazon DynamoDB à l'aide d'une application Python
- Validez et déployez automatiquement les politiques et les rôles IAM dans un compte AWS à l'aide d' CodePipelineIAM Access Analyzer et de macros AWS CloudFormation
- Sauvegardez les serveurs Sun SPARC dans l'émulateur Stromasys Charon-SSP sur le cloud AWS
- Créez un pipeline de données pour ingérer, transformer et analyser les données Google Analytics à l'aide du kit de AWS DataOps développement
- Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager
- Créez un pipeline pour les images de conteneurs renforcées à l'aide d' EC2 Image Builder et de Terraform
- Créez un MLOps flux de travail à l'aide d'Amazon SageMaker AI et d'Azure DevOps
- Centralisation de la résolution DNS à l'aide AWS Managed Microsoft AD et sur site de Microsoft Active Directory
- Enchaînez les services AWS en utilisant une approche sans serveur

- Nettoyez les ressources de AWS Account Factory for Terraform (AFT) en toute sécurité après la perte du fichier d'état
- Configurez la journalisation pour les applications .NET dans Amazon CloudWatch Logs en utilisant NLog
- Déployez en continu une application Web AWS Amplify moderne à partir d'un référentiel AWS CodeCommit
- Créez une image de conteneur Docker personnalisée SageMaker et utilisez-la pour la formation des modèles dans AWS Step Functions
- Créez un pipeline dans les régions AWS qui ne prennent pas en charge AWS CodePipeline
- Créez des alarmes pour des métriques personnalisées à l'aide de la détection des CloudWatch anomalies Amazon
- Personnalisez les noms de rôles par défaut en utilisant des AWS CDK aspects et des trappes d'échappement
- Déployez un pipeline qui détecte simultanément les problèmes de sécurité dans plusieurs livrables de code
- Déployez et gérez un lac de données sans serveur sur le cloud AWS en utilisant l'infrastructure sous forme de code
- Déployez des ressources et des packages Kubernetes à l'aide d'Amazon EKS et d'un référentiel de diagrammes Helm dans Amazon S3
- Déployez des applications à piles multiples à l'aide d'AWS CDK avec TypeScript
- Déployez des instances de cluster de basculement SQL Server sur Amazon EC2 et Amazon à l'aide FSx de Terraform
- Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform
- Développez des assistants avancés basés sur l'IA générative basés sur le chat en utilisant RAG et des instructions ReAct
- Activez Amazon de GuardDuty manière conditionnelle à l'aide de modèles AWS CloudFormation
- Configurez le dimensionnement automatique piloté par les événements dans Amazon EKS à l'aide d'Amazon EKS Pod Identity et KEDA
- Générez des recommandations personnalisées et reclassées à l'aide d'Amazon Personalize
- Recevez des notifications Amazon SNS lorsque l'état clé d'une clé AWS KMS change
- Identifiez automatiquement les images de conteneur dupliquées lors de la migration vers un référentiel Amazon ECR

- Implémentez la gestion des versions d'API basée sur les chemins en utilisant des domaines personnalisés dans Amazon API Gateway
- Améliorez les performances opérationnelles en activant Amazon DevOps Guru dans plusieurs régions AWS, sur plusieurs comptes et OUs avec le kit AWS CDK
- Installation de l'agent SSM sur les nœuds de travail Amazon EKS à l'aide de Kubernetes DaemonSet
- Intégrez le contrôleur universel Stonebranch à la modernisation du mainframe AWS
- Modernisation du mainframe : DevOps activée AWS avec Rocket Software Enterprise Suite
- Gérez les ensembles AWS IAM Identity Center d'autorisations sous forme de code en utilisant AWS CodePipeline
- Gérez les applications de conteneur sur site en configurant Amazon ECS Anywhere avec le kit AWS CDK
- Gérez AWS Organizations les politiques sous forme de code en utilisant AWS CodePipeline Amazon Bedrock
- Migrer des enregistrements DNS en masse vers une zone hébergée privée Amazon Route 53
- Migrez les charges de travail de création, de formation et de déploiement de ML vers Amazon à SageMaker l'aide des outils de développement AWS
- Surveillez l'utilisation d'une Amazon Machine Image partagée sur plusieurs Comptes AWS
- Optimisation des images Docker générées par AWS App2Container
- Orchestrez un pipeline ETL avec validation, transformation et partitionnement à l'aide d'AWS Step Functions
- Automatisez les déploiements bleu/vert des bases de données mondiales Amazon Aurora en utilisant les principes de l'IaC
- Préservez l'espace IP routable dans les conceptions VPC multi-comptes pour les sous-réseaux autres que les charges de travail
- Provisionner un produit Terraform à l'aide AWS Service Catalog d'un référentiel de code
- Répliquez les images filtrées des conteneurs Amazon ECR sur plusieurs comptes ou régions
- Rotation des informations d'identification de base de données sans redémarrer les conteneurs
- Exécutez les tâches d'automatisation d'AWS Systems Manager de manière synchrone depuis AWS Step Functions
- Configurez un pipeline CI/CD pour les charges de travail hybrides sur Amazon ECS Anywhere à l'aide d'AWS CDK et GitLab

- Configurer un pipeline CI/CD pour la migration de base de données à l'aide de Terraform
- Configurez une infrastructure multi-AZ pour un SQL Server Always On FCI à l'aide d'Amazon FSx
- Configurez automatiquement des robots UiPath RPA sur Amazon à l'aide EC2 d'AWS CloudFormation
- Simplifiez l'authentification des applications avec le protocole TLS mutuel dans Amazon ECS en utilisant Application Load Balancer
- Intégration des locataires dans l'architecture SaaS pour le modèle de silo à l'aide de C# et d'AWS CDK
- Utilisez Terraform pour activer automatiquement Amazon GuardDuty pour une organisation
- Utilisez les agents Amazon Bedrock pour automatiser la création de contrôles d'accès dans Amazon EKS via des instructions textuelles
- Validez le code Account Factory pour Terraform (AFT) localement
- Visualisez les résultats du modèle AI/ML à l'aide de Flask et AWS Elastic Beanstalk

Infrastructure

Rubriques

- Accédez à un hôte bastion à l'aide du gestionnaire de session et d'Amazon EC2 Instance Connect
- Centralisation de la résolution DNS à l'aide AWS Managed Microsoft AD et sur site de Microsoft Active Directory
- Centralisez la surveillance à l'aide d'Amazon CloudWatch Observability Access Manager
- Vérifiez la présence de balises obligatoires dans les EC2 instances au lancement
- Nettoyez les ressources de AWS Account Factory for Terraform (AFT) en toute sécurité après la perte du fichier d'état
- Connectez-vous à une EC2 instance Amazon à l'aide du gestionnaire de session
- Créez un pipeline dans les régions AWS qui ne prennent pas en charge AWS CodePipeline
- Personnalisez les noms de rôles par défaut en utilisant des AWS CDK aspects et des trappes d'échappement
- Déployez un cluster Cassandra sur Amazon EC2 avec une statique privée IPs pour éviter le rééquilibrage
- Étendez votre accès VRFs à AWS en utilisant AWS Transit Gateway Connect
- Recevez des notifications Amazon SNS lorsque l'état clé d'une clé AWS KMS change
- Préservez l'espace IP routable dans les conceptions VPC multi-comptes pour les sous-réseaux autres que les charges de travail
- Provisionner un produit Terraform à l'aide AWS Service Catalog d'un référentiel de code
- Enregistrez plusieurs comptes AWS avec une seule adresse e-mail à l'aide d'Amazon SES
- Configuration de la résolution DNS pour les réseaux hybrides dans un environnement AWS à compte unique
- Configurez automatiquement des robots UiPath RPA sur Amazon à l'aide EC2 d'AWS CloudFormation
- Configuration d'une PeopleSoft architecture à haute disponibilité sur AWS
- Configurer la reprise après sinistre pour Oracle JD Edwards EnterpriseOne avec AWS Elastic Disaster Recovery
- Configurer la détection des AWS CloudFormation dérives dans une organisation multirégionale et multi-comptes
- Importation réussie d'un compartiment S3 en tant que CloudFormation stack AWS

- Synchronisez les données entre les systèmes de fichiers Amazon EFS dans différentes régions AWS à l'aide d'AWS DataSync
- AWS Infrastructure de test à l'aide LocalStack de tests Terraform
- Mettez à niveau les clusters SAP Pacemaker de ENSA1 ENSA2
- Utilisez des zones de disponibilité cohérentes VPCs sur les différents comptes AWS
- Utiliser l'utilisateur IDs dans les politiques IAM pour le contrôle d'accès et l'automatisation
- Validez le code Account Factory pour Terraform (AFT) localement
- Plus de modèles

Accédez à un hôte bastion à l'aide du gestionnaire de session et d'Amazon EC2 Instance Connect

Créée par Piotr Chotkowski (AWS) et Witold Kowalik (AWS)

Récapitulatif

Un hôte bastion, parfois appelé boîte de saut, est un serveur qui fournit un point d'accès unique depuis un réseau externe aux ressources situées sur un réseau privé. Un serveur exposé à un réseau public externe, tel qu'Internet, présente un risque de sécurité potentiel en cas d'accès non autorisé. Il est important de sécuriser et de contrôler l'accès à ces serveurs.

Ce modèle décrit comment vous pouvez utiliser Session Manager et Amazon EC2 Instance Connect pour vous connecter en toute sécurité à un hôte bastion Amazon Elastic Compute Cloud (Amazon EC2) déployé dans votre Compte AWS. Le gestionnaire de session est une fonctionnalité de AWS Systems Manager. Les avantages de ce modèle incluent :

- L'hôte bastion déployé ne possède aucun port entrant ouvert exposé à l'Internet public. Cela réduit la surface d'attaque potentielle.
- Vous n'avez pas besoin de stocker et de gérer des clés Secure Shell (SSH) à long terme dans votre Compte AWS. Au lieu de cela, chaque utilisateur génère une nouvelle paire de clés SSH chaque fois qu'il se connecte à l'hôte Bastion. AWS Identity and Access Management Les politiques (IAM) associées aux informations d' AWS identification de l'utilisateur contrôlent l'accès à l'hôte Bastion.

Public visé

Ce modèle est destiné aux lecteurs ayant une connaissance de base d'Amazon EC2, d'Amazon Virtual Private Cloud (Amazon VPC) et de Hashicorp Terraform.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- AWS Command Line Interface (AWS CLI) version 2, installée et configurée
- Plug-in de gestion de session pour le AWS CLI, installé

- Terraform CLI, installée
- Stockage pour l'état Terraform, tel qu'un bucket Amazon Simple Storage Service (Amazon S3) et une table Amazon DynamoDB servant de backend distant pour stocker l'état Terraform. Pour plus d'informations sur l'utilisation de backends distants pour l'état Terraform, consultez Amazon S3 Backends (documentation Terraform). Pour un exemple de code qui configure la gestion de l'état à distance avec un backend Amazon S3, consultez remote-state-s3-backend (Terraform Registry). Notez les critères suivants :
  - Le compartiment Amazon S3 et la table DynamoDB doivent se trouver dans le même emplacement. Région AWS
  - Lors de la création de la table DynamoDB, la clé de partition doit `LockID` être (distinguez majuscules et minuscules) et le type de clé de partition doit l'être. `String` Tous les autres paramètres du tableau doivent être à leurs valeurs par défaut. Pour plus d'informations, reportez-vous aux sections À propos des clés primaires et Création d'une table dans la documentation DynamoDB.
- Un client SSH, installé

Limites

- Ce modèle est conçu comme une preuve de concept (PoC) ou comme base pour un développement ultérieur. Il ne doit pas être utilisé sous sa forme actuelle dans les environnements de production. Avant le déploiement, ajustez l'exemple de code dans le référentiel en fonction de vos besoins et de votre cas d'utilisation.
- Ce modèle suppose que l'hôte bastion cible utilise Amazon Linux 2 comme système d'exploitation. Bien qu'il soit possible d'utiliser d'autres Amazon Machine Images (AMIs), ce modèle ne s'applique pas aux autres systèmes d'exploitation.

> **Note**
>
> Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.

- Dans ce modèle, l'hôte bastion est situé dans un sous-réseau privé sans passerelle NAT ni passerelle Internet. Cette conception isole l' EC2 instance Amazon de l'Internet public. Vous pouvez ajouter une configuration réseau spécifique qui lui permet de communiquer avec Internet. Pour plus d'informations, consultez Connecter votre cloud privé virtuel (VPC) à d'autres réseaux dans la documentation Amazon VPC. De même, conformément au principe du moindre privilège,

l'hôte du bastion n'a accès à aucune autre ressource de votre site, Compte AWS sauf si vous lui accordez explicitement des autorisations. Pour plus d'informations, consultez la section Politiques basées sur les ressources dans la documentation IAM.

Versions du produit

- Version 2 de l'interface de ligne de commande AWS
- Terraform version 1.3.9

Architecture

Pile technologique cible

- Un VPC avec un seul sous-réseau privé
- Les points de terminaison VPC d'interface suivants :
  - `amazonaws.<region>.ssm`— Le point de terminaison du AWS Systems Manager service.
  - `amazonaws.<region>.ec2messages`— Systems Manager utilise ce point de terminaison pour passer des appels depuis l'agent SSM vers le service Systems Manager.
  - `amazonaws.<region>.ssmmessages`— Le gestionnaire de session utilise ce point de terminaison pour se connecter à votre EC2 instance Amazon via un canal de données sécurisé.
- Une EC2 instance `t3.nano` Amazon exécutant Amazon Linux 2
- Rôle IAM et profil d'instance
- Groupes de sécurité Amazon VPC et règles de groupe de sécurité pour les points de terminaison et l'instance Amazon EC2

Architecture cible

Le schéma montre le processus suivant :

1. L'utilisateur assume un rôle IAM autorisé à effectuer les opérations suivantes :
   - Authentifier, autoriser et se connecter à l'instance Amazon EC2
   - Démarrer une session avec le gestionnaire de session
2. L'utilisateur lance une session SSH via le gestionnaire de session.

3. Le gestionnaire de session authentifie l'utilisateur, vérifie les autorisations dans les politiques IAM associées, vérifie les paramètres de configuration et envoie un message à l'agent SSM pour ouvrir une connexion bidirectionnelle.
4. L'utilisateur transmet la clé publique SSH à l'hôte Bastion via les métadonnées Amazon. EC2 Cela doit être fait avant chaque connexion. La clé publique SSH reste disponible pendant 60 secondes.
5. L'hôte Bastion communique avec les points de terminaison VPC de l'interface pour Systems Manager et Amazon. EC2
6. L'utilisateur accède à l'hôte Bastion via le gestionnaire de session en utilisant un canal de communication bidirectionnel crypté TLS 1.2.

Automatisation et mise à l'échelle

Les options suivantes sont disponibles pour automatiser le déploiement ou faire évoluer cette architecture :

- Vous pouvez déployer l'architecture par le biais d'un pipeline d'intégration et de livraison continues (CI/CD).
- Vous pouvez modifier le code pour changer le type d'instance de l'hôte Bastion.
- Vous pouvez modifier le code pour déployer plusieurs hôtes bastions. Dans le `bastion-host/main.tf` fichier, dans le bloc de `aws_instance` ressources, ajoutez le `count` méta-argument. Pour plus d'informations, consultez la documentation Terraform.

Outils

Services AWS

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection

et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle. Ce modèle utilise le Gestionnaire de session, une fonctionnalité de Systems Manager.

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud. Ce modèle utilise la CLI Terraform.

Référentiel de code

Le code de ce modèle est disponible dans l'hôte GitHub Access a bastion à l'aide du gestionnaire de session et du référentiel Amazon EC2 Instance Connect.

Bonnes pratiques

- Nous vous recommandons d'utiliser des outils d'analyse de code automatisés pour améliorer la sécurité et la qualité du code. Ce modèle a été scanné à l'aide de Checkov, un outil d'analyse de code statique pour IaC. Nous vous recommandons au minimum d'effectuer des contrôles de validation et de formatage de base à l'aide des commandes `terraform validate` et `terraform fmt -check -recursive` Terraform.
- Il est recommandé d'ajouter des tests automatisés pour IaC. Pour plus d'informations sur les différentes approches pour tester le code Terraform, consultez Testing HashiCorp Terraform (article de blog Terraform).
- Lors du déploiement, Terraform utilise l' EC2 instance Amazon qui remplace chaque fois qu'une nouvelle version de l'AMI Amazon Linux 2 est détectée. Cela déploie la nouvelle version du système d'exploitation, y compris les correctifs et les mises à niveau. Si le calendrier de déploiement est peu fréquent, cela peut présenter un risque de sécurité car l'instance ne dispose pas des derniers correctifs. Il est important de mettre à jour et d'appliquer fréquemment des correctifs de sécurité aux EC2 instances Amazon déployées. Pour plus d'informations, consultez la section Gestion des mises à jour sur Amazon EC2.

- Ce modèle étant une preuve de concept, il utilise des politiques AWS gérées, telles que`AmazonSSMManagedInstanceCore`. AWS les politiques gérées couvrent les cas d'utilisation courants mais n'accordent pas d'autorisations de moindre privilège. Selon les besoins de votre cas d'utilisation, nous vous recommandons de créer des politiques personnalisées qui accordent des autorisations de moindre privilège pour les ressources déployées dans cette architecture. Pour plus d'informations, voir Commencer avec les politiques AWS gérées et passer aux autorisations du moindre privilège.
- Utilisez un mot de passe pour protéger l'accès aux clés SSH et stockez les clés dans un emplacement sécurisé.
- Configurez la journalisation et la surveillance pour l'hôte du bastion. La journalisation et la surveillance sont des éléments importants de la maintenance des systèmes, tant du point de vue opérationnel que de la sécurité. Il existe plusieurs manières de surveiller les connexions et l'activité dans votre hôte Bastion. Pour plus d'informations, consultez les rubriques suivantes dans la documentation de Systems Manager :
  - Surveillance AWS Systems Manager
  - Connexion et surveillance AWS Systems Manager
  - Activité des sessions d'audit
  - Journalisation de l’activité de session

Épopées

Déployez les ressources

Tâche	Description	Compétences requises
Clonez le référentiel de code.	1. Dans une interface de ligne de commande, remplacez votre répertoire de travail par l'emplacement où vous souhaitez stocker les fichiers d'exemple. 2. Entrez la commande suivante. `git clone https://github.com/aws-samp`	DevOps ingénieur, développeur

Tâche	Description	Compétences requises
	`les/secured-bastion-host-terraform.git`	

Tâche	Description	Compétences requises
Initialisez le répertoire de travail Terraform.	Cette étape n'est nécessaire que pour le premier déploiement. Si vous redéployez le modèle, passez à l'étape suivante. Dans le répertoire racine du dépôt cloné, entrez la commande suivante, où : • `$S3_STATE_BUCKET` est le nom du compartiment Amazon S3 qui contient l'état Terraform • `$PATH_TO_STATE_FILE` est la clé du fichier d'état Terraform, tel que `infra/bastion-host/tetfstate` • `$AWS_REGION` est la région dans laquelle le compartiment Amazon S3 est déployé `terraform init \ -backend-config="bucket=$S3_STATE_BUCKET" \ -backend-config="key=$PATH_TO_STATE_FILE" \ -backend-config="region=$AWS_REGION`	DevOps ingénieur, Développeur, Terraform

Tâche	Description	Compétences requises
	Note Vous pouvez également ouvrir le fichier config.tf et, dans la `terraform` section, fournir ces valeurs manuellement.	
Déployez les ressources.	1. Dans le répertoire racine du dépôt cloné, entrez la commande suivante. `terraform apply -var-file="dev.tfvars"` 2. Consultez la liste de toutes les modifications qui seront appliquées à votre Compte AWS, puis confirmez le déploiement. 3. Attendez que toutes les ressources soient déployées.	DevOps ingénieur, Développeur, Terraform

Configuration de l'environnement local

Tâche	Description	Compétences requises
Configurez la connexion SSH.	Mettez à jour le fichier de configuration SSH pour autoriser les connexions SSH via le gestionnaire de session. Pour obtenir des instructi	DevOps ingénieur

Tâche	Description	Compétences requises
	ons, consultez Autoriser les connexions SSH pour le gestionnaire de session. Cela permet aux utilisate urs autorisés de saisir une commande proxy qui démarre une session du gestionna ire de session et transfère toutes les données via une connexion bidirectionnelle.	
Générez les clés SSH.	Entrez la commande suivante pour générer une paire de clés SSH privées et publiques locales. Vous utilisez cette paire de clés pour vous connecter à l'hôte Bastion. `ssh-keygen -t rsa -f my_key`	DevOps ingénieur, développe ur

Connectez-vous à l'hôte Bastion à l'aide du gestionnaire de session

Tâche	Description	Compétences requises
Obtenez l'ID de l'instance.	1. Pour vous connecter à l'hôte bastion déployé, vous avez besoin de l'ID de l' EC2 instance Amazon. Procédez de l'une des manières suivantes pour trouver l'ID : • Ouvrez la EC2 console Amazon. Dans le	AWS général

Tâche	Description	Compétences requises

	panneau de navigation, choisissez Instances. Localisez l'instance hôte Bastion.
	• Dans le AWS CLI, entrez la commande suivante.
	`aws ec2 describe-instances`
	Pour filtrer les résultats, entrez la commande suivante, où se `$BASTION_HOST_TAG` trouve le tag que vous avez attribué à l'hôte du bastion. La valeur par défaut de cette balise est`sandbox-dev-bastion-host` .
	`aws ec2 describe-instances \ --filters "Name=tag:Name,Values=$BASTION_HOST_TAG" \ --output text \ --query 'Reservations[*].Instances[*].InstanceId' \ --output text`
	2. Copiez l'ID de l' EC2 instance Amazon. Vous	

Tâche	Description	Compétences requises
	utiliserez cet identifiant ultérieurement.	

Tâche	Description	Compétences requises
Envoyez la clé publique SSH.	**Note** Dans cette section, vous allez télécharger la clé publique vers les métadonnées de l'instance de l'hôte Bastion. Une fois la clé téléchargée, vous avez 60 secondes pour établir une connexion avec l'hôte du bastion. Au bout de 60 secondes, la clé publique est supprimée. Pour plus d'informations, consultez la section Dépannage de ce modèle. Effectuez rapidement les étapes suivantes pour éviter que la clé ne soit supprimée avant de vous connecter à l'hôte Bastion. 1. Envoyez la clé SSH à l'hôte Bastion à l'aide d'Amazon Instance EC2 Connect. Entrez la commande suivante, où :	AWS général

Tâche	Description	Compétences requises
	• `$INSTANCE_ID` est l'ID de l' EC2 instance Amazon • `$PUBLIC_KEY_FILE` est le chemin d'accès à votre fichier de clé publique, tel que `my_key.pub` **Important** Veillez à utiliser la clé publique et non la clé privée. `aws ec2-instance-connect send-ssh-public-key \ --instance-id $INSTANCE_ID \ --instance-os-user ec2-user \ --ssh-public-key file://$PUBLIC_KEY_FILE` 2. Attendez de recevoir un message indiquant que la clé a été téléchargée avec succès. Passez immédiatement à l'étape suivante.	

Tâche	Description	Compétences requises
Connectez-vous à l'hôte Bastion.	1. Entrez la commande suivante pour vous connecter à l'hôte bastion via le gestionnaire de session, où : • `$PRIVATE_KEY_FILE` est le chemin d'accès à votre clé privée, tel que `my_key` • `$INSTANCE_ID` est l'ID de l' EC2 instance Amazon `ssh -i $PRIVATE_KEY_FILE ec2-user@$INSTANCE_ID` 2. Confirmez la connexion en entrant`yes`. Cela ouvre une connexion SSH à l'aide du gestionnaire de session. **Note** Il existe d'autres options pour ouvrir une connexion SSH avec l'hôte Bastion. Pour plus d'informations, consultez la section Autres approches pour établir une connexion SSH avec l'hôte Bastion dans la	AWS général

Tâche	Description	Compétences requises
	section Informations supplémentaires de ce modèle.	

(Facultatif) Nettoyer

Tâche	Description	Compétences requises
Supprimez les ressources déployées.	1. Afin de supprimer toutes les ressources déployées , exécutez la commande suivante depuis le répertoire racine du référentiel cloné. `terraform destroy -var-file="dev.tfvars"` 2. Confirmez la suppression des ressources.	DevOps ingénieur, Développeur, Terraform

Résolution des problèmes

Problème	Solution
`TargetNotConnected` erreur lors de la tentative de connexion à l'hôte bastion	1. Redémarrez l'hôte Bastion conformément aux instructions de la section Redémarrer votre instance dans la EC2 documentation Amazon. 2. Une fois l'instance redémarrée avec succès, renvoyez la clé publique à l'hôte Bastion et tentez à nouveau de vous connecter.

Problème	Solution
`Permission denied` erreur lors de la tentative de connexion à l'hôte bastion	Une fois la clé publique téléchargée sur l'hôte du bastion, vous n'avez que 60 secondes pour établir la connexion. Après 60 secondes, la clé est automatiquement supprimée et vous ne pouvez pas l'utiliser pour vous connecter à l'instance. Dans ce cas, vous pouvez répéter l'étape pour renvoyer la clé à l'instance.

Ressources connexes

AWS documentation

- AWS Systems Manager Session Manager(documentation de Systems Manager)
- Installez le plugin Session Manager pour AWS CLI (documentation Systems Manager)
- Autoriser les connexions SSH pour Session Manager (documentation Systems Manager)
- À propos de l'utilisation d' EC2 Instance Connect (EC2 documentation Amazon)
- Connectez-vous à l'aide d' EC2 Instance Connect (EC2 documentation Amazon)
- Gestion des identités et des accès pour Amazon EC2 (EC2 documentation Amazon)
- Utilisation d'un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon (documentation IAM)
- Bonnes pratiques de sécurité dans le domaine de l'IAM (documentation IAM)
- Contrôlez le trafic vers les ressources à l'aide de groupes de sécurité (documentation Amazon VPC)

Autres ressources

- Page Web du développeur Terraform
- Commande : valider (documentation Terraform)
- Commande : fmt (documentation Terraform)
- Tester HashiCorp Terraform (HashiCorp article de blog)
- Page Web de Checkov

Informations supplémentaires

Autres approches pour établir une connexion SSH avec l'hôte Bastion

Réacheminement de port

Vous pouvez utiliser `-D 8888` cette option pour ouvrir une connexion SSH avec une redirection de port dynamique. Pour plus d'informations, consultez les instructions sur explainshell.com. Voici un exemple de commande permettant d'ouvrir une connexion SSH à l'aide de la redirection de port.

```
ssh -i $PRIVATE_KEY_FILE -D 8888 ec2-user@$INSTANCE_ID
```

Ce type de connexion ouvre un proxy SOCKS qui peut transférer le trafic depuis votre navigateur local via l'hôte Bastion. Si vous utilisez Linux ou macOS, pour voir toutes les options, entrez`man ssh`. Cela affiche le manuel de référence SSH.

À l'aide du script fourni

Au lieu d'exécuter manuellement les étapes décrites dans Connect to the bastion host by using Session Manager dans la section Epics, vous pouvez utiliser le script connect.sh inclus dans le référentiel de code. Ce script génère la paire de clés SSH, transmet la clé publique à l' EC2 instance Amazon et établit une connexion avec l'hôte Bastion. Lorsque vous exécutez le script, vous transmettez le tag et le nom de la clé en tant qu'arguments. Voici un exemple de commande permettant d'exécuter le script.

```
./connect.sh sandbox-dev-bastion-host my_key
```

Centralisation de la résolution DNS à l'aide AWS Managed Microsoft AD et sur site de Microsoft Active Directory

Créée par Brian Westmoreland (AWS)

Récapitulatif

Ce modèle fournit des conseils pour centraliser la résolution DNS dans un environnement AWS multi-comptes en utilisant à la fois AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) et Amazon Route 53. Dans ce modèle, l'espace de noms AWS DNS est un sous-domaine de l'espace de noms DNS local. Ce modèle fournit également des conseils sur la façon de configurer les serveurs DNS locaux pour transférer les requêtes AWS lorsque la solution DNS locale utilise Microsoft Active Directory.

Conditions préalables et limitations

Prérequis

- Un environnement AWS multi-comptes configuré à l'aide AWS Organizations de.
- Connectivité réseau établie entre Comptes AWS.
- Connectivité réseau établie entre AWS et l'environnement sur site (en utilisant AWS Direct Connect ou tout type de connexion VPN).
- AWS Command Line Interface (AWS CLI) configuré sur un poste de travail local.
- AWS Resource Access Manager (AWS RAM) utilisé pour partager les règles de Route 53 entre les comptes. Par conséquent, le partage doit être activé dans l' AWS Organizations environnement, comme décrit dans la section Epics.

Limites

- AWS Managed Microsoft AD L'édition standard est limitée à 5 partages.
- AWS Managed Microsoft AD L'édition Enterprise est limitée à 125 actions.
- La solution dans ce modèle se limite à Régions AWS ce support via le partage AWS RAM.

Versions du produit

- Microsoft Active Directory s'exécute sous Windows Server 2008, 2012, 2012 R2 ou 2016.

Architecture

Architecture cible

Dans cette conception, AWS Managed Microsoft AD est installé dans les services partagés Compte AWS. Bien qu'il ne s'agisse pas d'une exigence, ce modèle suppose cette configuration. Si vous configurez AWS Managed Microsoft AD différemment Compte AWS, vous devrez peut-être modifier les étapes de la section Epics en conséquence.

Cette conception utilise les résolveurs Route 53 pour prendre en charge la résolution de noms grâce aux règles Route 53. Si la solution DNS sur site utilise le DNS Microsoft, la création d'une règle de transfert conditionnelle pour l'espace de noms AWS (`aws.company.com`), qui est un sous-domaine de l'espace de noms DNS de l'entreprise (`company.com`), n'est pas simple. Si vous essayez de créer un redirecteur conditionnel traditionnel, une erreur se produira. Cela est dû au fait que Microsoft Active Directory est déjà considéré comme faisant autorité pour tous les sous-domaines de. `company.com` Pour contourner cette erreur, vous devez d'abord créer une délégation pour `aws.company.com` déléguer l'autorité de cet espace de noms. Vous pouvez ensuite créer le redirecteur conditionnel.

Le cloud privé virtuel (VPC) de chaque compte parlé peut avoir son propre espace de noms DNS unique basé sur l'espace de noms racine. AWS Dans cette conception, chaque compte Spoke ajoute une abréviation du nom du compte à l'espace de noms AWS de base. Une fois que les zones hébergées privées dans le compte parlé ont été créées, les zones sont associées au VPC local dans le compte parlé ainsi qu'au VPC dans le compte réseau central. AWS Cela permet au compte du AWS réseau central de répondre aux requêtes DNS relatives aux comptes parlés. Ainsi, Route 53 et Route AWS Managed Microsoft AD travaillent ensemble pour partager la responsabilité de la gestion de l'espace de AWS noms (`aws.company.com`).

Automatisation et mise à l'échelle

Cette conception utilise les points de terminaison Route 53 Resolver pour redimensionner les requêtes DNS entre AWS et votre environnement sur site. Chaque point de terminaison Route 53 Resolver comprend plusieurs interfaces réseau élastiques (réparties sur plusieurs zones de disponibilité), et chaque interface réseau peut traiter jusqu'à 10 000 requêtes par seconde. Route 53 Resolver prend en charge jusqu'à 6 adresses IP par point de terminaison. Au total, cette conception prend en charge jusqu'à 60 000 requêtes DNS par seconde réparties sur plusieurs zones de disponibilité pour une haute disponibilité.

De plus, ce modèle tient automatiquement compte de la future croissance interne AWS. Il n'est pas nécessaire de modifier les règles de transfert DNS configurées sur site pour prendre en charge les nouvelles zones hébergées privées VPCs et leurs zones associées qui sont ajoutées à AWS.

Outils

Services AWS

- AWS Directory Service for Microsoft Active Directorypermet à vos charges de travail et à vos AWS ressources sensibles aux annuaires d'utiliser Microsoft Active Directory dans le. AWS Cloud
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Resource Access Manager (AWS RAM) vous permet de partager vos ressources en toute sécurité afin Comptes AWS de réduire les frais opérationnels et de garantir visibilité et auditabilité.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.

Outils

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande. Dans ce modèle, le AWS CLI est utilisé pour configurer les autorisations Route 53.

Épopées

Création et partage d'un AWS Managed Microsoft AD répertoire

Tâche	Description	Compétences requises
Déployez AWS Managed Microsoft AD.	1. Créez et configurez un nouveau répertoire. Pour connaître les étapes détaillées, consultez la section Création de votre AWS Managed Microsoft AD dans le guide d'AWS Directory Service administration.	Administrateur AWS

Tâche	Description	Compétences requises
	2. Enregistrez les adresses IP des contrôleurs de AWS Managed Microsoft AD domaine. Elles seront référencées dans une étape ultérieure.	
Partagez le répertoire.	Une fois le répertoire créé, partagez-le avec d'autres membres Comptes AWS de l' AWS organisation. Pour obtenir des instructions, consultez la section Partager votre répertoire dans le Guide d'AWS Directory Service administration. **Note** AWS Managed Microsoft AD L'édition standard est limitée à 5 partages. L'édition Enterprise est limitée à 125 actions.	Administrateur AWS

Configurer Route 53

Tâche	Description	Compétences requises
Créez des résolveurs Route 53.	Les résolveurs Route 53 facilitent la résolution des requêtes DNS entre AWS et le centre de données sur site.	Administrateur AWS

Tâche	Description	Compétences requises
	1. Installez les résolveurs Route 53 en suivant les instructions du Guide du développeur Route 53. 2. Configurez les résolveurs Route 53 dans des sous-réseaux privés situés dans au moins deux zones de disponibilité au sein du compte AWS réseau central (VPC) pour une haute disponibilité. **Note** Bien que l'utilisation du compte AWS réseau central VPC ne soit pas obligatoire, les étapes restantes supposent cette configuration.	

Tâche	Description	Compétences requises

Créez les règles de la Route 53.	Votre cas d'utilisation spécifique peut nécessiter un grand nombre de règles Route 53, mais vous devrez configurer les règles suivantes comme référence :
	• Une règle sortante pour l'espace de noms local (`company.com`) en utilisant les résolveurs Route 53 sortants du compte réseau central. Les adresses IP cibles sont les serveurs DNS locaux.
	  • Associez cette règle au compte VPC du réseau central.
	• Une règle sortante pour l'espace de AWS noms (`aws.company.com`) en utilisant les résolveurs Route 53 sortants du compte réseau central. Les adresses IP cibles sont les adresses IP du résolveur Route 53 entrant dans le compte réseau central.
	  • N'associez pas cette règle au compte AWS réseau central VPC (qui héberge les résolveurs Route 53).
	• Une deuxième règle sortante pour l' AWS espace
		Administrateur AWS

Tâche	Description	Compétences requises
	de noms (`aws.company.com`) qui pointe vers les contrôleurs de AWS Managed Microsoft AD domaine (utilisez celle IPs de l'épopée précédente). • Associez cette règle au compte AWS réseau central VPC (qui héberge les résolveurs Route 53). • Ne partagez pas et n'associez pas cette règle à d'autres Comptes AWS. Pour plus d'informations, consultez la section Gestion des règles de transfert dans le Guide du développeur de Route 53.	

Tâche	Description	Compétences requises
Configurez un profil Route 53.	Un profil Route 53 est utilisé pour partager les règles avec les comptes Spoke. 1. Créez un nouveau profil Route 53 dans le compte réseau central en suivant les instructions du Guide du développeur Route 53. 2. Ajoutez la règle pour l'espace de noms local (`company.com`) au profil. 3. Ajoutez la première règle pour l' AWS espace de noms (`aws.company.com`), qui cible les adresses IP des résolveurs entrants Route 53, au profil. 4. Partagez le profil Route 53 avec l' AWS organisation. 5. Acceptez le partage des ressources du profil Route 53 dans chaque compte Spoke. 6. Associez le profil Route 53 à chaque VPC de compte Spoke.	Administrateur AWS

Configuration du DNS Active Directory sur site

Tâche	Description	Compétences requises
Créez la délégation.	Utilisez le composant logiciel enfichable Microsoft DNS (`dnsmgmt.msc`) pour créer une nouvelle délégation pour l'espace de `company.com` noms dans Active Directory. Le nom du domaine délégué doit être`aws`. Cela constitue le nom de domaine complet (FQDN) de la délégatio `naws.company.com` . Utilisez les adresses IP des contrôleurs de AWS Managed Microsoft AD domaine pour les valeurs IP du serveur de noms, et `server.aw s.company.com` utilisez-les pour le nom. (Cette délégation est uniquement destinée à la redondance, car un redirecteur conditionnel sera créé pour cet espace de noms qui aura priorité sur la délégation.)	Active Directory
Créez le redirecteur condition nel.	Utilisez le composant logiciel enfichable Microsoft DNS (`dnsmgmt.msc`) pour créer un nouveau redirecteur conditionnel pour. `aws.compa ny.com` Utilisez les adresses IP des résolveurs Route 53 AWS entrants dans	Active Directory

Tâche	Description	Compétences requises
	le DNS central Compte AWS pour la cible du redirecteur conditionnel.	

Créez des zones hébergées privées Route 53 pour Spoke Comptes AWS

Tâche	Description	Compétences requises
Créez les zones hébergées privées Route 53.	Créez une zone hébergée privée Route 53 dans chaque compte Spoke. Associez cette zone hébergée privée au VPC du compte Spoke. Pour connaître les étapes détaillées, consultez la section Création d'une zone hébergée privée dans le Guide du développeur de Route 53.	Administrateur AWS
Créez des autorisations.	Utilisez le AWS CLI pour créer une autorisation pour le compte AWS VPC du réseau central. Exécutez cette commande à partir du contexte de chaque rayon Compte AWS : `aws route53 create-vpc-association-authorization --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>`	Administrateur AWS

Tâche	Description	Compétences requises
	où : • `<hosted-zone-id>` est la zone hébergée privée Route 53 dans le compte Spoke. • `<region>`et `<vpc-id>` sont l'identifiant Région AWS et le VPC du compte VPC du AWS réseau central.	

Tâche	Description	Compétences requises
Créez des associations.	Créez l'association de zone hébergée privée Route 53 pour le compte VPC du AWS réseau central à l'aide du. AWS CLI Exécutez cette commande depuis le contexte du compte AWS réseau central : `aws route53 associate-vpc-with-hosted-zone --hosted-zone-id <hosted-zone-id> \ --vpc VPCRegion=<region>,VPCId=<vpc-id>` où : • `<hosted-zone-id>` est la zone hébergée privée Route 53 dans le compte Spoke. • `<region>`et `<vpc-id>` sont l'identifiant VPC Région AWS et le compte du AWS réseau central.	Administrateur AWS

Ressources connexes

- Simplifiez la gestion du DNS dans un environnement multi-comptes avec Route 53 Resolver (AWS article de blog)
- Création de votre AWS Managed Microsoft AD (AWS Directory Service documentation)
- Partage d'un AWS Managed Microsoft AD répertoire (AWS Directory Service documentation)
- Qu'est-ce que c'est Amazon Route 53 Resolver ? (documentation Amazon Route 53)

- Création d'une zone hébergée privée (documentation Amazon Route 53)
- Que sont les profils Amazon Route 53 ? (documentation Amazon Route 53)

Centralisez la surveillance à l'aide d'Amazon CloudWatch Observability Access Manager

Créée par Anand Krishna Varanasi (AWS), Jimmy Morgan (AWS), Ashish Kumar (AWS), Balaji Vedagiri (AWS), JAGDISH KOMAKULA (AWS), Sarat Chandra Pothula (AWS) et Vivek Thangamuthu (AWS)

Récapitulatif

L'observabilité est essentielle à la surveillance, à la compréhension et au dépannage des applications. Les applications qui couvrent plusieurs comptes, comme les AWS Control Tower implémentations de zones de landing zone, génèrent un grand nombre de journaux et de données de suivi. Pour résoudre rapidement les problèmes ou comprendre les analyses des utilisateurs ou les analyses commerciales, vous avez besoin d'une plateforme d'observabilité commune à tous les comptes. L'Amazon CloudWatch Observability Access Manager vous permet d'accéder à plusieurs journaux de comptes et de les contrôler à partir d'un emplacement central.

Vous pouvez utiliser le gestionnaire d'accès à l'observabilité pour consulter et gérer les journaux de données d'observabilité générés par les comptes sources. Les comptes sources sont des comptes individuels Comptes AWS qui génèrent des données d'observabilité pour leurs ressources. Les données d'observabilité sont partagées entre les comptes sources et les comptes de surveillance. Les données d'observabilité partagées peuvent inclure des métriques dans Amazon CloudWatch, des logs dans Amazon CloudWatch Logs et des traces in AWS X-Ray. Pour plus d'informations, consultez la documentation d'Observability Access Manager.

Ce modèle est destiné aux utilisateurs dont les applications ou les infrastructures s'exécutent en plusieurs parties Comptes AWS et qui ont besoin d'un emplacement commun pour consulter les journaux. Il explique comment configurer Observability Access Manager à l'aide de Terraform, pour surveiller l'état et l'état de santé de ces applications ou infrastructures. Vous pouvez installer cette solution de plusieurs manières :

- En tant que module Terraform autonome que vous configurez manuellement
- En utilisant un pipeline d'intégration continue et de livraison continue (CI/CD)
- En s'intégrant à d'autres solutions telles que AWS Control Tower Account Factory for Terraform (AFT)

Les instructions de la section Epics couvrent la mise en œuvre manuelle. Pour les étapes d'installation d'AFT, consultez le fichier README du référentiel GitHub Observability Access Manager.

Conditions préalables et limitations

Prérequis

- Terraform installé ou référencé dans votre système ou dans des pipelines automatisés. (Nous vous recommandons d'utiliser la dernière version.)
- Un compte que vous pouvez utiliser comme compte de surveillance centralisé. D'autres comptes créent des liens vers le compte de surveillance central afin de consulter les journaux.
- (Facultatif) Un référentiel de code source tel qu' GitHubAtlassian Bitbucket ou un système similaire. AWS CodeCommit Un référentiel de code source n'est pas nécessaire si vous utilisez des pipelines CI/CD automatisés.
- (Facultatif) Autorisations permettant de créer des pull requests (PRs) pour la révision du code et la collaboration en matière de code dans GitHub.

Limites

Observability Access Manager dispose des quotas de service suivants, qui ne peuvent pas être modifiés. Tenez compte de ces quotas avant de déployer cette fonctionnalité. Pour plus d'informations, consultez la section Quotas de CloudWatch service dans la CloudWatch documentation.

- Liens vers des comptes sources : vous pouvez associer chaque compte source à un maximum de cinq comptes de surveillance.
- Réservoirs : vous pouvez créer plusieurs récepteurs pour un compte, mais un seul récepteur par compte Région AWS est autorisé.

En outre :

- Les cuvettes et les liens doivent être créés de la même manière Région AWS ; ils ne peuvent pas être interrégionaux.

Surveillance entre régions et entre comptes

Pour la surveillance entre régions et entre comptes, vous pouvez choisir l'une des options suivantes :

- Créez des CloudWatch tableaux de bord inter-comptes et interrégionaux pour les alarmes et les métriques. Cette option ne prend pas en charge les journaux et les traces.
- Mettez en œuvre une journalisation centralisée à l'aide d'Amazon OpenSearch Service.
- Créez un récepteur par région à partir de tous les comptes locataires, envoyez les métriques vers un compte de surveillance centralisé (comme décrit dans ce modèle), puis utilisez des flux de CloudWatch métriques pour envoyer les données vers une destination externe commune ou vers des produits de surveillance tiers tels que Datadog, Dynatrace, Sumo Logic, Splunk ou New Relic.

Architecture

Composants

CloudWatch Observability Access Manager se compose de deux composants principaux qui permettent l'observabilité entre comptes :

- Un récepteur permet aux comptes source d'envoyer des données d'observabilité au compte de surveillance central. Un récepteur fournit essentiellement une passerelle à laquelle les comptes source peuvent se connecter. Il ne peut y avoir qu'une seule passerelle ou connexion réceptrice, et plusieurs comptes peuvent s'y connecter.
- Chaque compte source possède un lien vers la jonction de la passerelle réceptrice, et les données d'observabilité sont envoyées via ce lien. Vous devez créer un récepteur avant de créer des liens à partir de chaque compte source.

Architecture

Le schéma suivant illustre Observability Access Manager et ses composants.

Outils

Services AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.

Outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources sur site et dans le cloud.
- AWS Control Tower Account Factory for Terraform (AFT) met en place un pipeline Terraform pour vous aider à approvisionner et à personnaliser des comptes dans. AWS Control Tower Vous pouvez éventuellement utiliser AFT pour configurer Observability Access Manager à grande échelle sur plusieurs comptes.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Observability Access Manager.

Bonnes pratiques

- Dans AWS Control Tower les environnements, marquez le compte de journalisation comme compte de surveillance central (récepteur).
- Si plusieurs organisations possèdent plusieurs comptes AWS Organizations, nous vous recommandons d'inclure les organisations plutôt que les comptes individuels dans la politique de configuration. Si vous avez un petit nombre de comptes ou si les comptes ne font pas partie d'une organisation dans la politique de configuration du récepteur, vous pouvez décider d'inclure des comptes individuels à la place.

Épopées

Configuration du module d'évier

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le référentiel GitHub Observability Access Manager :	AWS DevOps, administrateur du cloud, administrateur AWS

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/cloudwatch-observability-access-manager-terraform`	

Tâche	Description	Compétences requises
Spécifiez les valeurs des propriétés du module récepteur.	Dans le `main.tf` fichier (dans le `deployments/aft-account-customizations/LOGGING/terraform/` dossier du référentiel), spécifiez les valeurs des propriétés suivantes : • `sink_name` : nom de l'CloudWatch évier. • `allowed_oam_resource_types` : Observability Access Manager prend actuellement en charge les CloudWatch métriques, les groupes de journaux et les AWS X-Ray traces. • `allowed_source_accounts` : comptes source autorisés à envoyer des journaux au compte CloudWatch récepteur central. • `allowed_source_organizations` : les AWS Control Tower organisations sources autorisées à envoyer des journaux vers le compte CloudWatch récepteur central. Pour plus d'informations, consultez AWS::Oam:	AWS DevOps, administrateur du cloud, administrateur AWS

Tâche	Description	Compétences requises
	:Sinkla AWS CloudFormation documentation.	

Installez le module d'évier.	Exportez les informations d'identification du compte Compte AWS que vous avez sélectionné comme compte de surveillance et installez le module récepteur Observabi lity Access Manager :
	`Terraform Init`
	`Terrafom Plan`
	`Terraform Apply`
		AWS DevOps, administrateur du cloud, administrateur AWS

Configuration du module de liaison

Tâche	Description	Compétences requises

Spécifiez les valeurs des propriétés du module de liaison.	Dans le `main.tf` fichier (dans le `deployments/aft-account-cus tomizations/LOGGIN G/terraform/` dossier du référentiel), spécifiez les valeurs des propriétés suivantes :
	• `account_label` : utilisez l'une des valeurs suivantes :
	  • `$AccountName` : nom du compte.
	  • `$AccountEmail` : adresse e-mail unique
		AWS DevOps, administrateur du cloud, architecte du cloud

Tâche	Description	Compétences requises
	au monde, qui inclut le domaine de messagerie (par exemple,`hello@example.com`) • `$AccountEmailNoDomain` : une adresse e-mail sans le nom de domaine. • `allowed_oam_resource_types` : Observability Access Manager prend actuellement en charge les CloudWatch métriques, les groupes de journaux et les AWS X-Ray traces. Pour plus d'informations, consultez AWS::Oam::Link la AWS CloudFormation documentation.	

Tâche	Description	Compétences requises

Installez le module de liaison pour les comptes individuels.	Exportez les informations d'identification des comptes individuels et installez le module de lien Observability Access Manager :
	`Terraform Plan`
	`Terraform Apply`
	Vous pouvez configurer le module de liaison individue llement pour chaque compte ou utiliser AFT pour installer automatiquement ce module sur un grand nombre de comptes.
		AWS DevOps, administrateur du cloud, architecte du cloud

Approuver sink-to-link les connexions

Tâche	Description	Compétences requises
Vérifiez le message d'état.	1. Connectez-vous au compte de surveillance. 2. Ouvrez la CloudWatch console. 3. Dans le panneau de navigation de gauche, choisissez Paramètres. Sur la droite, vous devriez voir le message d'état Monitorin g account enabled avec une coche verte. Cela signifie	

Tâche	Description	Compétences requises
	que le compte de surveillance dispose d'un récepteur Observability Access Manager auquel les liens des autres comptes se connecteront.	

Tâche	Description	Compétences requises
Approuvez les link-to-sink connexions.	1. Choisissez l'option Ressources pour lier les comptes sous le message d'état. Les informations confirment qu'il s'agit du compte de surveillance, répertorient les données partagées à partir des comptes sources des locataires (journaux, métriques, traces) et indiquent le libellé du compte sous la forme $AccountName. Cet écran propose deux options pour lier les comptes des locataires au compte de surveillance : approbation au niveau de l'organisation ou approbation au niveau du compte. Pour chaque option, vous pouvez choisir de télécharger un AWS CloudFormation modèle pour l'approbation ou d'approuver chaque compte individuellement. 2. Pour plus de simplicité, choisissez N'importe quel compte à approuver à chaque niveau de compte. Cette option fournit un lien d'approbation pour le compte.	AWS DevOps, administrateur du cloud, architecte du cloud

Tâche	Description	Compétences requises
	3. Choisissez Copier l'URL pour copier le lien. 4. Connectez-vous à chaque compte source. 5. Dans une fenêtre de navigateur, collez le lien, puis choisissez Approuver la connexion du lien au récepteur. 6. Répétez l'opération pour les comptes sources supplémentaires. Pour plus d'informations, consultez la section Lier les comptes de surveillance aux comptes source dans la CloudWatch documentation.	

Vérifier les données d'observabilité entre comptes

Tâche	Description	Compétences requises
Afficher les données entre comptes.	1. Connectez-vous au compte de surveillance central. 2. Ouvrez la CloudWatch console. 3. Dans le volet de navigation de gauche, choisissez des options pour afficher les journaux, les métriques et les traces entre comptes.	AWS DevOps, administrateur du cloud, architecte du cloud

(Facultatif) Permettre aux comptes source de faire confiance au compte de surveillance

Tâche	Description	Compétences requises
Consultez les métriques, les tableaux de bord, les journaux, les widgets et les alarmes d'autres comptes.	En tant que fonctionnalité supplémentaire, vous pouvez partager les CloudWatch métriques, les tableaux de bord, les journaux, les widgets et les alarmes avec d'autres comptes. Chaque compte utilise un rôle IAM appelé CloudWatch- CrossAcco untSharingRole pour accéder à ces données. Les comptes sources entretenant une relation de confiance avec le compte de surveillance central peuvent assumer ce rôle et consulter les données du compte de surveillance. CloudWatch fournit un exemple de CloudFormation script pour créer le rôle. Choisissez Gérer le rôle dans IAM et exécutez ce script dans les comptes sur lesquels vous souhaitez consulter les données. `{ "Version": "2012-10-17", "Statement": [ {`	AWS DevOps, administrateur du cloud, architecte du cloud

Tâche	Description	Compétences requises
	<pre>"Effect": "Allow", "Principal": { "AWS": ["arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root", "arn:aws:iam::XXXXXXXXXX:root"] }, "Action": "sts:AssumeRole" }] }</pre> Pour plus d'informations, consultez la section Activation de la fonctionnalité multi-comptes CloudWatch dans la CloudWatch documentation.	

(Facultatif) Afficher les comptes entre les régions à partir du compte de surveillance

Tâche	Description	Compétences requises
Configurez un accès entre comptes et entre régions.	Dans le compte de surveillance central, vous pouvez éventuellement ajouter un	AWS DevOps, administrateur du cloud, architecte du cloud

Tâche	Description	Compétences requises
	sélecteur de compte pour passer facilement d'un compte à l'autre et consulter leurs données sans avoir à vous authentifier. 1. Connectez-vous au compte de surveillance central. 2. Ouvrez la CloudWatch console. 3. Dans le panneau de navigation de gauche, choisissez Paramètres. 4. Dans la section Afficher plusieurs comptes entre régions, choisissez Configurer. 5. Choisissez Activer, puis cochez la case Afficher le sélecteur dans la console. 6. Choisissez l'une des options suivantes : • Saisie de l'identifiant du compte : cette option vous invite à saisir manuellement l'identif iant du compte chaque fois que vous souhaitez changer de compte pour afficher les données entre comptes. • Sélecteur de compte AWS Organization : si vous l'avez intégré	

Tâche	Description	Compétences requises
	CloudWatch AWS Organizations, cette option fournit un sélecteur déroulant avec une liste complète des comptes de l'organisation. • Sélecteur de compte personnalisé : cette option vous permet de saisir manuellement une liste de comptes IDs pour remplir le sélecteur. 7. Sélectionnez Enregistrer les modifications. Pour plus d'informations, consultez la section CloudWatch Console entre comptes et régions dans la CloudWatch documentation.	

Ressources connexes

- CloudWatch observabilité entre comptes (documentation Amazon CloudWatch)
- Référence d'API Amazon CloudWatch Observability Access Manager (CloudWatch documentation Amazon)
- Ressource : aws_oam_sink (documentation Terraform)
- Source de données : aws_oam_link (documentation Terraform)
- CloudWatchObservabilityAccessManager(documentation AWS Boto3)

Vérifiez la présence de balises obligatoires dans les EC2 instances au lancement

Créée par Susanne Kangnoh (AWS) et Archit Mathur (AWS)

Récapitulatif

Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud Amazon Web Services (AWS). Avec Amazon, vous EC2 n'avez plus besoin d'investir dans du matériel dès le départ, ce qui vous permet de développer et de déployer des applications plus rapidement.

Vous pouvez utiliser le balisage pour classer vos ressources AWS de différentes manières. EC2 le balisage d'instance est utile lorsque votre compte comporte de nombreuses ressources et que vous souhaitez identifier rapidement une ressource spécifique en fonction des balises. Vous pouvez attribuer des métadonnées personnalisées à vos EC2 instances à l'aide de balises. Une balise se compose d'une clé et d'une valeur définies par l'utilisateur. Nous vous recommandons de créer un ensemble cohérent de balises pour répondre aux exigences de votre organisation.

Ce modèle fournit un CloudFormation modèle AWS pour vous aider à surveiller les EC2 instances pour détecter des balises spécifiques. Le modèle crée un événement Amazon CloudWatch Events qui surveille l'AWS CloudTrail TagResourceou les UntagResourceévénements, afin de détecter le balisage ou le retrait de balises d'une nouvelle EC2 instance. Si une balise prédéfinie est absente, elle appelle une fonction AWS Lambda, qui envoie un message de violation à l'adresse e-mail que vous fournissez, à l'aide d'Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un bucket Amazon Simple Storage Service (Amazon S3) pour télécharger le code Lambda fourni.
- Adresse e-mail à laquelle vous souhaitez recevoir des notifications de violation.

Limites

- Cette solution prend en charge CloudTrail TagResourcenos UntagResourceévénements. Il ne crée pas de notifications pour d'autres événements.

- Cette solution vérifie uniquement les clés de balise. Il ne surveille pas les valeurs clés.

Architecture

Architecture du flux de travail

Automatisation et mise à l'échelle

- Vous pouvez utiliser le CloudFormation modèle AWS à plusieurs reprises pour différents comptes et régions AWS. Vous ne devez exécuter le modèle qu'une seule fois dans chaque région ou compte.

Outils

Services AWS

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) est un service Web qui fournit une capacité de calcul sécurisée et redimensionnable dans le cloud. Il est conçu pour faciliter le cloud computing à l'échelle du Web pour les développeurs.
- AWS CloudTrail CloudTrail est un service AWS qui vous aide en matière de gouvernance, de conformité, d'audit opérationnel et de gestion des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS. CloudWatch Events prend connaissance des changements opérationnels au fur et à mesure qu'ils se produisent et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état.
- AWS Lambda — Lambda est un service de calcul qui prend en charge l'exécution de code sans qu'il soit nécessaire de configurer ou de gérer des serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service Web qui permet aux applications, aux utilisateurs finaux et aux appareils d'envoyer et de recevoir instantanément des notifications depuis le cloud.

Code

Ce modèle inclut une pièce jointe contenant deux fichiers :

- `index.zip`est un fichier compressé qui inclut le code Lambda pour ce modèle.
- `ec2-require-tags.yaml`est un CloudFormation modèle qui déploie le code Lambda.

Consultez la section Epics pour plus d'informations sur l'utilisation de ces fichiers.

Épopées

Déployer le code Lambda

Tâche	Description	Compétences requises
Téléchargez le code dans un compartiment S3.	Créez un nouveau compartiment S3 ou utilisez un compartiment S3 existant pour télécharger le `index.zip` fichier joint (code Lambda). Ce compartiment doit se trouver dans la même région AWS que les ressources (EC2 instances) que vous souhaitez surveiller.	Architecte du cloud
Déployez le CloudFormation modèle.	Ouvrez la console Cloudformation dans la même région AWS que le compartiment S3 et déployez le `ec2-requi`	Architecte du cloud

Tâche	Description	Compétences requises
	`re-tags.yaml` fichier fourni dans la pièce jointe. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou sélectionné dans le premier épisode épique. Ce compartiment S3 contient le fichier .zip pour le code Lambda et doit se trouver dans la même région AWS que CloudFormation le modèle et EC2 les instances que vous souhaitez surveiller.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple, ou). `index.zip` `controls/index.zip`	Architecte du cloud
Indiquez une adresse e-mail.	Indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications de violation.	Architecte du cloud

Tâche	Description	Compétences requises
Définissez un niveau de journalisation.	Spécifiez le niveau de journalisation et la verbosité. `Info`désigne des messages d'information détaillés sur la progression de l'application et ne doit être utilisé que pour le débogage. `Error`désigne les événements d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situations potentiellement dangereuses.	Architecte du cloud
Entrez les clés de tag requises.	Entrez les clés de tag que vous souhaitez vérifier. Si vous souhaitez spécifier plusieurs clés, séparez-les par des virgules, sans espaces. (Par exemple, `ApplicationId,CreatedBy,Environment,Organization` recherche quatre clés.) L'événement CloudWatch Events recherche ces clés de balise et envoie une notification si elles ne sont pas trouvées.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'abonnement par e-mail.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Pour recevoir des notificat ions, vous devez confirmer cet abonnement par e-mail.	Architecte du cloud

Ressources connexes

- Création d'un compartiment (documentation Amazon S3)
- Chargement d'objets (documentation Amazon S3)
- Marquez vos EC2 ressources Amazon (EC2 documentation Amazon)
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail (CloudWatch documentation Amazon)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Nettoyez les ressources de AWS Account Factory for Terraform (AFT) en toute sécurité après la perte du fichier d'état

Créée par Gokendra Malviya (AWS)

Récapitulatif

Lorsque vous utilisez AWS Account Factory for Terraform (AFT) pour gérer votre AWS Control Tower environnement, AFT génère un fichier d'état Terraform pour suivre l'état et la configuration des ressources créées par Terraform. La perte du fichier d'état Terraform peut créer des défis importants pour la gestion et le nettoyage des ressources. Ce modèle fournit une approche systématique pour identifier et supprimer en toute sécurité les ressources liées à l'AFT tout en préservant l'intégrité de votre AWS Control Tower environnement.

Le processus est conçu pour garantir le retrait correct de tous les composants AFT, même sans la référence au fichier d'état d'origine. Ce processus fournit une voie claire pour rétablir et reconfigurer avec succès l'AFT dans votre environnement, afin de minimiser les perturbations de vos AWS Control Tower opérations.

Pour plus d'informations sur l'AFT, consultez la AWS Control Tower documentation.

Conditions préalables et limitations

Prérequis

- Compréhension approfondie de l'architecture AFT.
- Accès administrateur aux comptes suivants :
  - Compte de gestion AFT
  - AWS Control Tower Compte de gestion
  - Compte Log Archive
  - Compte d'audit
- Vérification qu'aucune politique de contrôle des services (SCPs) ne contient de restrictions ou de limitations susceptibles de bloquer la suppression de ressources liées à l'AFT.

Limites

- Ce processus permet de nettoyer efficacement les ressources, mais il ne peut pas récupérer les fichiers d'état perdus, et certaines ressources peuvent nécessiter une identification manuelle.

- La durée du processus de nettoyage dépend de la complexité de votre environnement et peut prendre plusieurs heures.
- Ce modèle a été testé avec la version 1.12.2 d'AFT et supprime les ressources suivantes. Si vous utilisez une autre version d'AFT, vous devrez peut-être supprimer des ressources supplémentaires.

Nom du service	Nombre de ressources
AWS CodeBuild	6
AWS CodeCommit	4
AWS CodePipeline	4
Amazon DynamoDB	5
Amazon Elastic Compute Cloud (Amazon EC2)	16
Amazon EventBridge	4
AWS Identity and Access Management Rôles (IAM)	40
AWS Key Management Service (AWS KMS)	2
AWS Lambda	17
Amazon Simple Storage Service (Amazon S3)	2
Amazon Simple Notification Service (Amazon SNS)	2
Amazon Simple Queue Service (Amazon SQS)	2
AWS Systems Manager	62
AWS Step Functions	4

> **Important**
>
> Les ressources supprimées par les étapes de ce modèle ne peuvent pas être récupérées. Avant de suivre ces étapes, vérifiez soigneusement les noms des ressources et assurez-vous qu'ils ont été créés par AFT.

Architecture

Le schéma suivant montre les composants AFT et le flux de travail de haut niveau. AFT met en place un pipeline Terraform qui vous aide à approvisionner et à personnaliser vos comptes. AWS Control Tower AFT suit un GitOps modèle pour automatiser les processus de provisionnement des comptes dans AWS Control Tower. Vous créez un fichier Terraform pour une demande de compte et vous le validez dans un référentiel, qui fournit les entrées qui déclenchent le flux de travail AFT pour le provisionnement du compte. Une fois le provisionnement du compte terminé, AFT peut exécuter automatiquement des étapes de personnalisation supplémentaires.

Dans cette architecture :

- AWS Control Tower Le compte de gestion Compte AWS est un compte dédié au AWS Control Tower service. Ceci est également généralement appelé compte AWS payeur ou compte AWS Organizations de gestion.
- Le compte AFT Management Compte AWS est dédié aux opérations de gestion AFT. Ce compte est différent du compte de gestion de votre organisation.
- Le compte Vended contient tous les composants et contrôles de base que vous avez sélectionnés. Compte AWS AFT AWS Control Tower vend un nouveau compte.

Pour plus d'informations sur cette architecture, voir Présentation de l'AFT dans l' AWS Control Tower atelier.

Outils

Services AWS

- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives.

- AWS Account Factory for Terraform (AFT) met en place un pipeline Terraform pour vous aider à approvisionner et à personnaliser les comptes et les ressources dans. AWS Control Tower
- AWS Organizationsvous permet de gérer et de gouverner votre environnement de manière centralisée à mesure que vous développez et faites évoluer vos AWS ressources. Organizations vous permet de créer des comptes et d'allouer des ressources, de regrouper des comptes pour organiser vos flux de travail, d'appliquer des politiques de gouvernance et de simplifier la facturation en utilisant un mode de paiement unique pour tous vos comptes.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser. Ce modèle nécessite des rôles et des autorisations IAM.

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources cloud et sur site.

Bonnes pratiques

- Pour AWS Control Tower, consultez la section Meilleures pratiques pour AWS Control Tower les administrateurs dans la AWS Control Tower documentation.
- Pour IAM, consultez la section Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Supprimer les ressources AFT dans le compte de gestion AFT

Tâche	Description	Compétences requises
Supprimez les ressources identifiées par la balise AFT.	1. Connectez-vous au compte de gestion AFT avec les autorisations d'adminis trateur. 2. Ouvrez la AWS Resource Groups console.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	3. Sélectionnez la région dans laquelle AWS Control Tower a été déployé. 4. Dans le volet de navigation, choisissez Tag Editor. 5. Pour les types de ressource s, sélectionnez Tous les types de ressources pris en charge. 6. Pour les balises, tapez managed_by comme clé de balise et AFT comme valeur de balise. 7. Choisissez Rechercher des ressources. Cette recherche affiche toutes les ressources créées par AFT. 8. Identifiez les noms des ressources et supprimez -les à l'aide des consoles de service correspon dantes. Par exemple, pour supprimer des ressource s du Parameter Store, procédez comme suit : a. Ouvrez la AWS Systems Manager console. b. Dans le panneau de navigation, choisissez Stockage de paramètres.	

Tâche	Description	Compétences requises
	c. Dans la zone de recherche, cliquez pour afficher le menu déroulant, choisisse z Name, choisissez equals, puis tapez /aft. d. Supprimez les paramètre s par lots de 10. (Il s'agit du nombre maximum que vous pouvez supprimer en même temps.) Pour la version 1.12.2 d'AFT, il y aura environ 62 ressources de magasin de paramètre s à supprimer. Tous les noms de paramètres commenceront par /aft. Cependant, toutes les ressources ne peuvent pas être identifiées par AWS Resource Groups. Dans les étapes suivantes, vous trouverez et supprimerez les ressources restantes.	

Tâche	Description	Compétences requises
Supprimez les rôles IAM.	1. Connectez-vous au compte de gestion AFT avec les autorisations d'adminis trateur. 2. Ouvrez la console IAM. 3. Supprimez ces rôles dans l'ordre indiqué (l'ordre est important en raison des dépendances) : • `aft-*` • `AWSAFTAdmin` • `AWSAFTExecution` • `AWSAFTService` • `codebuild_trigger_role`	Administrateur AWS, AWS DevOps, DevOps ingénieur
Supprimez le coffre AWS Backup de sauvegarde.	1. Ouvrez la AWS Backup console. 2. Localisez le coffre de sauvegarde nomméaws_backup_vault . 3. Vérifiez que le coffre-fort ne contient aucune sauvegarde active. 4. Supprimeraws_backup_vault .	Administrateur AWS, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Supprimez les CloudWatch ressources Amazon.	1. Ouvrez la CloudWatch console. 2. Supprimez les ressources suivantes dans l'ordre indiqué : a. Bus d'événements : Supprimer`aws_cloudwatch_event_bus` . b. Journaux : recherchez le préfixe AFT et supprimez tous les groupes de journaux associés. c. Définitions des requêtes : supprimez les requêtes suivantes : • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`	Administrateur AWS, AWS DevOps, DevOps ingénieur
Supprimez AWS KMS des ressources.	1. Passez à la région secondaire, qui sert de backend pour le suivi de l'état de l'AFT. 2. Ouvrez la AWS KMS console. 3. Supprimez l'alias nommé AFT.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Supprimer les ressources AFT dans le compte Log Archive

Tâche	Description	Compétences requises
Supprimez les compartiments S3.	1. Connectez-vous au compte Log Archive avec des autorisations d'administrateur. 2. Ouvrez la console Amazon S3. 3. Videz les compartiments suivants : • `aws-aft-logs-471112509802-us-east-1` • `aws-aft-s3-access-logs-471112509802-us-east-1` (Remplacez `111122223333` par votre identifiant de compte.) 4. Supprimez les deux compartiments.	Administrateur AWS, AWS DevOps, DevOps ingénieur
Supprimez les rôles IAM.	1. Ouvrez la console IAM. 2. Vérifiez que les rôles suivants ne sont utilisés par aucun service actif : • `AWSAFTService` • `AWSAFTExecution` 3. Supprimez les deux rôles.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Supprimer les ressources AFT dans le compte d'audit

Tâche	Description	Compétences requises
Supprimez les rôles IAM.	1. Connectez-vous au compte d'audit avec des autorisations d'administrateur. 2. Ouvrez la console IAM. 3. Vérifiez que les rôles suivants ne sont utilisés par aucun service actif : • `AWSAFTService` • `AWSAFTExecution` 4. Supprimez les deux rôles.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Supprimer les ressources AFT dans le compte AWS Control Tower de gestion

Tâche	Description	Compétences requises
Supprimez les rôles IAM.	1. Connectez-vous au compte de AWS Control Tower gestion avec des autorisations d'administrateur. 2. Ouvrez la console IAM. 3. Vérifiez que les rôles suivants ne sont utilisés par aucun service actif : • `AWSAFTService` • `AWSAFTExecution` • `aft-control-tower-events-rule` 4. Supprimez les trois rôles.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
Supprimez EventBridge les règles.	1. Ouvrez la EventBridge console Amazon. 2. Dans le volet de navigation de gauche, choisissez Rules (Règles). 3. Recherchez et sélectionnez la règle nommée`aft-capture-ct-events` . 4. Choisissez Supprimer et confirmez la suppression lorsque vous y êtes invité.	Administrateur AWS, AWS DevOps, DevOps ingénieur

Résolution des problèmes

Problème	Solution
Le détachement de la passerelle Internet a échoué.	Lorsque vous supprimez des ressources identifiées par la balise AFT, si vous rencontrez ce problème lorsque vous détachez ou supprimez la passerelle Internet, vous devez d'abord supprimer les points de terminaison VPC : 1. Connectez-vous au compte AFT Management, puis ouvrez la console Amazon VPC. 2. Dans le volet de navigation, dans la liste Filtrer par VPC, choisissez le VPC nommé. aft-management-vpc 3. Dans le volet de navigation, choisissez Points de terminaison. 4. Sélectionnez les points de terminaison associés au VPC. aft-management-vpc

Problème	Solution
	• Vérifiez la colonne VPC ID avant de la supprimer pour éviter de supprimer les mauvais points de terminaison. • Veillez à ne supprimer que les points de terminaison associés au VPC AFT. 5. Choisissez Actions, Delete VPC endpoints (Supprimer le point de terminaison d'un VPC). 6. Dans la boîte de dialogue de confirmat ion, tapez Supprimer, puis sélectionnez Supprimer. 7. Attendez que l'état du terminal passe à Supprimé. La suppression peut prendre quelques minutes.

Problème	Solution
Vous ne trouvez pas les CloudWatch requêtes spécifiées.	Si vous ne trouvez pas les CloudWatch requêtes créées par AFT, procédez comme suit : 1. Connectez-vous au compte AFT Management, puis ouvrez la CloudWatch console. 2. Dans le volet de navigation, sous Logs, sélectionnez Logs Insights. 3. Dans le coin supérieur droit, cliquez sur l'icône Requêtes enregistrées et exemples. Vous devriez maintenant être en mesure de voir les requêtes AFT. Pour une capture d'écran, consultez la section Informations supplémentaires. 4. Sélectionnez les requêtes suivantes, puis choisissez Actions, Supprimer pour les supprimer. • `Customization Logs by Account ID` • `Customization Logs by Customization Request ID`

Ressources connexes

- ARRIÈRE :
  - GitHub Référentiel
  - Atelier
  - Documentation
- AWS Control Tower documentation

Informations supplémentaires

Pour afficher les requêtes AFT sur le tableau de bord de CloudWatch Logs Insights, choisissez l'icône de requêtes enregistrées et d'exemples dans le coin supérieur droit, comme illustré dans la capture d'écran suivante :

Connectez-vous à une EC2 instance Amazon à l'aide du gestionnaire de session

Créée par Jason Cornick (AWS), Abhishek Bastikoppa (AWS) et Yaniv Ron (AWS)

Récapitulatif

Ce modèle décrit comment se connecter à une instance Amazon Elastic Compute Cloud (Amazon EC2) à l'aide du Session Manager, une fonctionnalité d'AWS Systems Manager. À l'aide de ce modèle, vous pouvez exécuter des commandes bash sur une EC2 instance via un navigateur Web. Le gestionnaire de session n'exige pas l'ouverture de ports entrants et n'exige pas d'adresses IP publiques pour les EC2 instances. En outre, il n'est plus nécessaire de gérer des hôtes bastions avec différentes clés Secure Shell (SSH). Vous pouvez régir l'accès à Session Manager à l'aide des politiques AWS Identity and Access Management (IAM) et configurer la journalisation, qui enregistre des informations importantes, telles que l'accès aux instances et les actions.

Dans ce modèle, vous configurez un rôle IAM et l'associez à une EC2 instance Linux que vous approvisionnez à l'aide d'une Amazon Machine Image (AMI). Vous configurez ensuite la connexion à Amazon CloudWatch Logs et utilisez le gestionnaire de session pour démarrer une session avec l'instance.

Bien que ce modèle se connecte à une EC2 instance Linux dans le cloud Amazon Web Services (AWS), vous pouvez utiliser cette approche pour utiliser le gestionnaire de session pour les connexions avec d'autres serveurs, tels que des serveurs sur site ou d'autres machines virtuelles.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Autorisations d'accès au nœud géré. Pour obtenir des instructions, consultez la section Contrôler l'accès des sessions utilisateur aux nœuds gérés.
- Points de terminaison VPC pour `ssm`, `ec2messages`, `ssmmessages` et. `s3` Pour obtenir des instructions, consultez la section Create VPC endpoints dans la documentation de Systems Manager.

Architecture

Pile technologique cible

- Gestionnaire de session
- Amazon EC2
- CloudWatch Journaux

Architecture cible

1. L'utilisateur authentifie son identité et ses informations d'identification via IAM.
2. L'utilisateur lance une session SSH via le gestionnaire de session et envoie des appels d'API à l' EC2 instance.
3. L'agent AWS Systems Manager SSM, qui est installé sur l' EC2 instance, se connecte au gestionnaire de session et exécute les commandes.
4. À des fins d'audit et de surveillance, le gestionnaire de session envoie les données de journalisation à CloudWatch Logs. Vous pouvez également envoyer les données du journal vers un compartiment Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez la section Journalisation des données de session à l'aide d'Amazon S3 (documentation Systems Manager).

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement. Ce modèle utilise une Amazon Machine Image (AMI) pour approvisionner une EC2 instance Linux.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Systems Manager vous aide à gérer vos applications et votre infrastructure exécutées dans le cloud AWS. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos ressources AWS en toute sécurité à grande échelle. Ce modèle utilise le Gestionnaire de session, une fonctionnalité de Systems Manager.

Bonnes pratiques

Nous vous recommandons d'en savoir plus sur le pilier de sécurité d'AWS Well-Architected Framework, d'explorer les options de chiffrement et d'appliquer les recommandations de sécurité dans la section Configuration du gestionnaire de session (documentation de Systems Manager).

Épopées

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez le rôle IAM.	Créez le rôle IAM pour l'agent SSM. Suivez les instructions de la section Création d'un rôle pour un service AWS (documentation IAM) et notez les points suivants : 1. Pour le service AWS, choisissez EC2. 2. Pour les politiques d'autorisation, choisissez `AmazonSSMManagedInstanceCore` . 3. Dans Nom du rôle, entrez `EC2_SSM_Role` .	Administrateur système AWS
Créez l' EC2 instance.	1. Créez l' EC2 instance. Suivez les instructions de la section Lancer une instance (EC2 documentation Amazon) et notez les points suivants : a. Dans la section Nom et balises, choisissez Ajouter des balises supplémentaires.	Administrateur système AWS

Tâche	Description	Compétences requises
	Dans Clé, entrez `Name`, et dans Valeur, entrez `Productio n_Server_One` . b. Choisissez une AMI Amazon Linux sur laquelle l'agent SSM est préinstallé. Pour une liste complète, voir AMIsavec l'agent SSM préinstallé (documentation Systems Manager). c. Dans la section Détails avancés, dans le profil d'instance IAM, choisisse z EC2_SSM_Role. 2. Ouvrez la console Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager/. 3. Dans le volet de navigation, choisissez Fleet Manager. 4. Vérifiez que l'instance apparaît dans la liste des nœuds gérés.	

Tâche	Description	Compétences requises
Configurez la journalisation.	1. Créez un groupe de CloudWatch journaux dans Logs. Suivez les instructions de la section Créer un groupe de CloudWatch journaux (documentation sur les journaux). Nommez le nouveau groupe de journaux`SessionManager` . 2. Configurez la journalisation pour le gestionnaire de session. Suivez les instructions de la section Journalisation des données de session à l'aide d'Amazon CloudWatch Logs (documentation Systems Manager) et notez les points suivants : a. Ne sélectionnez pas Autoriser uniquement les groupes de CloudWatch journaux chiffrés. b. Dans Choisissez un groupe de journaux dans la liste, sélectionnez SessionManager.	Administrateur système AWS

Connectez-vous à l'instance

Tâche	Description	Compétences requises
Connectez-vous à l' EC2 instance.	1. Démarrez une session dans la console Systems Manager. Pour obtenir des instructions, voir Démarrer une session (documentation de Systems Manager). Pour les instances Target, cliquez sur le bouton d'option situé à gauche de l'instance Production_Server_One. 2. Une fois la connexion établie, exécutez plusieurs commandes bash. 3. Dans la console Systems Manager, mettez fin à la session. Pour obtenir des instructions, reportez-vous à la section Fin d'une session (documentation de Systems Manager).	Administrateur système AWS
Validez la journalisation.	1. Dans CloudWatch Logs, ouvrez le flux de journaux pour le groupe de journaux. Pour obtenir des instructions, voir Afficher les données des CloudWatch journaux (documentation des journaux). 2. Dans les données du journal, vérifiez que les	Administrateur système AWS

Tâche	Description	Compétences requises
	commandes que vous avez exécutées dans l'article précédent sont répertoriées.	

Résolution des problèmes

Problème	Solution
Problèmes IAM	Pour obtenir de l'aide, consultez la section Résolution des problèmes (documentation IAM).

Ressources connexes

- Compléter les prérequis du gestionnaire de session (documentation de Systems Manager)
- Conception et mise en œuvre de la journalisation et de la surveillance avec Amazon CloudWatch (AWS Prescriptive Guidance)

Créez un pipeline dans les régions AWS qui ne prennent pas en charge AWS CodePipeline

Créée par Anand Krishna Varanasi (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

AWS CodePipeline est un service d'orchestration de livraison continue (CD) qui fait partie d'un ensemble d' DevOps outils d'Amazon Web Services (AWS). Il s'intègre à une grande variété de sources (telles que les systèmes de contrôle de version et les solutions de stockage), aux produits et services d'intégration continue (CI) d'AWS et de ses partenaires, ainsi qu'aux produits open source afin de fournir un service de end-to-end flux de travail pour des déploiements rapides d'applications et d'infrastructures.

Cependant, il CodePipeline n'est pas pris en charge dans toutes les régions AWS et il est utile de disposer d'un orchestrateur invisible qui connecte les CI/CD services. This pattern describes how to implement an end-to-end workflow pipeline in AWS Regions where CodePipeline isn’t yet supported by using AWS CI/CD services AWS tels qu'AWS CodeCommit CodeBuild, AWS et AWS CodeDeploy.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- CLI AWS Cloud Development Kit (AWS CDK) version 2.28 ou ultérieure

Architecture

Pile technologique cible

Le schéma suivant montre un pipeline créé dans une région qui ne le prend pas en charge CodePipeline, telle que la région Afrique (Le Cap). Un développeur envoie les fichiers de CodeDeploy configuration (également appelés scripts d'accroche du cycle de vie de déploiement) vers le référentiel Git hébergé par CodeCommit. (Voir le GitHub référentiel fourni avec ce modèle.) Une EventBridge règle Amazon est automatiquement initiée. CodeBuild

Les fichiers CodeDeploy de configuration sont extraits dans le CodeCommit cadre de l'étape source du pipeline et transférés vers CodeBuild.

Dans la phase suivante, CodeBuild exécute les tâches suivantes :

1. Télécharge le fichier TAR du code source de l'application. Vous pouvez configurer le nom de ce fichier à l'aide de Parameter Store, une fonctionnalité d'AWS Systems Manager.
2. Télécharge les fichiers CodeDeploy de configuration.
3. Crée une archive combinée du code source de l'application et des fichiers de CodeDeploy configuration spécifiques au type d'application.
4. Lance le CodeDeploy déploiement sur une instance Amazon Elastic Compute Cloud (Amazon EC2) à l'aide de l'archive combinée.

Outils

Services AWS

- AWS CodeBuild est un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS CodeDeploy automatise les déploiements sur Amazon EC2 ou sur site, les fonctions AWS Lambda ou les services Amazon Elastic Container Service (Amazon ECS).
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.

Code

Le code de ce modèle est disponible dans le référentiel GitHub CodePipeline Unsupported Regions.

Épopées

Configurez votre poste de travail de développeur

Tâche	Description	Compétences requises
Installez l'interface de ligne de commande AWS CDK.	Pour obtenir des instructions, consultez la documentation AWS CDK.	AWS DevOps
Installez un client Git.	Pour créer des validations, vous pouvez utiliser un client Git installé sur votre ordinateur local, puis transférer vos validations vers le CodeCommit référentiel. Pour effectuer la configuration CodeCommit avec votre client Git, consultez la CodeCommit documentation.	AWS DevOps
Installez NPM.	Installez le gestionnaire de packages npm. Pour plus d'informations, consultez la documentation npm.	AWS DevOps

Configuration du pipeline

Tâche	Description	Compétences requises
Clonez le référentiel de code.	Clonez le référentiel GitHub CodePipeline Unsupported Regions sur votre machine locale en exécutant la commande suivante.	DevOps ingénieur

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/invisible-codepipeline-unsupported-regions`	

Tâche	Description	Compétences requises
Définissez les paramètres dans cdk.json.	Ouvrez le `cdk.json` fichier et saisissez les valeurs des paramètres suivants : `"pipeline_account" :"XXXXXXXXXXXX", "pipeline_region":" us-west-2", "repo_name": "app-dev-repo", "ec2_tag_key": "test-vm", "configName" : "cbdeployconfig", "deploymentGroupName": "cbdeploygroup", "applicationName" : "cbdeployapplication", "projectName" : "CodeBuildProject"` où : • `pipeline_account` est le compte AWS sur lequel le pipeline sera construit. • `pipeline_region` est la région AWS dans laquelle le pipeline sera construit. • `repo_name` est le nom du CodeCommit dépôt. • `ec2_tag_key` est la balise attachée à l' EC2 instance sur laquelle vous souhaitez déployer le code.	AWS DevOps

Tâche	Description	Compétences requises
	• `configName` est le nom du fichier CodeDeploy de configuration. • `deploymentGroupNam e` est le nom du groupe CodeDeploy de déploieme nt. • `applicationName` est le nom de CodeDeploy l'application. • `projectName` est le nom CodeBuild du projet.	

Configurez la bibliothèque de constructions AWS CDK.	Dans le GitHub référentiel cloné, utilisez les commandes suivantes pour installer la bibliothèque de construct ions AWS CDK, créer votre application et synthétiser afin de générer le CloudFormation modèle AWS pour l'applica tion.
	`npm i aws-cdk-lib`
	`npm run build`
	`cdk synth`
		AWS DevOps

Déployez l'exemple d'applica tion AWS CDK.	Déployez le code en exécutant la commande suivante dans une région non prise en charge (telle que`af-south-1`). `cdk deploy`	AWS DevOps

Configurez le CodeCommit référentiel pour CodeDeploy

Tâche	Description	Compétences requises
Configurez le CI/CD pour l'application.	Clonez le CodeCommit référentiel que vous avez spécifié dans le `cdk.json` fichier (appelé `app-dev-repo` par défaut) pour configurer le pipeline CI/CD pour l'application. `git clone https://git-codecommit.us-west-2.amazonaws.com/v1/repos/app-dev-repo` où le nom du référentiel et la région dépendent des valeurs que vous avez fournies dans le `cdk.json` fichier.	AWS DevOps

Testez le pipeline

Tâche	Description	Compétences requises
Testez le pipeline à l'aide des instructions de déploiement.	Le `CodeDeploy_Files` dossier du référentiel GitHub CodePipeline Unsupported Regions contient des exemples de fichiers qui indiquent le déploiement CodeDeploy de l'application. Le `appspec.yml` fichier est un fichier CodeDeploy de configuration qui contient des crochets permettan	AWS DevOps

Tâche	Description	Compétences requises
	t de contrôler le flux de déploiement des applicati ons. Vous pouvez utiliser les fichiers d'exemple `index.html` , `start_ser ver.sh` `stop_server.sh` , et `install_dependenci es.sh` pour mettre à jour un site Web hébergé sur Apache. Ce sont des exemples : vous pouvez utiliser le code du GitHub référentiel pour déployer n'importe quel type d'application. Lorsque les fichiers sont transférés vers le CodeCommit référenti el, le pipeline invisible est lancé automatiquement. Pour obtenir les résultats du déploiement, vérifiez les résultats des différentes phases dans les CodeDeploy consoles CodeBuild et.	

Ressources connexes

- Mise en route (documentation AWS CDK)
- Présentation du Cloud Development Kit (CDK) (AWS Workshop Studio)
- Atelier AWS CDK

Personnalisez les noms de rôles par défaut en utilisant des AWS CDK aspects et des trappes d'échappement

Créée par SANDEEP SINGH (AWS) et James Jacob (AWS)

Récapitulatif

Ce modèle montre comment personnaliser les noms par défaut des rôles créés par AWS Cloud Development Kit (AWS CDK) des constructions. La personnalisation des noms de rôles est souvent nécessaire si votre organisation a des contraintes spécifiques basées sur des conventions de dénomination. Par exemple, votre organisation peut définir des limites d'autorisations AWS Identity and Access Management (IAM) ou des politiques de contrôle des services (SCPs) qui nécessitent un préfixe spécifique dans les noms de rôles. Dans de tels cas, les noms de rôle par défaut générés par AWS CDK les constructions peuvent ne pas respecter ces conventions et devront peut-être être modifiés. Ce modèle répond à ces exigences en utilisant des trappes d'évacuation et des aspects dans le AWS CDK. Vous utilisez des trappes d'échappement pour définir des noms de rôles personnalisés, et des aspects pour appliquer un nom personnalisé à tous les rôles, afin de garantir le respect des politiques et des contraintes de votre organisation.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Prérequis spécifiés dans la documentation AWS CDK

Limites

- Les aspects filtrent les ressources en fonction des types de ressources, de sorte que tous les rôles partagent le même préfixe. Si vous avez besoin de préfixes de rôle différents pour différents rôles, un filtrage supplémentaire basé sur d'autres propriétés est nécessaire. Par exemple, pour attribuer différents préfixes aux rôles associés à des AWS Lambda fonctions, vous pouvez filtrer en fonction d'attributs ou de balises de rôle spécifiques, et appliquer un préfixe pour les rôles liés à Lambda et un autre préfixe pour les autres rôles.
- Les noms de rôle IAM ont une longueur maximale de 64 caractères. Les noms de rôles modifiés doivent donc être rognés pour respecter cette restriction.

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Pile technologique cible

- AWS CDK
- AWS CloudFormation

Architecture cible

- Une AWS CDK application se compose d'une ou de plusieurs AWS CloudFormation piles, qui sont synthétisées et déployées pour gérer les AWS ressources.
- Pour modifier une propriété d'une ressource AWS CDK gérée qui n'est pas exposée par une construction de couche 2 (L2), vous utilisez une trappe d'échappement pour remplacer les CloudFormation propriétés sous-jacentes (dans ce cas, le nom du rôle) et un aspect pour appliquer le rôle à toutes les ressources de l' AWS CDK application pendant le processus de synthèse de la pile. AWS CDK

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS CDK L'interface de ligne de commande (AWS CDK CLI) (également appelée boîte à AWS CDK outils) est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre AWS CDK application. La `cdk` commande CLI est le principal outil d'interaction avec votre AWS CDK application. Il exécute votre application, interroge le modèle d'application que vous avez défini, produit et déploie les CloudFormation modèles générés par le. AWS CDK
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.

Référentiel de code

Le code source et les modèles de ce modèle sont disponibles dans le référentiel GitHub CDK Aspects Override.

Bonnes pratiques

Consultez les meilleures pratiques d'utilisation de l' AWS CDK in pour TypeScript créer des projets IaC sur le site Web AWS Prescriptive Guidance.

Épopées

Installation de la AWS CDK CLI

Tâche	Description	Compétences requises
Installez la AWS CDK CLI.	Pour installer la AWS CDK CLI globalement, exécutez la commande suivante : `npm install -g aws-cdk`	AWS DevOps
Vérifiez la version.	Exécutez la commande : `cdk --version` Vérifiez que vous utilisez la version 2 de la AWS CDK CLI.	AWS DevOps
Démarrez l' AWS CDK environnement.	Avant de déployer les AWS CloudFormation modèles, préparez le compte et le compte Région AWS que vous souhaitez utiliser. Exécutez la commande : `cdk bootstrap <account>/<Region>`	AWS DevOps

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section AWS CDK bootstrapping dans la AWS documentation.	

Déployez l' AWS CDK application pour démontrer l'utilisation des aspects

Tâche	Description	Compétences requises

Configurez le projet.	1. Clonez le GitHub dépôt de ce modèle sur votre ordinateur local :
	`git clone https://github.com/aws-samples/cdk-aspects-override`
	2. Accédez au répertoire du projet sur votre ordinateur local.
	3. Installez les dépendances du projet :
	`npm ci`
		AWS DevOps

Déployez des piles avec des noms de rôle par défaut attribués par le AWS CDK.	Déployez deux CloudFormation piles (`ExampleStack1` et`ExampleStack2`) contenant les fonctions Lambda et leurs rôles associés :	AWS DevOps

Tâche	Description	Compétences requises
	`npm run deploy:ExampleAppWithoutAspects` Le code ne transmet pas explicitement les propriétés des rôles. Les noms des rôles seront donc construits par le AWS CDK. Pour un exemple de sortie, consultez la section Informations supplémentaires.	

Tâche	Description	Compétences requises

Déployez des piles comportant des aspects.	Au cours de cette étape, vous appliquez un aspect qui applique une convention de nom de rôle en ajoutant un préfixe à tous les rôles IAM déployés dans le projet. AWS CDK L'aspect est défini dans le `lib/aspects.ts` fichier. L'aspect utilise une trappe d'échappement pour remplacer le nom du rôle en ajoutant un préfixe. L'aspect est appliqué aux piles du `bin/app-with-aspects.ts` fichier. Le préfixe du nom de rôle utilisé dans cet exemple est`dev-unicorn` .
	
	1. Modifiez le fichier `bin/app-with-aspects.ts` .
	2. Dans le fichier, mettez à jour la variable `ROLE_NAME_PREFIX` avec le préfixe `dev-unicorn` :
	
	`const app = new cdk.App();`
	
	`// Define a prefix for the role names`
	`const ROLE_NAME_PREFIX = 'dev-unicorn';`
		AWS DevOps

Tâche	Description	Compétences requises

	``
	// Instantiate the
	 RoleNamingConventi
	onAspect with the
	 desired prefix
	const roleNamin
	gConventionAspect
	 = new RoleNamin
	gConventionAspect(
	ROLE_NAME_PREFIX);
	``
	3. Déployez l' AWS CDK application avec les aspects suivants :
	``
	npm run deploy:Ex
	ampleAppWithAspects
	``
	Pour un exemple de sortie, consultez la section Informations supplémentaires.	

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez vos AWS CloudFormation piles.	Une fois que vous avez fini d'utiliser ce modèle, exécutez la commande suivante pour nettoyer les ressources afin d'éviter des coûts supplémentaires : ``` cdk destroy --all -f && cdk --app npx ts-node bin/app-with-aspec ```	AWS DevOps

Tâche	Description	Compétences requises
	`ts.ts' destroy --all -f`	

Résolution des problèmes

Problème	Solution
Vous rencontrez des problèmes lors de l'utilisation du AWS CDK.	Consultez la section Résolution AWS CDK des problèmes courants dans la AWS CDK documentation.

Ressources connexes

- AWS Cloud Development Kit (AWS CDK)
- AWS CDK documentation
- AWS CDK sur GitHub
- Trappes d'évacuation
- Aspects et AWS CDK

Informations supplémentaires

Noms de rôles créés par AWS CloudFormation Without Aspects

```
Outputs:
ExampleStack1WithoutAspects.Function1RoleName = example-stack1-without-as-
Function1LambdaFunctionSe-y7FYTY6FXJXA
ExampleStack1WithoutAspects.Function2RoleName = example-stack1-without-as-
Function2LambdaFunctionSe-dDZV4rkWqWnI
...

Outputs:
ExampleStack2WithoutAspects.Function3RoleName = example-stack2-without-as-
Function3LambdaFunctionSe-ygMv49iTyMq0
```

Noms de rôles créés par AWS CloudFormation with aspects

```
Outputs:
ExampleStack1WithAspects.Function1RoleName = dev-unicorn-
Function1LambdaFunctionServiceRole783660DC
ExampleStack1WithAspects.Function2RoleName = dev-unicorn-
Function2LambdaFunctionServiceRole2C391181
...

Outputs:
ExampleStack2WithAspects.Function3RoleName = dev-unicorn-
Function3LambdaFunctionServiceRole4CAA721C
```

Déployez un cluster Cassandra sur Amazon EC2 avec une statique privée IPs pour éviter le rééquilibrage

Créée par Dipin Jain (AWS)

Récapitulatif

L'adresse IP privée d'une instance Amazon Elastic Compute Cloud (Amazon EC2) est conservée tout au long de son cycle de vie. Cependant, l'adresse IP privée peut changer lors d'une panne système planifiée ou imprévue, par exemple lors d'une mise à niveau d'Amazon Machine Image (AMI). Dans certains scénarios, la conservation d'une adresse IP statique privée peut améliorer les performances et le temps de restauration des charges de travail. Par exemple, l'utilisation d'une adresse IP statique pour un nœud initial d'Apache Cassandra empêche le cluster de subir une surcharge de rééquilibrage.

Ce modèle décrit comment associer une interface Elastic Network secondaire aux EC2 instances afin de maintenir l'adresse IP statique pendant le réhébergement. Le modèle se concentre sur les clusters Cassandra, mais vous pouvez utiliser cette implémentation pour toute architecture bénéficiant d'une statique IPs privée.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Service (AWS) actif

Versions du produit

- DataStax version 5.11.1
- Système d'exploitation : Ubuntu 16.04.6 LTS

Architecture

Architecture de la source

La source peut être un cluster Cassandra sur une machine virtuelle (VM) sur site ou sur des EC2 instances du cloud AWS. Le schéma suivant illustre le second scénario. Cet exemple inclut quatre nœuds de cluster : trois nœuds de départ et un nœud de gestion. Dans l'architecture source, une seule interface réseau est attachée à chaque nœud.

Architecture cible

Le cluster de destination est hébergé sur EC2 des instances dotées d'une interface Elastic Network secondaire attachée à chaque nœud, comme illustré dans le schéma suivant.

Automatisation et mise à l'échelle

Vous pouvez également automatiser l'attachement d'une deuxième interface Elastic network à un groupe EC2 Auto Scaling, comme décrit dans une vidéo du centre de connaissances AWS.

Épopées

Configurer un cluster Cassandra sur Amazon EC2

Tâche	Description	Compétences requises
Lancez EC2 des nœuds pour héberger un cluster Cassandra.	Sur la EC2 console Amazon, lancez quatre EC2 instances pour vos nœuds Ubuntu dans votre compte AWS. Trois nœuds (de départ) sont utilisés pour le cluster Cassandra, et le quatrième nœud fait office de nœud de gestion de cluster sur lequel vous installerez DataStax Enterprise (DSE) OpsCenter. Pour obtenir des instructions, consultez la EC2 documentation Amazon.	Ingénieur cloud
Confirmez les communications entre les nœuds.	Assurez-vous que les quatre nœuds peuvent communiquer entre eux via les ports de gestion de base de données et de cluster.	Ingénieur réseau

Tâche	Description	Compétences requises
Installez DSE OpsCenter sur le nœud de gestion.	Installez DSE OpsCenter 6.1 à partir du paquet Debian sur le nœud de gestion. Pour obtenir des instructions, consultez la DataStax documentation.	DBA

Tâche	Description	Compétences requises
Créez une interface réseau secondaire.	Cassandra génère un identifiant unique universel (UUID) pour chaque nœud en fonction de l'adresse IP de l' EC2 instance associée à ce nœud. Cet UUID est utilisé pour distribuer des nœuds virtuels (vnodes) sur le ring. Lorsque Cassandra est déployée sur EC2 des instances, les adresses IP sont attribuées automatiquement aux instances au fur et à mesure de leur création. En cas de panne planifiée ou imprévue, l'adresse IP de la nouvelle EC2 instance change, la distribution des données change et l'ensemble de l'anneau doit être rééquilibré. Cela n'est pas souhaitable. Pour conserver l'adresse IP attribuée, utilisez une interface Elastic network secondaire dotée d'une adresse IP fixe. 1. Sur la EC2 console Amazon, choisissez Network Interfaces, Create network interface. 2. Pour Sous-réseau, sélectionnez le sous-réseau dans lequel vous avez créé l' EC2 instance.	Ingénieur cloud

Tâche	Description	Compétences requises
	3. Pour IPv4 Adresse privée, choisissez Attribuer automatiquement. 4. Pour les groupes de sécurité, sélectionnez un groupe de sécurité, puis choisissez Créer une interface réseau. Pour plus d'informations sur la création d'une interface réseau, consultez la EC2 documentation Amazon.	
Connectez l'interface réseau secondaire aux nœuds du cluster.	1. Sur la EC2 console Amazon, sélectionnez Instances. 2. Cochez la case correspon dant à l' EC2 instance que vous avez créée précédemment. 3. Sélectionnez Actions, Mise en réseau, Attacher l’interfa ce réseau. 4. Sélectionnez l'interface réseau que vous avez créée à l'étape précédente, puis choisissez Attacher. Pour plus d'informations sur la connexion d'une interface réseau, consultez la EC2 documentation Amazon.	Ingénieur cloud

Tâche	Description	Compétences requises
Ajoutez des itinéraires dans Amazon EC2 pour résoudre le problème du routage asymétrique.	Lorsque vous connectez la deuxième interface réseau, le réseau effectuera très probablement un routage asymétrique. Pour éviter cela, vous pouvez ajouter des itinéraires pour les nouvelles interfaces réseau. Pour une explication détaillée du routage asymétrique et pour y remédier, consultez la vidéo du centre de connaissances AWS intitulée Overcoming Asymmetric Routing on Multi-Home Servers (article de Patrick dans le Linux Journal McManus, 5 avril 2004).	Ingénieur réseau
Mettez à jour les entrées DNS pour qu'elles pointent vers l'adresse IP de l'interface réseau secondaire.	Pointez le nom de domaine complet (FQDN) du nœud vers l'adresse IP de l'interface réseau secondaire.	Ingénieur réseau
Installez et configurez le cluster Cassandra à l'aide de OpsCenter DSE.	Lorsque les nœuds du cluster sont prêts avec les interfaces réseau secondaires, vous pouvez installer et configurer le cluster Cassandra.	DBA

Restaurer le cluster en cas de défaillance d'un nœud

Tâche	Description	Compétences requises
Créez une AMI pour le nœud de départ du cluster.	Effectuez une sauvegarde des nœuds afin de pouvoir les restaurer avec des fichiers binaires de base de données en cas de défaillance du nœud. Pour obtenir des instructions, consultez la section Créer une AMI dans la EC2 documentation Amazon.	Administrateur des sauvegardes
Restaurez après une défaillance du nœud.	Remplacez le nœud défaillant par une nouvelle EC2 instance lancée depuis l'AMI et attachez l'interface réseau secondaire du nœud défaillant.	Administrateur des sauvegardes
Vérifiez que le cluster Cassandra est sain.	Lorsque le nœud de remplacement est actif, vérifiez l'état du cluster dans DSE OpsCenter.	DBA

Ressources connexes

- Installation de DSE OpsCenter 6.1 à partir du paquet Debian (DataStax documentation)
- Comment faire fonctionner une interface réseau secondaire dans une EC2 instance Ubuntu (vidéo du centre de connaissances AWS)
- Bonnes pratiques pour exécuter Apache Cassandra sur Amazon EC2 (article de blog AWS)

Étendez votre accès VRFs à AWS en utilisant AWS Transit Gateway Connect

Créée par Adam Till (AWS), Yashar Araghi (AWS), Vikas Dewangan (AWS) et Mohideen (AWS) HajaMohideen

Récapitulatif

Le routage et le transfert virtuels (VRF) sont une fonctionnalité des réseaux traditionnels. Il utilise des domaines de routage logiques isolés, sous forme de tables de routage, pour séparer le trafic réseau au sein d'une même infrastructure physique. Vous pouvez configurer AWS Transit Gateway pour prendre en charge l'isolation VRF lorsque vous connectez votre réseau sur site à AWS. Ce modèle utilise un exemple d'architecture pour se connecter sur site VRFs à différentes tables de routage de passerelles de transit.

Ce modèle utilise des interfaces virtuelles de transit (VIFs) dans AWS Direct Connect et des pièces jointes Connect de la passerelle de transit pour étendre le VRFs. Un VIF de transit est utilisé pour accéder à une ou plusieurs passerelles de transit Amazon VPC associées aux passerelles Direct Connect. Une pièce jointe Connect connecte une passerelle de transit à un dispositif virtuel tiers exécuté dans un VPC. Une pièce jointe Connect de passerelle de transit prend en charge le protocole de tunnel GRE (Generic Routing Encapsulation) pour des performances élevées, et le protocole BGP (Border Gateway Protocol) pour le routage dynamique.

L'approche décrite dans ce modèle présente les avantages suivants :

- Grâce à Transit Gateway Connect, vous pouvez annoncer jusqu'à 1 000 itinéraires à l'homologue Transit Gateway Connect et recevoir jusqu'à 5 000 itinéraires de ce dernier. L'utilisation de la fonctionnalité Direct Connect transit VIF sans Transit Gateway Connect est limitée à 20 préfixes par passerelle de transit.
- Vous pouvez maintenir l'isolation du trafic et utiliser Transit Gateway Connect pour fournir des services hébergés sur AWS, quels que soient les schémas d'adresses IP utilisés par vos clients.
- Le trafic VRF n'a pas besoin de traverser une interface virtuelle publique. Cela facilite le respect des exigences de conformité et de sécurité dans de nombreuses entreprises.
- Chaque tunnel GRE prend en charge jusqu'à 5 Gbit/s, et vous pouvez avoir jusqu'à quatre tunnels GRE par pièce jointe Connect de passerelle de transit. Cela est plus rapide que de nombreux autres types de connexion, tels que les connexions Site-to-Site VPN AWS qui prennent en charge jusqu'à 1,25 Gbit/s.

Conditions préalables et limitations

Prérequis

- Les comptes AWS requis ont été créés (voir l'architecture pour plus de détails)
- Autorisations permettant d'assumer un rôle AWS Identity and Access Management (IAM) dans chaque compte.
- Les rôles IAM de chaque compte doivent être autorisés à fournir des ressources AWS Transit Gateway et AWS Direct Connect. Pour plus d'informations, consultez Authentification et contrôle d'accès pour vos passerelles de transport et gestion des identités et des accès pour Direct Connect.
- Les connexions Direct Connect ont été créées avec succès. Pour plus d'informations, voir Création d'une connexion à l'aide de l'assistant de connexion.

Limites

- Il existe des limites pour les pièces jointes des passerelles de VPCs transit aux comptes de production, d'assurance qualité et de développement. Pour plus d'informations, consultez la section Pièces jointes d'une passerelle de transit à un VPC.
- Il existe des restrictions concernant la création et l'utilisation des passerelles Direct Connect. Pour plus d'informations, consultez la section Quotas AWS Direct Connect.

Architecture

Architecture cible

L'exemple d'architecture suivant fournit une solution réutilisable pour déployer le transport en commun VIFs avec les pièces jointes Connect de la passerelle de transit. Cette architecture assure la résilience en utilisant plusieurs emplacements Direct Connect. Pour plus d'informations, consultez la section Résilience maximale dans la documentation de Direct Connect. La production, l'assurance qualité et le développement du VRFs réseau sur site sont étendus à AWS et isolés à l'aide de tables de routage dédiées.

Dans l'environnement AWS, deux comptes sont dédiés à l'extension VRFs : un compte Direct Connect et un compte de hub réseau. Le compte Direct Connect contient la connexion et le transit VIFs pour chaque routeur. Vous créez le transit VIFs à partir du compte Direct Connect, mais vous

le déployez sur le compte du hub réseau afin de pouvoir l'associer à la passerelle Direct Connect dans le compte du hub réseau. Le compte du hub réseau contient la passerelle Direct Connect et la passerelle de transit. Les ressources AWS sont connectées comme suit :

1. VIFs Connectez les routeurs des sites Direct Connect à AWS Direct Connect dans le compte Direct Connect.
2. Un VIF de transit connecte Direct Connect à la passerelle Direct Connect dans le compte du hub réseau.
3. Une association de passerelle de transit connecte la passerelle Direct Connect à la passerelle de transit dans le compte du hub réseau.
4. Les pièces jointes Connect connectent la passerelle de transit VPCs aux comptes de production, d'assurance qualité et de développement.

Architecture Transit VIF

Le schéma suivant montre les détails de configuration du transit VIFs. Cet exemple d'architecture utilise un VLAN pour la source du tunnel, mais vous pouvez également utiliser un loopback.

Vous trouverez ci-dessous les détails de configuration, tels que les numéros de système autonomes (ASNs), pour le transit VIFs.

Ressource	Élément	Detail
routeur-01	ASN	65534
routeur-02	ASN	65534
routeur-03	ASN	65534
routeur-04	ASN	65534
Passerelle Direct Connect	ASN	64601
Passerelle de transit	ASN	64600
	Bloc d'adresse CIDR	10,10,254,0/24

Architecture Connect de Transit Gateway

Le diagramme et les tableaux suivants décrivent comment configurer un seul VRF via une pièce jointe Connect de passerelle de transit. En outre VRFs, attribuez des adresses IP GRE uniques à un tunnel IDs, à une passerelle de transit et à un BGP dans des blocs CIDR. L'adresse IP GRE de l'homologue correspond à l'adresse IP de l'homologue du routeur indiquée dans le VIF de transit.

Le tableau suivant contient les détails de configuration du routeur.

Routeur	Tunnel	Adresse IP	Source	Destination
routeur-01	Tunnel 1	169,254,101,17	VLAN 60	10,10,254,1
			169,254,100,1	
routeur-02	Tunnel 11	169,254,101,81	VLAN 61	10,10.254,11
			169,254,100,5	
routeur-03	Tunnel 21	169,254,101,145	VLAN 62	10,10.254,21
			169,254,100,9	
routeur-04	Tunnel 31	169,254,101,209	VLAN 63	10,10.254,31
			169,254,100,13	

Le tableau suivant contient les détails de configuration de la passerelle de transit.

Tunnel	Adresse IP GRE de la passerelle de transit	Adresse IP GRE homologue	BGP à l'intérieur de blocs CIDR
Tunnel 1	10,10,254,1	VLAN 60	169,254,106,16/29
		169,254,100,1	
Tunnel 11	10,10.254,11	VLAN 61	169,254,101,80/29
		169,254,100,5	

Tunnel 21	10,10.254,21	VLAN 62 169,254,100,9	169,254,101,144/29
Tunnel 31	10,10.254,31	VLAN 63 169,254,100,13	169,254,101,208/29

Déploiement

La section Epics décrit comment déployer un exemple de configuration pour un seul VRF sur plusieurs routeurs clients. Une fois les étapes 1 à 5 terminées, vous pouvez créer de nouvelles pièces jointes Connect pour la passerelle de transit en suivant les étapes 6 à 7 pour chaque nouveau VRF que vous étendez à AWS :

1. Créez la passerelle de transit.
2. Créez une table de routage Transit Gateway pour chaque VRF.
3. Créez les interfaces virtuelles de transport en commun.
4. Créez la passerelle Direct Connect.
5. Créez l'interface virtuelle de la passerelle Direct Connect et les associations de passerelle avec les préfixes autorisés.
6. Créez la pièce jointe Connect pour la passerelle de transit.
7. Créez les homologues de Transit Gateway Connect.
8. Associez la pièce jointe Connect de la passerelle de transit à la table de routage.
9. Annoncez les itinéraires aux routeurs.

Outils

Services AWS

- AWS Direct Connect relie votre réseau interne à un emplacement Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les services AWS publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- AWS Transit Gateway est un hub central qui connecte des clouds privés virtuels (VPCs) et des réseaux sur site.

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Épopées

Planifier l'architecture

Tâche	Description	Compétences requises
Créez des diagrammes d'architecture personnalisés.	1. Dans la section Pièces jointes, téléchargez le modèle de diagramme. 2. Ouvrez le schéma ci-joint dans Microsoft Office PowerPoint. 3. Sur la diapositive de présentation de l'architecture, personnalisez le schéma d'architecture pour votre environnement. Identifiez les locaux VRFs qui doivent être étendus à votre environnement AWS. 4. Sur la diapositive Transit VIF, personnalisez le schéma d'architecture. Identifiez les numéros AS des routeurs, de la passerelle Direct Connect et de la passerelle de transit. Identifiez les adresses IP à chaque extrémité du VIF de transit.	Architecte cloud, administrateur réseau

Tâche	Description	Compétences requises
	5. Sur la diapositive Transit Gateway Connect, personnalisez un schéma d'architecture pour chaque VRF. Identifiez toutes les adresses IP requises pour configurer les routeurs et les homologues de Transit Gateway Connect.	

Création des ressources Transit Gateway

Tâche	Description	Compétences requises
Créez la passerelle de transit.	1. Connectez-vous au compte du hub réseau. 2. Suivez les instructions de la section Créer une passerelle de transit. Notez ce qui suit pour ce modèle : • Pour le numéro de système autonome (ASN) côté Amazon, entrez un ASN unique. Dans le cadre de cet exemple, l'ASN est`64600`. • Sélectionnez Support DNS. • Pour cet exemple d'architecture, la prise en charge du VPN ECMP, l'association de tables de routage par défaut, la	Administrateur réseau, architecte cloud

Tâche	Description	Compétences requises
	prorogation de la table de routage par défaut et la prise en charge de la multidiffusion ne sont pas requises. • Pour les blocs CIDR de passerelle de transit, entrez les blocs IPv4 CIDR de votre passerelle de transit. Aux fins de cet exemple, le bloc CIDR est`10.100.254.0/24` .	
Créez la table de routage de la passerelle de transit.	Suivez les instructions de la section Créer une table de routage pour une passerelle de transit. Notez ce qui suit pour ce modèle : • Dans le champ Name tag, donnez un nom à la table de routage de la passerelle de transit. Nous vous recommandons d'utiliser un nom correspondant au VRF, tel que`routetable-dev-vrf` . • Pour Transit gateway ID, choisissez la passerelle de transit que vous avez créée précédemment.	Architecte cloud, administrateur réseau

Création des interfaces virtuelles de transport

Tâche	Description	Compétences requises
Créez les interfaces virtuelles de transport en commun.	1. Connectez-vous au compte Direct Connect. 2. Suivez les instructions de la section Création d'une interface virtuelle de transit vers la passerelle Direct Connect. Notez ce qui suit pour ce modèle : • Dans Nom de l'interface virtuelle, entrez le nom du VIF de transit. Nous vous recommandons d'utiliser un nom correspondant au routeur, tel que `transit-vif-router01` . • Pour Connexion, sélectionnez le routeur, tel que `router-01` . • Pour le propriétaire de l'interface virtuelle, entrez l'ID du compte du hub réseau. Pour obtenir des instructions, consultez Afficher l'identifiant de votre compte AWS. • Pour la passerelle Direct Connect, ne faites aucune sélection. Vous connectez la passerelle Direct Connect lors d'une étape suivante.	Architecte cloud, administrateur réseau

Tâche	Description	Compétences requises

	• Pour le VLAN, entrez le VLAN du routeur, par exemple. `60`
	• Pour l'ASN BGP, entrez l'ASN du routeur, par exemple. `65534`
	• Sous Additional Settings (Paramètres supplémentaires), procédez comme suit :
	  • Sélectionnez IPv4.
	  • Pour l'adresse IP de l'homologue de votre routeur, entrez l'adresse IP de l'homologue du routeur, telle que`169.254.100.1` .
	  • Pour l'adresse IP homologue du routeur Amazon, entrez l'adresse IP homologue du routeur Amazon, par exemple`169.254.100.2` .
	  • Pour la clé d'authentification BGP, un mot de passe est requis. Si ce champ est laissé vide, AWS crée une clé qui n'est accessible que dans ce compte.	

Tâche	Description	Compétences requises
	3. Répétez ces instructions pour créer tous les transits VIFs pour le VRF.	

Création des ressources Direct Connect

Tâche	Description	Compétences requises
Créez une passerelle Direct Connect.	1. Connectez-vous au compte du hub réseau. 2. Suivez les instructions de la section Création d'une passerelle Direct Connect. Notez ce qui suit pour ce modèle : • Pour l'ASN côté Amazon, entrez l'ASN de la passerelle Direct Connect, tel que. `64601` • Ne choisissez pas de passerelle privée virtuelle .	Architecte cloud, administrateur réseau
Connectez la passerelle Direct Connect au transit VIFs.	1. Dans le compte du hub réseau, ouvrez la console AWS Direct Connect à l'adresse https://console.aws.amazon.com/directconnect/v2/. 2. Dans le volet de navigation, sélectionnez Interfaces virtuelles.	Architecte cloud, administrateur réseau

Tâche	Description	Compétences requises
	3. Sélectionnez un nouveau VIF de transit, puis choisissez Accepter. 4. Choisissez la passerelle Direct Connect que vous avez créée. 5. Répétez ces instructions pour chaque VIF de transit.	
Créez les associations de passerelle Direct Connect avec les préfixes autorisés.	Dans le compte du hub réseau, suivez les instructions de la section Pour associer une passerelle de transit. Notez ce qui suit pour ce modèle : • Pour les passerelles, choisissez la passerelle de transit que vous avez créée précédemment. • Pour les préfixes autorisés, entrez le bloc CIDR attribué à la passerelle de transit, tel que. **`10.100.254.0/24`** La création de cette association crée automatiquement une pièce jointe Transit Gateway dotée d'un type de ressource Direct Connect Gateway. Il n'est pas nécessaire que cette pièce jointe soit associée à une table de routage de passerelle de transit.	Architecte cloud, administrateur réseau

Tâche	Description	Compétences requises
Créez la pièce jointe Connect pour la passerelle de transit.	1. Dans le compte du hub réseau, ouvrez la console Amazon VPC à l'adresse. https://console.aws.amazon.com/vpc/ 2. Dans le volet de navigation, choisissez Attachements de la passerelle de transit. 3. Choisissez Create transit gateway attachment (Créer un attachement de la passerelle de attachement de la passerelle de transit). 4. Dans le champ Name tag, entrez le nom de la pièce jointe. Nous vous recommandons d'utiliser un nom correspondant au VRF, tel que`PROD-VRF`. 5. Pour Transit gateway ID, choisissez la passerelle de transit que vous avez créée précédemment. 6. Pour Attachment type (Type d'attachement), choisissez Connect. 7. Pour Transport Attachment ID, choisissez la passerelle Direct Connect que vous avez créée précédemment. 8. Choisissez Create transit gateway attachment (Créer	Architecte cloud, administrateur réseau

Tâche	Description	Compétences requises
	un attachement de la passerelle de transit). 9. Répétez cette étape pour chaque VRF que vous étendez.	

Tâche	Description	Compétences requises
Créez les homologues de Transit Gateway Connect.	1. Dans le compte du hub réseau, suivez les instructions de la section Create a Transit Gateway Connect peer (tunnel GRE). Notez ce qui suit pour ce modèle : • Dans le champ Name tag, entrez le nom de l'homologue Transit Gateway Connect. Nous vous recommandons d'utiliser un nom correspondant au routeur, tel que `connectpeer-router01` . • Pour l'adresse GRE de la passerelle de transit, entrez l'adresse IP attribuée à partir du bloc CIDR de la passerelle de transit, telle que `10.100.254.1` . • Pour l'adresse GRE homologue, entrez l'adresse IP attribuée au VLAN créé sur le routeur pour le VIF de transit, telle que `169.254.100.1` . À condition qu'AWS puisse accéder à l'adresse IP, vous pouvez utiliser n'importe quelle interface, telle que VLAN ou Loopback,	

Tâche	Description	Compétences requises
	pour l'adresse GRE homologue. • Pour les blocs BGP Inside CIDR (IPv4), entrez l'adresse IP du bloc BGP Inside CIDR, telle que. `169.254.101.16/29` • Pour l'ASN homologue, entrez l'ASN du routeur, par exemple. `65534` 2. Répétez ces instructions pour créer un tunnel GRE pour chaque routeur.	

Annoncer les itinéraires aux routeurs

Tâche	Description	Compétences requises
Faites de la publicité pour les itinéraires.	Associez la nouvelle pièce jointe Connect de la passerelle de transit à la table de routage que vous avez créée précédemment pour ce VRF. Par exemple, associez la pièce jointe Connect de la passerelle de transit de production à la table de `Production-VRF` routage. Créez un itinéraire statique pour le préfixe annoncé aux routeurs.	Administrateur réseau, architecte cloud

Tâche	Description	Compétences requises
	1. Connectez-vous au compte du hub réseau. 2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/. 3. Dans le volet de navigation, sous Transit Gateways, choisissez Transit gateway route tables. 4. Sélectionnez la table de routage `Production-VRF`. 5. Dans le menu Actions, choisissez Créer un itinéraire statique. 6. Pour le CIDR, entrez le bloc CIDR pour l'itinéraire annoncé vers la pièce jointe de la passerelle de transit dans le VPC cible, tel que. `10.100.1.0/24` 7. Pour Choisir une pièce jointe, choisissez la pièce jointe Connect appropriée pour la passerelle de transport en commun. 8. Choisissez Create static route (Créer un acheminement statique).	

Ressources connexes

Documentation AWS

- Documentation Direct Connect
  - Utilisation des passerelles Direct Connect
  - Associations de passerelles de transit
  - Interfaces virtuelles AWS Direct Connect
- Documentation sur Transit Gateway
  - Travailler avec les passerelles de transport en commun
  - Pièces jointes d'une passerelle de transit à une passerelle Direct Connect
  - Pièces jointes Transit Gateway Connect et homologues de Transit Gateway Connect
  - Création d'une pièce jointe Connect pour une passerelle de transit

Articles de blog AWS

- Segmentation des réseaux hybrides avec AWS Transit Gateway connect
- Utilisation d'AWS Transit Gateway connect pour étendre VRFs et augmenter la publicité sur les préfixes IP

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Recevez des notifications Amazon SNS lorsque l'état clé d'une clé AWS KMS change

Créée par Shubham Harsora (AWS), Aromal Raj Jayarajan (AWS) et Navdeep Pareek (AWS)

Récapitulatif

Les données et métadonnées associées à une clé AWS Key Management Service (AWS KMS) sont perdues lorsque cette clé est supprimée. La suppression est irréversible et vous ne pouvez pas récupérer les données perdues (y compris les données cryptées). Vous pouvez éviter les pertes de données en configurant un système de notification pour vous avertir des modifications de statut des principaux états de vos clés AWS KMS.

Ce modèle vous montre comment surveiller les modifications de statut des clés AWS KMS en utilisant Amazon EventBridge et Amazon Simple Notification Service (Amazon SNS) pour émettre des notifications automatisées chaque fois que l'état clé d'une clé AWS KMS change de ou. `Disabled` `PendingDeletion` Par exemple, si un utilisateur essaie de désactiver ou de supprimer une clé AWS KMS, vous recevrez une notification par e-mail contenant des informations sur la tentative de changement de statut. Vous pouvez également utiliser ce modèle pour planifier la suppression des clés AWS KMS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec un utilisateur AWS Identity and Access Management (IAM)
- Une clé AWS KMS

Architecture

Pile technologique

- Amazon EventBridge
- AWS Key Management Service (AWS KMS)
- Amazon Simple Notification Service (Amazon SNS)

Architecture cible

Le schéma suivant montre une architecture permettant de créer un processus de surveillance et de notification automatisé pour détecter toute modification de l'état d'une clé AWS KMS.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur désactive ou planifie la suppression d'une clé AWS KMS.
2. Une EventBridge règle évalue le programme `Disabled` ou l'`PendingDeletion`événement.
3. La EventBridge règle invoque la rubrique Amazon SNS.
4. Amazon SNS envoie un message de notification par e-mail aux utilisateurs.

> **Note**
>
> Vous pouvez personnaliser le message électronique en fonction des besoins de votre organisation. Nous vous recommandons d'inclure des informations sur les entités dans lesquelles la clé AWS KMS est utilisée. Cela peut aider les utilisateurs à comprendre l'impact de la suppression de la clé AWS KMS. Vous pouvez également planifier une notification par e-mail de rappel envoyée un ou deux jours avant la suppression de la clé AWS KMS.

Automatisation et mise à l'échelle

La CloudFormation pile AWS déploie toutes les ressources et tous les services nécessaires au bon fonctionnement de ce modèle. Vous pouvez implémenter le modèle indépendamment dans un seul compte, ou en utilisant AWS CloudFormation StackSets pour plusieurs comptes indépendants ou unités organisationnelles dans AWS Organizations.

Outils

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur les comptes AWS et les régions AWS. Le CloudFormation modèle de ce modèle décrit toutes les ressources AWS que vous souhaitez, et CloudFormation fournit et configure ces ressources pour vous.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications et

services AWS, et achemine ces données vers des cibles telles qu'AWS Lambda. EventBridge simplifie le processus de création d'architectures pilotées par les événements.

- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Code

Le code de ce modèle est disponible dans le référentiel de désactivation et de suppression planifiée des clés GitHub Monitor AWS KMS.

Épopées

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le référentiel de désactivation et de suppression planifiée des clés GitHub Monitor AWS KMS sur votre machine locale en exécutant la commande suivante : `git clone https://github.com/aws-samples/aws-kms-deletion-notification`	Administrateur AWS, architecte du cloud
Mettez à jour les paramètres du modèle.	Dans un éditeur de code, ouvrez le `Alerting-KMS-Events.yaml` CloudFormation modèle que vous avez cloné à partir du référentiel, puis mettez à jour les paramètres suivants :	Administrateur AWS, architecte du cloud

Tâche	Description	Compétences requises
	• Pour `DestinationEmailAddress`, entrez une adresse e-mail active que vous prévoyez d'utiliser pour recevoir la notification SNS. • Pour `SNSTopicName`, entrez un nom pour votre rubrique SNS.	

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	1. Connectez-vous à AWS Management Console et ouvrez la console CloudFormation . 2. Dans le volet de navigation, choisissez Create stack, puis sélectionnez With new resources (standard). 3. Sur la page Identifier les ressources, choisissez Next. 4. Sur la page Spécifier le modèle, pour Source du modèle, sélectionnez Télécharger un fichier modèle. 5. Choisissez Choisir un fichier, sélectionnez le `Alerting-KMS-Events.yaml` fichier dans votre GitHub référentiel cloné, puis cliquez sur Suivant. 6. Dans le champ Nom de la pile, entrez le nom de la pile. 7. Sélectionnez Envoyer.	Administrateur AWS, architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'e-mail d'abonnement.	Une fois le CloudFormation modèle déployé avec succès,	Administrateur AWS, architecte du cloud

Tâche	Description	Compétences requises
	Amazon SNS envoie un message de confirmation d'abonnement à l'adresse e-mail que vous avez fournie dans CloudFormation le modèle. Pour recevoir des notifications, vous devez confirmer cet abonnement par e-mail. Pour plus d'informations, consultez Confirmer l'abonnement dans le manuel Amazon SNS Developer Guide.	

Testez la notification d'abonnement

Tâche	Description	Compétences requises
Désactivez les clés AWS KMS.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS KMS. 2. Pour modifier la région, choisissez le nom de la région actuellement affichée, puis choisissez la région vers laquelle vous souhaitez passer. 3. Dans le volet de navigation, sélectionnez Clés gérées par le client. 4. Cochez la case correspondant à la clé AWS KMS que	Administrateur AWS

Tâche	Description	Compétences requises
	vous souhaitez activer ou désactiver. 5. Pour désactiver la clé AWS KMS, choisissez Key actions, puis Disable.	
Validez l'abonnement.	Confirmez que vous avez reçu l'e-mail de notification Amazon SNS.	Administrateur AWS

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez la CloudFormation pile.	1. Connectez-vous à AWS Management Console et ouvrez la console CloudFormation . 2. Dans le volet de navigation, choisissez Stack (Piles). 3. Sélectionnez la pile que vous avez créée précédemment, puis choisissez Supprimer.	Administrateur AWS

Ressources connexes

- AWS CloudFormation (documentation AWS)
- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Création d'architectures pilotées par les événements sur AWS (documentation AWS Workshop Studio)
- Bonnes pratiques relatives aux services de gestion des clés AWS (livre blanc AWS)

- Bonnes pratiques de sécurité pour AWS Key Management Service (Guide du développeur AWS KMS)

Informations supplémentaires

Amazon SNS fournit un chiffrement en transit par défaut. Pour respecter les meilleures pratiques en matière de sécurité, vous pouvez également activer le chiffrement côté serveur pour Amazon SNS à l'aide d'une clé gérée par le client AWS KMS.

Préservez l'espace IP routable dans les conceptions VPC multi-comptes pour les sous-réseaux autres que les charges de travail

Créée par Adam Spicer (AWS)

Récapitulatif

Amazon Web Services (AWS) a publié les meilleures pratiques qui recommandent d'utiliser des sous-réseaux dédiés dans un cloud privé virtuel (VPC) pour les pièces jointes des passerelles de transit et les points de terminaison Gateway Load Balancer (pour prendre en charge AWS Network Firewall ou des appareils tiers). Ces sous-réseaux sont utilisés pour contenir des interfaces réseau élastiques pour ces services. Si vous utilisez à la fois AWS Transit Gateway et un Gateway Load Balancer, deux sous-réseaux sont créés dans chaque zone de disponibilité pour le VPC. En raison de leur conception, ces sous-réseaux supplémentaires ne peuvent pas être plus petits qu'un masque /28 et peuvent consommer un espace IP routable précieux qui pourrait autrement être utilisé pour des charges de travail routables. VPCs Ce modèle montre comment vous pouvez utiliser une plage de routage interdomaine sans classe (CIDR) secondaire et non routable pour ces sous-réseaux dédiés afin de préserver l'espace IP routable.

Conditions préalables et limitations

Prérequis

- Stratégie multi-VPC pour un espace IP routable
- Une plage CIDR non routable pour les services que vous utilisez (pièces jointes à des passerelles de transit et points de terminaison GatewayLoad Balancer ou Network Firewall)

Architecture

Architecture cible

Ce modèle inclut deux architectures de référence : une architecture comporte des sous-réseaux pour les pièces jointes de passerelle de transit (TGW) et un point de terminaison Gateway Load Balancer GWLBe (), et la seconde architecture possède des sous-réseaux pour les pièces jointes TGW uniquement.

Architecture 1 – VPC rattaché au TGW avec routage d'entrée vers une appliance

Le schéma suivant représente une architecture de référence pour un VPC qui couvre deux zones de disponibilité. Lors de l'entrée, le VPC utilise un modèle de routage d'entrée pour diriger le trafic destiné au sous-réseau public vers bump-in-the-wire une appliance à des fins d'inspection du pare-feu. Une pièce jointe TGW prend en charge la sortie des sous-réseaux privés vers un VPC distinct.

Ce modèle utilise une plage d'adresses CIDR non routable pour le sous-réseau d'attachement TGW et le sous-réseau. GWLBe Dans la table de routage TGW, ce CIDR non routable est configuré avec une route en trou noir (statique) en utilisant un ensemble de routes plus spécifiques. Si les itinéraires devaient être propagés vers la table de routage TGW, ces itinéraires en trou noir plus spécifiques s'appliqueraient.

Dans cet exemple, le CIDR routable /23 est divisé et entièrement alloué aux sous-réseaux routables.

Architecture 2 — VPC rattaché au TGW

Le schéma suivant représente une autre architecture de référence pour un VPC qui couvre deux zones de disponibilité. Une pièce jointe TGW prend en charge le trafic sortant (sortie) des sous-réseaux privés vers un VPC distinct. Il utilise une plage d'adresses CIDR non routable uniquement pour le sous-réseau des pièces jointes TGW. Dans la table de routage TGW, ce CIDR non routable est configuré avec un itinéraire en trou noir en utilisant un ensemble de routes plus spécifiques. Si les itinéraires devaient être propagés vers la table de routage TGW, ces itinéraires en trou noir plus spécifiques s'appliqueraient.

Dans cet exemple, le CIDR routable /23 est divisé et entièrement alloué aux sous-réseaux routables.

Outils

Services et ressources AWS

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS. Dans ce modèle, les VPC secondaires CIDRs sont utilisés pour préserver l'espace IP routable dans la charge de travail. CIDRs
- Le routage d'entrée de la passerelle Internet (associations de périphérie) peut être utilisé avec les points de terminaison Gateway Load Balancer pour les sous-réseaux dédiés non routables.

- AWS Transit Gateway est un hub central qui connecte VPCs les réseaux sur site. Dans ce modèle, VPCs sont rattachés de manière centralisée à une passerelle de transit, et les pièces jointes de la passerelle de transit se trouvent dans un sous-réseau dédié non routable.
- Les équilibreurs de charge de passerelle vous permettent de déployer, de mettre à l'échelle et de gérer des appareils virtuels, telles que des pare-feu, des systèmes de détection et de prévention des intrusions et des systèmes d'inspection approfondie des paquets. La passerelle sert de point d'entrée et de sortie unique pour l'ensemble du trafic. Dans ce modèle, les points de terminaison d'un Gateway Load Balancer peuvent être utilisés dans un sous-réseau dédié non routable.
- AWS Network Firewall est un pare-feu réseau dynamique et géré, ainsi qu'un service de détection et de prévention des intrusions VPCs destiné au cloud AWS. Dans ce modèle, les points de terminaison d'un pare-feu peuvent être utilisés dans un sous-réseau dédié non routable.

Référentiel de code

Un runbook et des CloudFormation modèles AWS pour ce modèle sont disponibles dans le référentiel de modèles CIDR secondaires GitHub non routables. Vous pouvez utiliser les fichiers d'exemple pour configurer un laboratoire de travail dans votre environnement.

Bonnes pratiques

AWS Transit Gateway

- Utilisez un sous-réseau distinct pour chaque attachement de VPC de passerelle de transit.
- Allouez un sous-réseau /28 à partir de la plage d'adresses CIDR non routable secondaire pour les sous-réseaux d'attachement de la passerelle de transit.
- Dans la table de routage de chaque passerelle de transit, ajoutez un itinéraire statique plus spécifique pour la plage d'adresses CIDR non routable sous forme de trou noir.

Gateway Load Balancer et routage d'entrée

- Utilisez le routage d'entrée pour diriger le trafic depuis Internet vers les points de terminaison Gateway Load Balancer.
- Utilisez un sous-réseau distinct pour chaque point de terminaison Gateway Load Balancer.
- Allouez un sous-réseau /28 à partir de la plage d'adresses CIDR non routable secondaire pour les sous-réseaux de point de terminaison Gateway Load Balancer.

Épopées

Créez VPCs

Tâche	Description	Compétences requises
Déterminez la plage d'adresses CIDR non routable.	Déterminez une plage d'adresses CIDR non routable qui sera utilisée pour le sous-réseau d'attachement de la passerelle de transit et (éventuellement) pour tout sous-réseau de point de terminaison Gateway Load Balancer ou Network Firewall. Cette plage de CIDR sera utilisée comme CIDR secondaire pour le VPC. Il ne doit pas être routable depuis la plage d'adresses CIDR principale du VPC ou depuis le réseau plus vaste.	Architecte du cloud
Déterminez les plages d'adresses CIDR routables pour. VPCs	Déterminez un ensemble de plages CIDR routables qui seront utilisées pour votre. VPCs Cette plage de CIDR sera utilisée comme CIDR principal pour votre. VPCs	Architecte du cloud
Créez VPCs.	Créez le vôtre VPCs et attachez-le à la passerelle de transit. Chaque VPC doit avoir une plage d'adresses CIDR principale routable et une plage d'adresses CIDR secondaire non routable, en fonction des plages que vous	Architecte du cloud

Tâche	Description	Compétences requises
	avez déterminées au cours des deux étapes précédentes.	

Configurer les itinéraires en trou noir de Transit Gateway

Tâche	Description	Compétences requises
Créez des trous non routables plus spécifiques CIDRs tels que des trous noirs.	Chaque table de routage de passerelle de transit doit comporter un ensemble de routes en trou noir créées pour les routes non CIDRs routables. Ils sont configurés pour garantir que tout trafic provenant du VPC CIDR secondaire reste non routable et ne pénètre pas dans le réseau plus vaste. Ces routes doivent être plus spécifiques que le CIDR non routable défini comme CIDR secondaire sur le VPC. Par exemple, si le CIDR secondaire non routable est 100.64.0.0/26, les routes en trou noir dans la table de routage de la passerelle de transit doivent être 100.64.0.0/27 et 100.64.0.32/27.	Architecte du cloud

Ressources connexes

- Bonnes pratiques pour le déploiement de Gateway Load Balancer
- Architectures d'inspection distribuées avec Gateway Load Balancer

- Journée d'immersion dans la mise en réseau – Laboratoire de pare-feu Internet vers VPC
- Bonnes pratiques pour la conception de passerelles de transit

Informations supplémentaires

La plage d'adresses CIDR secondaire non routable peut également être utile lorsque vous travaillez avec des déploiements de conteneurs à plus grande échelle qui nécessitent un grand nombre d'adresses IP. Vous pouvez utiliser ce modèle avec une passerelle NAT privée pour utiliser un sous-réseau non routable pour héberger vos déploiements de conteneurs. Pour plus d'informations, consultez le billet de blog Comment résoudre l'épuisement des adresses IP privées avec une solution NAT privée.

Provisionner un produit Terraform à l'aide AWS Service Catalog d'un référentiel de code

Créée par le Dr Rahul Sharad Gaikwad (AWS) et Tamilselvan (AWS)

Récapitulatif

AWS Service Catalog prend en charge le provisionnement en libre-service avec gouvernance de vos configurations HashiCorp Terraform. Si vous utilisez Terraform, vous pouvez utiliser Service Catalog comme outil unique pour organiser, gérer et distribuer vos configurations Terraform à grande échelle. AWS Vous pouvez accéder aux principales fonctionnalités de Service Catalog, notamment le catalogage de modèles d'infrastructure en tant que code (iAc) standardisés et préapprouvés, le contrôle d'accès, le provisionnement des ressources cloud avec un accès minimal, le versionnement, le partage avec des milliers de Comptes AWS personnes et le balisage. Les utilisateurs finaux, tels que les ingénieurs, les administrateurs de bases de données et les scientifiques des données, consultent la liste des produits et des versions auxquels ils ont accès, et ils peuvent les déployer en une seule action.

Ce modèle vous aide à déployer AWS des ressources à l'aide du code Terraform. Le code Terraform du GitHub référentiel est accessible via Service Catalog. En utilisant cette approche, vous intégrez les produits à vos flux de travail Terraform existants. Les administrateurs peuvent créer des portefeuilles Service Catalog et y ajouter AWS Launch Wizard des produits à l'aide de Terraform.

Les avantages de cette solution sont les suivants :

- Grâce à la fonctionnalité de restauration de Service Catalog, en cas de problème lors du déploiement, vous pouvez rétablir une version précédente du produit.
- Vous pouvez facilement identifier les différences entre les versions du produit. Cela vous permet de résoudre les problèmes lors du déploiement.
- Vous pouvez configurer une connexion au référentiel dans Service Catalog, par exemple vers GitHub ou GitLab. Vous pouvez apporter des modifications au produit directement via le référentiel.

Pour plus d'informations sur les avantages généraux de AWS Service Catalog, voir Qu'est-ce que Service Catalog ?

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Un GitHub ou un autre référentiel contenant les fichiers de configuration Terraform au format ZIP. BitBucket
- AWS Serverless Application Model Interface de ligne de commande (AWS SAM CLI), installée.
- AWS Command Line Interface (AWS CLI), installé et configuré.
- Allez-y, installé.
- Python version 3.9, installé. AWS SAM La CLI nécessite cette version de Python.
- Autorisations pour écrire et exécuter AWS Lambda des fonctions et autorisations pour accéder aux produits et aux portefeuilles Service Catalog et les gérer.

Architecture

Le schéma suivant illustre le flux de travail suivant :

1. Lorsqu'une configuration Terraform est prête, un développeur crée un fichier .zip contenant tout le code Terraform. Le développeur télécharge le fichier .zip dans le référentiel de code connecté à Service Catalog.
2. Un administrateur associe le produit Terraform à un portefeuille dans Service Catalog. L'administrateur crée également une contrainte de lancement qui permet aux utilisateurs finaux de fournir le produit.
3. Dans Service Catalog, les utilisateurs finaux lancent AWS des ressources à l'aide de la configuration Terraform. Ils peuvent choisir la version du produit à déployer.

Outils

Services AWS

- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Service Catalogvous permet de gérer de manière centralisée les catalogues de services informatiques approuvés. AWS Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.

Autres services

- Go est un langage de programmation open source pris en charge par Google.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Si vous avez besoin d'exemples de configurations Terraform que vous pouvez déployer via Service Catalog, vous pouvez utiliser les configurations du référentiel Amazon GitHub Macie Organization Setup Using Terraform. L'utilisation des exemples de code de ce référentiel n'est pas obligatoire.

Bonnes pratiques

- Au lieu de fournir les valeurs des variables dans le fichier de configuration Terraform (`terraform.tfvars`), configurez les valeurs des variables lors du lancement du produit via Service Catalog.
- N'accordez l'accès au portefeuille qu'à des utilisateurs ou administrateurs spécifiques.
- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation AWS Identity and Access Management (IAM).

Épopées

Configurez votre poste de travail local

Tâche	Description	Compétences requises
(Facultatif) Installez Docker.	Si vous souhaitez exécuter les AWS Lambda fonctions dans votre environnement de développement, installez Docker. Pour connaître la marche à suivre, consultez la rubrique Installer Docker Engine de la documentation Docker.	DevOps ingénieur

Tâche	Description	Compétences requises

Installez le AWS Service Catalog moteur pour Terraform.	1. Entrez la commande suivante pour cloner le référentiel AWS Service Catalog Engine for Terraform.
	`git clone https://github.com/aws-samples/service-catalog-engine-for-terraform-os.git`
	2. Accédez au répertoire racine du référentiel cloné.
	3. Entrez la commande suivante. Cela permet d'installer le moteur.
	`run ./bin/bash/deploy-tre.sh -r`
	Le Région AWS paramètre défini dans votre profil par défaut n'est pas utilisé lors de l'installation automatique. Vous indiquez plutôt la région lorsque vous exécutez cette commande.
		DevOps ingénieur, administrateur AWS

Connect le GitHub référentiel

Tâche	Description	Compétences requises
Créez une connexion au GitHub référentiel.	1. Connectez-vous à la console Developer Tools	Administrateur AWS

Tâche	Description	Compétences requises
	AWS Management Console, puis ouvrez-la. Vous pouvez accéder à la console Developer Tools en choisissant un service tel que AWS CodePipeline ou AWS CodeDeploy. 2. Dans le volet de navigation de gauche, choisissez Paramètres, puis Connections. 3. Choisissez Créer une connexion. 4. Sélectionnez le référentiel dans lequel vous conservez le code source de Terraform. Par exemple, vous pouvez choisir Bitbucket ou GitHub Enterprise Server. GitHub 5. Entrez le nom de la connexion, puis choisissez Connect. 6. Lorsque vous y êtes invité, authentifiez le référentiel. Une fois l'authentification terminée, la connexion est créée et le statut devient actif.	

Créer un produit Terraform dans Service Catalog

Tâche	Description	Compétences requises
Créez le produit Service Catalog.	1. Ouvrez la AWS Service Catalog console. 2. Accédez à la section Administration, puis sélectionnez Liste des produits. 3. Choisissez Créer un produit. 4. Sur la page Créer un produit dans la section Détails du produit, choisissez le type de produit externe. Service Catalog utilise ce type de produit pour prendre en charge les produits Terraform Community Edition. 5. Entrez le nom et le propriétaire du produit Service Catalog. 6. Sélectionnez Spécifiez votre référentiel de code à l'aide d'un CodeStar fournisseur. 7. Entrez les informations suivantes pour votre référentiel : • Connectez-vous à votre fournisseur en utilisant AWS CodeConnections — Sélectionnez la	Administrateur AWS

Tâche	Description	Compétences requises
	connexion que vous avez créée précédemment. • Référentiel — Sélectionnez le référentiel. • Branche : sélectionnez la branche. • Chemin du fichier modèle : choisissez le chemin dans lequel le fichier modèle de code est stocké. Le nom du fichier doit se terminer par `tar.gz`. 8. Sous Nom et description de la version, fournissez des informations sur la version du produit. 9. Choisissez Créer un produit.	

Tâche	Description	Compétences requises
Créez un portefeuille.	1. Ouvrez la AWS Service Catalog console. 2. Accédez à la section Administration, puis choisissez Portfolios. 3. Choisissez Créer un portefeuille. 4. Entrez les valeurs suivantes : • Nom du portefeuille — `Sample terraform` • Description du portefeuille — `Sample portfolio for Terraform configurations` • Propriétaire — Vos coordonnées, telles qu'une adresse e-mail 5. Choisissez Créer.	Administrateur AWS

Tâche	Description	Compétences requises
Ajoutez le produit Terraform au portefeuille.	1. Ouvrez la AWS Service Catalog console. 2. Accédez à la section Administration, puis sélectionnez Liste des produits. 3. Sélectionnez le produit Terraform que vous avez créé précédemment. 4. Choisissez Actions, puis sélectionnez Ajouter un produit au portefeuille. 5. Choisissez le `Sample terraform` portefeuille. 6. Choisissez Ajouter un produit au portefeuille.	Administrateur AWS

Tâche	Description	Compétences requises
Créez la stratégie d'accès.	1. Ouvrez la console AWS Identity and Access Management (IAM). 2. Dans le panneau de navigation, sélectionnez Policies (Politiques). 3. Dans le panneau de contenu, sélectionnez Créer une politique. 4. Choisissez l'option JSON. 5. Entrez l'exemple de politique JSON dans Politique d'accès dans la section Informations supplémentaires de ce modèle. 6. Choisissez Suivant. 7. Sur la page Réviser et créer, dans le champ Nom de la politique , entrez`TerraformResourceCreationAndArtifactAccessPolicy` . 8. Choisissez Create Policy (Créer une politique).	Administrateur AWS

Tâche	Description	Compétences requises
Créez une politique de confiance personnalisée.	1. Ouvrez la console IAM. 2. Dans le panneau de navigation, choisissez Roles (Rôles). 3. Sélectionnez Create role (Créer un rôle). 4. Sous Type d'entité fiable, choisissez Politique de confiance personnalisée. 5. Dans l'éditeur de stratégie JSON, entrez l'exemple de politique JSON dans Politique de confiance dans la section Informations supplémentaires de ce modèle. 6. Choisissez Suivant. 7. Sous Politiques d'autorisations, choisissez celles `TerraformResourceCreationAndArtifactAccessPolicy` que vous avez créées précédemment. 8. Choisissez Suivant. 9. Sous Détails du rôle, dans la zone Nom du rôle, entrez`SCLaunch-product` .	Administrateur AWS

Tâche	Description	Compétences requises
	Important Le nom du rôle doit commencer par`SCLaunch`. 10. Choisissez Créer un rôle.	

Tâche	Description	Compétences requises
Ajoutez une contrainte de lancement au produit Service Catalog.	1. Connectez-vous au en AWS Management Console tant qu'utilisateur disposant d'autorisations administratives. 2. Ouvrez la AWS Service Catalog console. 3. Dans le volet de navigation, sélectionnez Portfolios. 4. Choisissez le portfolio que vous avez créé précédemment. 5. Sur la page des détails du portefeuille, choisissez l'onglet Contraintes, puis sélectionnez Créer une contrainte. 6. Pour Produit, sélectionnez le produit Terraform que vous avez créé précédemment. 7. Sous Contrainte de lancement, pour Méthode, choisissez Enter role name. 8. Dans le champ Nom du rôle, entrez`SCLaunch-product` . 9. Choisissez Créer.	Administrateur AWS

Tâche	Description	Compétences requises
Accordez l'accès au produit.	1. Ouvrez la AWS Service Catalog console. 2. Dans le volet de navigation, sélectionnez Portfolios. 3. Choisissez le portfolio que vous avez créé précédemment. 4. Choisissez l'onglet Accès, puis choisissez Accorder l'accès. 5. Choisissez l'onglet Rôles, puis sélectionnez le rôle qui doit avoir accès pour déployer ce produit. 6. Choisissez Grant access (Accorder l'accès).	Administrateur AWS

Tâche	Description	Compétences requises
Lancez le produit.	1. Connectez-vous en AWS Management Console tant qu'utilisateur autorisé à déployer le produit Service Catalog. 2. Ouvrez la AWS Service Catalog console. 3. Dans le volet de navigation, sélectionnez Products. 4. Choisissez le produit que vous avez créé précédemment, puis choisissez Launch product. 5. Entrez le nom du produit et définissez les paramètres requis. 6. Choisissez Launch product.	DevOps ingénieur

Vérification du déploiement

Tâche	Description	Compétences requises
Validez le déploiement.	Il existe deux machines AWS Step Functions d'état pour le flux de travail de provisionnement du Service Catalog : • `ManageProvisionedProductStateMachine` — Service Catalog invoque cette machine d'état lors du provisionnement d'un nouveau produit	DevOps ingénieur

Tâche	Description	Compétences requises
	Terraform et lors de la mise à jour d'un produit fourni par Terraform existant. • `TerminateProvisionedProductStateMachine` — Service Catalog invoque cette machine d'état lors de la résiliation d'un produit approvisionné par Terraform existant. Vous consultez les journaux de la machine `ManageProvisionedProductStateMachine` d'état pour confirmer que le produit a été approvisionné. 1. Connectez-vous à la AWS Step Functions console AWS Management Console, puis ouvrez-la. 2. Dans le volet de navigation de gauche, sélectionnez State machines. 3. Choisissez`ManageProvisionedProductStateMachine` . 4. Dans la liste des exécutions, entrez l'ID de produit fourni pour localiser l'exécution.	

Tâche	Description	Compétences requises
	Note Les noms des compartiments principaux du fichier d'état commencent `sc-terraform-engine-state-` par. 5. Vérifiez que toutes les ressources requises ont été créées dans le compte.	

Nettoyer les infrastructures

Tâche	Description	Compétences requises
Supprimez les produits approvisionnés.	1. Connectez-vous en AWS Management Console tant qu'utilisateur autorisé à déployer le produit Service Catalog. 2. Ouvrez la AWS Service Catalog console. 3. Dans le menu de navigation de gauche, choisissez Provisioned products. 4. Sélectionnez le produit que vous avez créé. 5. Dans la liste Actions, choisissez Terminate.	DevOps ingénieur

Tâche	Description	Compétences requises
	6. Dans la zone de texte de confirmation, entrez`terminate` , puis choisissez Terminer le produit approvisionné. 7. Répétez ces étapes pour mettre fin à tous les produits approvisionnés.	

Tâche	Description	Compétences requises
Supprimez le AWS Service Catalog moteur de Terraform.	1. Connectez-vous au en AWS Management Console tant qu'utilisateur disposant d'autorisations administratives. 2. Ouvrez la console Amazon Simple Storage Service (Amazon S3). 3. Dans le volet de navigation, choisissez Compartiments. 4. Sélectionnez le `sc-terraform-engine-logging-XXXX` compartiment. 5. Choisissez Vide. 6. Répétez les étapes 4 à 5 pour les compartiments suivants : • `sc-terraform-engine-state-XXXX` • `terraform-engine-bootstrap-XXXX` 7. Ouvrez la AWS CloudFormation console, puis vérifiez que vous êtes dans la bonne position Région AWS. 8. Dans le menu de navigation de gauche, choisissez Stacks. 9. Sélectionnez`SAM-TRE`, puis choisissez Supprimer.	Administrateur AWS

Tâche	Description	Compétences requises
	Patientez jusqu'à ce que la pile soit supprimée. 10. Sélectionnez `Bootstrap-TRE`, puis choisissez Supprimer. Patientez jusqu'à ce que la pile soit supprimée.	

Ressources connexes

AWS documentation

- Commencer à utiliser un produit Terraform

Documentation Terraform

- Installation de Terraform
- Configuration du backend Terraform
- Documentation du fournisseur Terraform AWS

Informations supplémentaires

Politique d'accès

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
```

```
            }
        },
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Politique d’approbation

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "GivePermissionsToServiceCatalog",
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account_id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
TerraformExecutionRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogExternalParameterParserRole*",
                        "arn:aws:iam::accounti_id:role/TerraformEngine/
ServiceCatalogTerraformOSParameterParserRole*"
                    ]
                }
            }
        }
    ]
}
```

Enregistrez plusieurs comptes AWS avec une seule adresse e-mail à l'aide d'Amazon SES

Créée par Joe Wozniak (AWS) et Shubhangi Vishwakarma (AWS)

Récapitulatif

Ce modèle décrit comment vous pouvez dissocier les adresses e-mail réelles de l'adresse e-mail associée à un. Compte AWS Comptes AWS exigent qu'une adresse e-mail unique soit fournie au moment de la création du compte. Dans certaines organisations, l'équipe de gestion Comptes AWS doit assumer la charge de gérer de nombreuses adresses e-mail uniques avec son équipe de messagerie. Cela peut s'avérer difficile pour les grandes entreprises qui en gèrent de nombreuses Comptes AWS. De plus, si votre système de messagerie n'autorise pas l'adressage plus ou le sous-adressage tels que définis dans Sieve Email Filtering : Subaddress Extension (RFC 5233), en ajoutant un signe plus (+) et un identifiant à la fin de la partie locale de l'adresse e-mail, par exemple `admin+123456789123@example.com` —ce modèle peut aider à surmonter cette limitation.

Ce modèle fournit une solution de vente d'adresses e-mail unique qui permet aux Compte AWS propriétaires d'associer une adresse e-mail à plusieurs Comptes AWS. Les adresses e-mail réelles des Compte AWS propriétaires sont ensuite associées à ces adresses e-mail générées dans un tableau. La solution gère tous les e-mails entrants pour les comptes de messagerie uniques, recherche le propriétaire de chaque compte, puis transmet tous les messages reçus au propriétaire.

Conditions préalables et limitations

Prérequis

- Accès administratif à un Compte AWS.
- Accès à un environnement de développement.
- (Facultatif) La connaissance des AWS Cloud Development Kit (AWS CDK) flux de travail et du langage de programmation Python vous aidera à résoudre les problèmes ou à apporter des modifications.

Limites

- La longueur totale de l'adresse e-mail vendue est de 64 caractères. Pour plus de détails, consultez CreateAccountla référence de AWS Organizations l'API.

Versions du produit

- Node.js version 12.7.0 ou ultérieure
- Python 3.9 ou version ultérieure
- Paquets Python pip et virtualenv
- AWS CDK version 2.23.0 ou ultérieure
- Docker 20.10.x ou version ultérieure

Architecture

Pile technologique cible

- AWS CloudFormation pile
- AWS Lambda fonctions
- Règle et ensemble de règles Amazon Simple Email Service (Amazon SES)
- AWS Identity and Access Management Rôles et politiques (IAM)
- Politique relative aux compartiments et aux compartiments Amazon Simple Storage Service (Amazon S3)
- AWS Key Management Service (AWS KMS) politique clé et clé
- Rubrique et politique relatives à Amazon Simple Notification Service (Amazon SNS)
- Table Amazon DynamoDB

Architecture cible

Ce diagramme montre deux flux :

- Flux de distribution d'adresses e-mail : dans le diagramme, le flux de distribution d'adresses e-mail (section inférieure) commence généralement par une solution de vente de comptes ou une automatisation externe, ou est invoqué manuellement. Dans la demande, une fonction Lambda est appelée avec une charge utile contenant les métadonnées nécessaires. La fonction utilise ces informations pour générer un nom de compte et une adresse e-mail uniques, les stocke dans une base de données DynamoDB et renvoie les valeurs à l'appelant. Ces valeurs peuvent ensuite être utilisées pour créer un nouveau Compte AWS (généralement en utilisant AWS Organizations).

- Flux de transfert d'e-mails : Ce flux est illustré dans la partie supérieure du schéma précédent. Lorsqu'un Compte AWS est créé à l'aide de l'e-mail du compte généré à partir du flux de vente d'adresses e-mail, il AWS envoie divers e-mails, tels que la confirmation de l'enregistrement du compte et des notifications périodiques, à cette adresse e-mail. En suivant les étapes de ce modèle, vous Compte AWS configurez Amazon SES pour recevoir des e-mails pour l'ensemble du domaine. Cette solution configure les règles de transfert qui permettent à Lambda de traiter tous les e-mails entrants, de vérifier si T0 l'adresse figure dans le tableau DynamoDB et de transférer le message à l'adresse e-mail du propriétaire du compte. L'utilisation de ce processus permet aux propriétaires de comptes d'associer plusieurs comptes à une seule adresse e-mail.

Automatisation et mise à l'échelle

Ce modèle utilise le AWS CDK pour automatiser entièrement le déploiement. La solution utilise des services AWS gérés qui seront (ou peuvent être configurés pour) évoluer automatiquement en fonction de vos besoins. Les fonctions Lambda peuvent nécessiter une configuration supplémentaire pour répondre à vos besoins de dimensionnement. Pour plus d'informations, consultez la section Comprendre le dimensionnement des fonctions Lambda dans la documentation Lambda.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- Amazon Simple Email Service (Amazon SES) vous permet d'envoyer et de recevoir des e-mails en utilisant vos propres adresses e-mail et domaines.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Outils nécessaires au déploiement

- Environnement de développement avec accès AWS CLI et IAM à votre Compte AWS. Pour plus de détails, consultez les liens dans la section Ressources connexes.
- Sur votre système de développement, installez les éléments suivants :
  - Outil de ligne de commande Git, disponible sur le site Web de téléchargement de Git.
  - AWS CLI pour configurer les informations d'accès pour le AWS CDK. Pour plus d’informations, consultez la documentation AWS CLI.
  - Python version 3.9 ou ultérieure, disponible sur le site Web de téléchargement de Python.
  - Paquets Python pip et virtualenv. Pour les instructions d'installation, consultez la documentation pip et la documentation virtualenv.
  - Node.js version 12.7.0 ou ultérieure. Pour les instructions d'installation, consultez la documentation Node.js.
  - AWS CDK version 2.23.0 ou ultérieure. Pour les instructions d'installation, consultez la AWS CDK documentation.
  - Docker version 20.10.x ou ultérieure. Pour les instructions d'installation, consultez la documentation Docker.

Code

Le code de ce modèle est disponible dans le référentiel GitHub Compte AWS d'e-mails d'usine.

Épopées

Allouer un environnement de déploiement cible

Tâche	Description	Compétences requises
Identifiez ou créez un Compte AWS.	Identifiez une solution existante ou nouvelle Compte AWS à laquelle vous disposez d'un accès administratif complet, afin de déployer la solution de messagerie.	Administrateur AWS, administrateur du cloud
Configurez un environnement de déploiement.	Configurez un environnement de déploiement facile à utiliser et configurez les dépendances en suivant ces étapes : 1. Configurez votre environnement de développement avec les outils répertoriés dans la section Outils. 2. Clonez la base de code du référentiel d'e-mails d' GitHub Compte AWS usine dans votre environnement de développement à l'aide de la commande : `git clone https://github.com/aws-samples/aws-account-factory-email` 3. Dans le `requirements.txt` fichier (à la racine du référentiel), mettez à jour la ligne	AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises
	commençant par `aws-cdk-lib==` pour qu'elle corresponde à la AWS CDK version exécutée dans votre environnement. Pour identifier la version, utilisez la `cdk --version` commande.	

Configurer un domaine vérifié

Tâche	Description	Compétences requises
Identifiez et attribuez un domaine.	La fonctionnalité de transfert d'e-mails nécessite un domaine dédié. Identifiez et attribuez un domaine ou un sous-domaine que vous pouvez vérifier auprès d'Amazon SES. Ce domaine doit être disponible pour recevoir les e-mails entrants dans l' Compte AWS endroit où la solution de transfert d'e-mails est déployée. Exigences relatives au domaine : • Le domaine doit être un domaine ou un sous-domaine standard. • Le domaine doit pouvoir être résolu par DNS en externe, car il sera utilisé	Administrateur cloud, administrateur réseau, administrateur DNS

Tâche	Description	Compétences requises
	pour recevoir des e-mails provenant de l'extérieur de l'organisation.	
Vérifiez le domaine.	Vérifiez que le domaine identifié peut être utilisé pour accepter les e-mails entrants. Suivez les instructions de la section Vérification de votre domaine pour la réception d'e-mails par Amazon SES dans la documentation Amazon SES. Cela nécessitera une coordination avec la personne ou l'équipe responsable des enregistrements DNS du domaine.	Développeur d'applications, AWS DevOps
Configurez des enregistrements MX.	Configurez votre domaine avec des enregistrements MX qui pointent vers les points de terminaison Amazon SES de votre Compte AWS région. Pour plus d'informations, consultez la section Publication d'un enregistrement MX pour la réception d'e-mails par Amazon SES dans la documentation Amazon SES.	Administrateur cloud, administrateur réseau, administrateur DNS

Déployez la solution de distribution et de transfert d'e-mails

Tâche	Description	Compétences requises
Modifiez les valeurs par défaut dans`cdk.json`.	Modifiez certaines des valeurs par défaut dans le `cdk.json` fichier (à la racine du référentiel) afin que la solution fonctionne correctem ent après son déploiement. 1. Modifiez la `SES_DOMAI N_NAME` valeur pour qu'elle corresponde au nom de domaine que vous avez vérifié précédemment. 2. Modifiez la `ADDRESS_F ROM` valeur pour inclure le même domaine que celui dans`SES_DOMAI N_NAME` . La partie locale de l'adresse doit être déterminée par votre équipe cloud. Cette adresse devient l'`FROM`adresse de chaque e-mail transféré via la solution. 3. Modifiez la `ADDRESS_A DMIN` valeur pour qu'elle corresponde à l'adresse e-mail vers laquelle les messages entrants non correspondants seront transférés. Cette valeur doit être une adresse e-mail valide et fonctionnelle.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises

Déployez la solution de distribution et de transfert d'e-mails.	1. Créez un environnement virtuel Python :
	`python -m venv .venv`
	2. Activez l'environnement virtuel Python :
	`source .venv/bin/activate`
	Ou, sur la plate-forme Windows, utilisez :
	`% .venv\Scripts\activate.bat`
	3. Installez toutes les exigences de Python sans erreur :
	`pip install -r requirements.txt`
	4. Synthétisez le CloudFormation modèle :
	`cdk synth`
	Vérifiez qu'il n'y a aucune erreur et que le CloudFormation modèle complet contient le résultat attendu.
	5. (Facultatif) Si vous déployez le AWS CDK code dans l'environnement actuel
		Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises

	Compte AWS ou dans la région pour la première fois, démarrez l'environ nement. Pour plus d'informa tions, consultez AWS CDK Bootstrapping dans la AWS CDK documentation.
	
	`cdk bootstrap aws://AWS-ACCOUNT-NUMBER/REGION`
	
	Remplacez `AWS-ACCOU NT-NUMBER` et `REGION` par les valeurs réelles.
	6. Déployez la solution :
	
	`cdk bootstrap`
	`cdk deploy`
	
	Les commandes devraient s'exécuter sans erreur.	

Tâche	Description	Compétences requises
Vérifiez que la solution a été déployée.	Vérifiez que la solution a été déployée avec succès avant de commencer les tests : 1. Ouvrez la AWS CloudFormation console et recherchez une CloudFormation pile contenant le nom `AwsMailFwdStack` . 2. Vérifiez que cette `AwsMailFwdStack` pile possède les ressources suivantes : • Fonctions Lambda • Règles et ensemble de règles Amazon SES • Rôles et politiques IAM • Politique relative aux compartiments et aux compartiments Amazon S3 • AWS KMS politique clé et clé • Rubrique Amazon SNS et politique relative aux rubriques • Tableau DynamoDB	Développeur d'applications, AWS DevOps

Vérifiez que la vente et le transfert d'e-mails fonctionnent comme prévu

Tâche	Description	Compétences requises
Vérifiez que l'API fonctionne.	Au cours de cette étape, vous soumettez des données de test à l'API de la solution et vous confirmez que la solution produit le résultat attendu et que les opérations de backend ont été effectuées comme prévu. Exécutez manuellement la fonction Lambda Vend Email en utilisant une entrée de test. (Pour un exemple, consultez le fichier sample_vend_request.json.) Pour `OwnerAddress`, utilisez une adresse e-mail valide. L'API doit renvoyer un nom de compte et un e-mail contenant les valeurs attendues.	Développeur d'applications, AWS DevOps
Vérifiez que l'e-mail est transféré.	Au cours de cette étape, vous envoyez un e-mail de test via le système et vous vérifiez qu'il est transféré au destinataire attendu. 1. Obtenez l'adresse e-mail du compte à la dernière étape. 2. Envoyez un e-mail à cette adresse avec le sujet du test et le corps du texte.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	3. Confirmez que vous avez reçu l'e-mail à l'adresse e-mail du propriétaire du compte. 4. Vérifiez que l'`FROM`adresse e-mail que vous avez reçue correspond aux `ADDRESS_FROM` paramètres définis dans`scdk.json`. 5. Vérifiez que l'objet et le corps de l'e-mail reçu sont identiques à ceux du message envoyé d'origine.	

Résolution des problèmes

Problème	Solution
Le système ne transmet pas les e-mails comme prévu.	Vérifiez que votre configuration est correcte : 1. Vous devez avoir terminé le processus de vérification Amazon SES pour votre domaine. 2. Votre domaine doit être correctement configuré avec des enregistrements MX pointant vers les points de terminaison Amazon SES de votre Compte AWS région. Pour plus d'informations, consultez la section Publication d'un enregistrement MX pour la réception d'e-mails par Amazon SES dans la documentation Amazon SES.

Problème	Solution
	Après avoir vérifié la configuration de votre domaine, procédez comme suit : 1. Ouvrez la CloudWatch console Amazon correspondant au compte et à la région dans lesquels vous avez déployé la solution, puis accédez aux groupes de CloudWatch journaux dans le volet de navigation. 2. Recherchez dans la liste des groupes de journaux`SesMailForwardLogGroup` . 3. Examinez les journaux de ce groupe pour voir si des erreurs sont générées lors du processus de vente et de transfert d'e-mails.

Problème	Solution
Lorsque vous essayez de déployer la AWS CDK pile, vous recevez un message d'erreur similaire au message suivant : « Erreur de format du modèle : types de ressources non reconnus »	Dans la plupart des cas, ce message d'erreur signifie que la région que vous ciblez ne dispose pas de tous les services AWS disponibles. Si vous utilisez une EC2 instance Amazon pour déployer la solution, vous ciblez peut-être une région différente de celle dans laquelle l'instance est exécutée. **Note** Par défaut, il est AWS CDK déployé dans la région et le compte que vous avez configurés dans le AWS CLI. Solutions possibles : 1. Vérifiez si tous les services nécessaires à cette solution (voir la section relative à la pile technologique Target plus haut dans ce modèle) correspondent à ceux Région AWS que vous ciblez en consultant les services AWS par région. 2. Si vous utilisez une EC2 instance et que vous ciblez une région différente de celle dans laquelle votre instance est exécutée, assurez-vous de définir la variable d'`AWS_DEFAULT_REGION` environnement ou de définir une région avec le AWS CLI avant de déployer la solution. Pour plus d'informations, consultez la section Configuration des variables d'environnement AWS CLI dans la AWS CLI documentation. Vous pouvez également modifier le `app.py` fichier situé à la racine du référentiel pour

Problème	Solution
	inclure un identifiant de compte et une région codés en dur en suivant les instructions de la AWS CDK documentation relative aux environnements.
Lorsque vous déployez la solution, vous recevez le message d'erreur suivant : « Échec du déploiement : erreur AwsMailFwdStack : SSM parameter /cdk-bootstrap/hnb659fds/version introuvable. L'environnement a-t-il été amorcé ? Veuillez exécuter 'cdk bootstrap' »	Si vous n'avez jamais déployé de AWS CDK ressources dans la région Compte AWS et que vous ciblez, vous devez d'abord exécuter la `cdk bootstrap` commande comme l'indique l'erreur. Si cette erreur persiste après avoir exécuté la commande d'amorçage, vous essayez peut-être de déployer la solution dans une région différente de celle dans laquelle votre environnement de développement est exécuté. Pour résoudre ce problème, définissez la variable d'`AWS_DEFAULT_REGION` environnement ou définissez une région avec le AWS CLI avant de déployer la solution. Vous pouvez également modifier le `app.py` fichier situé à la racine du référentiel pour inclure un identifiant de compte et une région codés en dur en suivant les instructions de la AWS CDK documentation relative aux environnements.

Ressources connexes

- Pour obtenir de l'aide sur l'installation du AWS CLI, voir Installation ou mise à jour vers la dernière version du AWS CLI.
- Pour obtenir de l'aide sur la configuration du AWS CLI avec les informations d'identification d'accès IAM, consultez Configuration des paramètres pour le AWS CLI.
- Pour obtenir de l'aide concernant le AWS CDK, consultez Getting started with the AWS CDK.

Informations supplémentaires

Coûts

Lorsque vous déployez cette solution, le Compte AWS titulaire peut encourir des coûts liés à l'utilisation des services suivants. Il est important que vous compreniez comment ces services sont facturés afin de connaître les éventuels frais. Pour plus d'informations sur les tarifs, consultez les pages suivantes :

- Tarification d'Amazon SES
- Tarification d'Amazon S3
- AWS KMS tarification
- AWS Lambda tarification
- Tarification d'Amazon DynamoDB

Configuration de la résolution DNS pour les réseaux hybrides dans un environnement AWS à compte unique

Créée par Abdullahi Olaoye (AWS)

Récapitulatif

Ce modèle décrit comment configurer une architecture de système de noms de domaine (DNS) entièrement hybride qui permet la résolution end-to-end DNS des ressources sur site, des ressources AWS et des requêtes DNS Internet, sans surcharge administrative. Le modèle décrit comment configurer les règles de transfert Amazon Route 53 Resolver qui déterminent où une requête DNS provenant d'AWS doit être envoyée, en fonction du nom de domaine. Les requêtes DNS pour les ressources locales sont transmises aux résolveurs DNS locaux. Les requêtes DNS pour les ressources AWS et les requêtes DNS Internet sont résolues par Route 53 Resolver.

Ce modèle couvre la résolution DNS hybride dans un environnement AWS à compte unique. Pour plus d'informations sur la configuration des requêtes DNS sortantes dans un environnement AWS multi-comptes, consultez le modèle Configurer la résolution DNS pour les réseaux hybrides dans un environnement AWS multi-comptes.

Conditions préalables et limitations

Prérequis

- Un compte AWS
- Un cloud privé virtuel (VPC) dans votre compte AWS
- Une connexion réseau entre l'environnement sur site et votre VPC, via le réseau privé virtuel AWS (AWS VPN) ou AWS Direct Connect
- Adresses IP de vos résolveurs DNS locaux (accessibles depuis votre VPC)
- Nom de domaine/sous-domaine à transférer vers des résolveurs locaux (par exemple, onprem.mydc.com)
- Nom de domaine/sous-domaine pour la zone hébergée privée AWS (par exemple, myvpc.cloud.com)

Architecture

Pile technologique cible

- Zone hébergée privée Amazon Route 53
- Amazon Route 53 Resolver
- Amazon VPC
- VPN AWS ou Direct Connect

Architecture cible

Outils

- Amazon Route 53 Resolver facilite le cloud hybride pour les entreprises clientes en permettant une résolution fluide des requêtes DNS sur l'ensemble de votre cloud hybride. Vous pouvez créer des points de terminaison DNS et des règles de transfert conditionnelles pour résoudre les espaces de noms DNS entre votre centre de données local et votre. VPCs
- La zone hébergée privée Amazon Route 53 est un conteneur qui contient des informations sur la manière dont vous souhaitez que Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs que vous créez avec le service Amazon VPC.

Épopées

Configuration d'une zone hébergée privée

Tâche	Description	Compétences requises
Créez une zone hébergée privée Route 53 pour un nom de domaine réservé AWS tel que myvpc.cloud.com.	Cette zone contient les enregistrements DNS pour les ressources AWS qui doivent être résolues à partir de l'environnement sur site. Pour obtenir des instructions, consultez la section Création d'une zone hébergée privée dans la documentation de Route 53.	Administrateur réseau, administrateur système

Tâche	Description	Compétences requises
Associez la zone hébergée privée à votre VPC.	Pour permettre aux ressources de votre VPC de résoudre les enregistrements DNS dans cette zone hébergée privée, vous devez associer votre VPC à la zone hébergée. Pour obtenir des instructions, consultez la section Création d'une zone hébergée privée dans la documentation de Route 53.	Administrateur réseau, administrateur système

Configuration des points de terminaison Route 53 Resolver

Tâche	Description	Compétences requises
Créez un point de terminaison entrant.	Route 53 Resolver utilise le point de terminaison entrant pour recevoir les requêtes DNS des résolveurs DNS locaux. Pour obtenir des instructions, consultez la section Transférer des requêtes DNS entrantes vers votre VPCs adresse dans la documentation de Route 53. Notez l'adresse IP du point de terminaison entrant.	Administrateur réseau, administrateur système
Créez un point de terminaison sortant.	Route 53 Resolver utilise le point de terminaison sortant pour envoyer des requêtes DNS aux résolveurs DNS locaux. Pour obtenir des	Administrateur réseau, administrateur système

Tâche	Description	Compétences requises
	instructions, consultez la section Transfert de requêtes DNS sortantes vers votre réseau dans la documentation de Route 53. Notez l'ID du point de terminaison de sortie.	

Configurez une règle de transfert et associez-la à votre VPC

Tâche	Description	Compétences requises
Créez une règle de transfert pour le domaine local.	Cette règle indiquera à Route 53 Resolver de transférer toutes les requêtes DNS pour les domaines locaux (tels que onprem.mydc.com) aux résolveurs DNS locaux. Pour créer cette règle, vous aurez besoin des adresses IP des résolveurs DNS locaux et de l'ID du point de terminaison sortant pour le résolveur Route 53. Pour obtenir des instructions, consultez la section Gestion des règles de transfert dans la documentation de Route 53.	Administrateur réseau, administrateur système
Associez la règle de transfert à votre VPC.	Pour que la règle de transfert prenne effet, vous devez l'associer à votre VPC. Route 53 Resolver prend ensuite la règle en compte lors de la résolution d'un domaine. Pour obtenir des instructions,	Administrateur réseau, administrateur système

Tâche	Description	Compétences requises
	consultez la section Gestion des règles de transfert dans la documentation de Route 53.	

Configuration de résolveurs DNS locaux

Tâche	Description	Compétences requises
Configurez le transfert conditionnel dans les résolveurs DNS sur site.	Pour que les requêtes DNS soient envoyées à la zone hébergée privée Route 53 depuis l'environnement local, vous devez configurer le transfert conditionnel dans les résolveurs DNS locaux. Cela indique aux résolveur s DNS de transférer toutes les requêtes DNS pour le domaine AWS (par exemple, pour myvpc.cloud.com) à l'adresse IP du point de terminaison entrant pour le résolveur Route 53.	Administrateur réseau, administrateur système

Tester la résolution end-to-end DNS

Tâche	Description	Compétences requises
Testez la résolution DNS depuis AWS vers l'environ nement sur site.	Depuis un serveur du VPC, effectuez une requête DNS pour un domaine local (tel que server1.onprem.mydc.com).	Administrateur réseau, administrateur système

Tâche	Description	Compétences requises
Testez la résolution DNS depuis l'environnement sur site vers AWS.	À partir d'un serveur sur site, effectuez une résolution DNS pour un domaine AWS (tel que server1.myvpc.cloud.com).	Administrateur réseau, administrateur système

Ressources connexes

- Gestion DNS centralisée du cloud hybride avec Amazon Route 53 et AWS Transit Gateway (blog AWS Networking & Content Delivery)
- Simplifiez la gestion du DNS dans un environnement multi-comptes avec Route 53 Resolver (blog de sécurité AWS)
- Utilisation de zones hébergées privées (documentation Route 53)
- Mise en route avec Route 53 Resolver (documentation Route 53)

Configurez automatiquement des robots UiPath RPA sur Amazon à l'aide EC2 d'AWS CloudFormation

Créée par le Dr Rahul Sharad Gaikwad (AWS) et Tamilselvan (AWS)

Récapitulatif

Ce modèle explique comment déployer des robots d'automatisation robotique des processus (RPA) sur des instances Amazon Elastic Compute Cloud (Amazon EC2). Il utilise un pipeline EC2 Image Builder pour créer une Amazon Machine Image (AMI) personnalisée. Une AMI est une image de machine virtuelle (VM) préconfigurée qui contient le système d'exploitation (OS) et le logiciel préinstallé pour déployer EC2 les instances. Ce modèle utilise des CloudFormation modèles AWS pour installer l'édition UiPath Studio Community sur l'AMI personnalisée. UiPath est un outil RPA qui vous aide à configurer des robots pour automatiser vos tâches.

Dans le cadre de cette solution, les instances EC2 Windows sont lancées à l'aide de l'AMI de base, et l'application UiPath Studio est installée sur les instances. Le modèle utilise l'outil Microsoft System Preparation (Sysprep) pour dupliquer l'installation personnalisée de Windows. Ensuite, il supprime les informations sur l'hôte et crée une AMI finale à partir de l'instance. Vous pouvez ensuite lancer les instances à la demande en utilisant l'AMI finale avec vos propres conventions de dénomination et votre propre configuration de surveillance.

> **Note**
>
> Ce modèle ne fournit aucune information sur l'utilisation des robots RPA. Pour plus d'informations, consultez la UiPath documentation. Vous pouvez également utiliser ce modèle pour configurer d'autres applications de robots RPA en personnalisant les étapes d'installation en fonction de vos besoins.

Ce modèle fournit les automatisations et les avantages suivants :

- Déploiement et partage d'applications : vous pouvez créer Amazon EC2 AMIs pour le déploiement d'applications et les partager entre plusieurs comptes via un pipeline EC2 Image Builder, qui utilise des CloudFormation modèles AWS comme scripts d'infrastructure en tant que code (IaC).

- EC2 Provisionnement et mise à l'échelle d'Amazon : les modèles CloudFormation iAC fournissent des séquences de noms d'ordinateurs personnalisées et automatisent les jointures Active Directory.
- Observabilité et surveillance : le modèle configure les CloudWatch tableaux de bord Amazon pour vous aider à surveiller les EC2 indicateurs Amazon (tels que l'utilisation du processeur et du disque).
- Avantages de la RPA pour votre entreprise : la RPA améliore la précision car les robots peuvent exécuter les tâches assignées automatiquement et de manière cohérente. La RPA augmente également la vitesse et la productivité car elle supprime les opérations sans valeur ajoutée et gère les activités répétitives.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorisations AWS Identity and Access Management (IAM) pour le déploiement de modèles CloudFormation
- Politiques IAM pour configurer la distribution d'AMI entre comptes avec Image Builder EC2

Architecture

1. L'administrateur fournit l'AMI Windows de base dans le `ec2-image-builder.yaml` fichier et déploie la pile dans la CloudFormation console.
2. La CloudFormation pile déploie le pipeline EC2 Image Builder, qui inclut les ressources suivantes :
   - `Ec2ImageInfraConfiguration`
   - `Ec2ImageComponent`
   - `Ec2ImageRecipe`
   - `Ec2AMI`
3. Le pipeline EC2 Image Builder lance une EC2 instance Windows temporaire à l'aide de l'AMI de base et installe les composants requis (dans ce cas, UiPath Studio).
4. EC2 Image Builder supprime toutes les informations sur l'hôte et crée une AMI à partir de Windows Server.

5. Vous mettez à jour le `ec2-provisioning yaml` fichier avec l'AMI personnalisée et lancez un certain nombre d' EC2 instances en fonction de vos besoins.
6. Vous déployez la macro Count à l'aide d'un CloudFormation modèle. Cette macro fournit une propriété Count pour les CloudFormation ressources afin que vous puissiez facilement spécifier plusieurs ressources du même type.
7. Vous mettez à jour le nom de la macro dans le CloudFormation `ec2-provisioning.yaml` fichier et vous déployez la pile.
8. L'administrateur met à jour le `ec2-provisioning.yaml` fichier en fonction des besoins et lance la pile.
9. Le modèle déploie EC2 des instances avec l'application UiPath Studio.

Outils

Services AWS

- AWS vous CloudFormation aide à modéliser et à gérer les ressources d'infrastructure de manière automatisée et sécurisée.
- Amazon vous CloudWatch aide à observer et à surveiller les ressources et les applications sur AWS, sur site et sur d'autres clouds.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul sécurisée et redimensionnable dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- EC2 Image Builder simplifie la création, le test et le déploiement de machines virtuelles et d'images de conteneurs à utiliser sur AWS ou sur site.
- Amazon vous EventBridge aide à créer des applications pilotées par des événements à grande échelle sur AWS, sur des systèmes existants ou sur des applications SaaS (Software as a Service).
- AWS Identity and Access Management (IAM) vous permet de contrôler en toute sécurité l'accès aux ressources AWS. Avec IAM, vous pouvez gérer de manière centralisée les autorisations qui contrôlent les ressources AWS auxquelles les utilisateurs peuvent accéder. Vous pouvez utiliser IAM pour contrôler les personnes qui s’authentifient (sont connectées) et sont autorisées (disposent d’autorisations) à utiliser des ressources.
- AWS Lambda est un service de calcul sans serveur piloté par les événements qui vous permet d'exécuter du code pour pratiquement n'importe quel type d'application ou de service principal sans

provisionner ni gérer de serveurs. Vous pouvez appeler des fonctions Lambda à partir de plus de 200 services AWS et applications SaaS, et ne payer que pour ce que vous utilisez.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Systems Manager Agent (SSM Agent) aide Systems Manager à mettre à jour, gérer et configurer des EC2 instances, des appareils périphériques, des serveurs sur site et des machines virtuelles ()VMs.

Référentiels de code

Le code de ce modèle est disponible dans la configuration du bot GitHub UiPath RPA à l'aide CloudFormation du référentiel. Le modèle utilise également une macro disponible dans le référentiel AWS CloudFormation Macros.

Bonnes pratiques

- AWS publie un nouveau Windows AMIs chaque mois. Ils contiennent les derniers correctifs, pilotes et agents de lancement du système d'exploitation. Nous vous recommandons d'utiliser l'AMI la plus récente lorsque vous lancez de nouvelles instances ou lorsque vous créez vos propres images personnalisées.
- Appliquez tous les correctifs de sécurité Windows ou Linux disponibles lors de la création d'images.

Épopées

Déployer un pipeline d'images pour l'image de base

Tâche	Description	Compétences requises
Configurez un pipeline EC2 Image Builder.	1. Clonez la configuration du bot UiPath RPA à l'aide du CloudFormation référentiel ou téléchargez le `ec2-image-builder.yaml` modèle depuis le référentiel. 2. Connectez-vous à l'AWS Management Console, puis	AWS DevOps

Tâche	Description	Compétences requises
	ouvrez la CloudFormation console AWS. 3. Sélectionnez Créer la pile. 4. Dans la section Spécifier un modèle, sélectionnez Charger un modèle de fichier. 5. Localisez et téléchargez le `ec2-image-builder.yaml` modèle depuis votre ordinateur, puis choisissez Next. 6. Fournissez des paramètres d'entrée pour votre pile ou acceptez les valeurs par défaut. Choisissez Suivant. **Note** Le nombre et les valeurs des paramètres peuvent varier en fonction de vos valeurs d'entrée. 7. Configurez éventuellement les options de pile, puis choisissez Next. 8. Vérifiez les détails de votre stack. 9. À la fin de l'écran, cochez la case pour confirmer	

Tâche	Description	Compétences requises
	les fonctionnalités, puis choisissez Soumettre. 10. Surveillez la progression de la pile. Lorsque le statut est `CREATE_COMPLETE` défini, le déploiement est prêt.	
Afficher les paramètres EC2 d'Image Builder.	Les paramètres EC2 d'Image Builder incluent la configuration de l'infrastructure, les paramètres de distribution et les paramètres d'analyse de sécurité. Pour consulter les paramètres, procédez comme suit : 1. Ouvrez la console EC2 Image Builder. 2. Dans le volet de navigation, accédez aux différents paramètres d'Image Builder. **Note** Il est recommandé d'apporter des mises à jour à EC2 Image Builder uniquement via le CloudFormation modèle.	AWS DevOps

Tâche	Description	Compétences requises
Affichez le pipeline d'images.	Pour afficher le pipeline d'images déployé, procédez comme suit : 1. Sur la console EC2 Image Builder, choisissez Image pipelines dans le volet de navigation. 2. Sélectionnez le pipeline d'images que vous avez créé. 3. Consultez les détails de configuration des images de sortie, de la recette des images, de la configura tion de l'infrastructure, des paramètres de distribution, EventBridge des règles Amazon et des balises.	AWS DevOps

Tâche	Description	Compétences requises
Afficher les journaux d'Image Builder.	EC2 Les journaux Image Builder sont agrégés en groupes de CloudWatch journaux. Pour consulter les journaux, procédez comme suit CloudWatch : 1. Ouvrez la CloudWatch console. 2. Dans le panneau de navigation de gauche, choisissez Logs (Journaux), Log groups (Groupes de journaux). 3. Choisissez le nom du groupe de journaux. EC2 Les journaux Image Builder sont agrégés dans le groupe de journaux `/aws/imagebuilder/XXX` . 4. Vérifiez les derniers journaux du flux de journal correspondant pour détecter toute erreur rencontrée lors de l'exécution du pipeline d'images. EC2 Les journaux Image Builder sont également stockés dans un compartiment S3. Pour consulter les journaux contenus dans le compartiment :	AWS DevOps

Tâche	Description	Compétences requises
	1. Ouvrez la console Amazon S3. 2. Dans la liste Compartiments, sélectionnez le nom de votre compartiment. Les journaux sont agrégés dans le compartiment S3`<stack-name>-XXXXXX` .	
Téléchargez le UiPath fichier dans un compartiment S3.	1. Téléchargez le `.msi` fichier pour UiPath Studio à partir de l'emplacement https://download.uipath.com/UiPathStudioCommunity.msi. 2. Chargez le fichier dans un compartiment S3. 3. Mettez à jour le nom du compartiment et la clé de fichier dans le `ec2-image-builder.yaml` modèle, dans la section des données utilisateur, ligne 310.	AWS DevOps

Déployez et testez la macro Count

Tâche	Description	Compétences requises
Déployez la macro Count.	1. Clonez ou téléchargez la CloudFormation macro Count. 2. Accédez au dossier `Count`.	DevOps ingénieur

Tâche	Description	Compétences requises
	3. Vous aurez besoin d'un compartiment S3 pour stocker les CloudFormation artefacts. Si vous n'avez pas encore de compartiment S3, créez-en un avec ce nom`aws s3 mb s3://<bucket name>` .	

	4. Package du modèle de macro Count. Le modèle utilise le modèle d'application sans serveur (SAM) AWS, il doit donc être transformé avant de pouvoir le déployer.
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket <your bucket name here> \ --output-template-file packaged.yaml`
	Par exemple :
	`aws cloudformation package \ --template-file template.yaml \ --s3-bucket count-macro-ec2 \ --output-template-file packaged.yaml`	

Tâche	Description	Compétences requises
	5. Déployez le modèle empaqueté pour créer une CloudFormation pile. `aws cloudformation deploy \ --stack-name Count-macro \ --template-file packaged.yaml \ --capabilities CAPABILITY_IAM` Si vous souhaitez utiliser la console, suivez les instructions de l'épopée précédente ou de la CloudFormation documentation.	
Testez la macro Count.	Pour tester les fonctionnalités de la macro, essayez de lancer l'exemple de modèle fourni avec la macro. `aws cloudformation deploy \ --stack-name Count-test \ --template-file test.yaml \ --capabilities CAPABILITY_IAM`	DevOps ingénieur

Déployez la CloudFormation pile pour approvisionner les instances avec l'image personnalisée

Tâche	Description	Compétences requises
Déployez le modèle de EC2 provisionnement Amazon.	Pour déployer EC2 Image Pipeline à l'aide de CloudFormation : 1. Téléchargez le `ec2-provisioning.yaml` modèle depuis le GitHub référentiel ou localisez-le sur votre ordinateur si vous l'avez cloné. 2. Ouvrez la CloudFormation console. 3. Répétez les étapes du premier épisode (ou suivez les instructions de la CloudFormation documentation) pour effectuer le déploiement`ec2-provisioning.yaml` .	AWS DevOps
Consultez les EC2 paramètres Amazon.	Les EC2 paramètres Amazon incluent la sécurité, la mise en réseau, le stockage, les vérifications d'état, la surveillance et les configurations des balises. Pour consulter ces configurations, procédez comme suit : 1. Ouvrez la EC2 console Amazon. 2. Dans le volet de navigation, choisissez Instances, puis	AWS DevOps

Tâche	Description	Compétences requises
	sélectionnez l' EC2 instance créée par le modèle de EC2 provisionnement Amazon. 3. Dans le résumé de l'instance, sélectionnez les onglets pour afficher les EC2 paramètres Amazon correspondants.	

Tâche	Description	Compétences requises
Consultez le CloudWatch tableau de bord.	1. Ouvrez la CloudWatch console. 2. Dans le panneau de navigation, choisissez Dashboards (Tableaux de bord). 3. Choisissez le tableau de bord qui porte le nom de votre stack. **Note** Une fois que vous avez approvisionné la pile, il faut du temps pour remplir le tableau de bord avec des métriques. Le tableau de bord fournit les indicateurs suivants : `CPUUtilization DiskUtilization MemoryUtilization ,,NetworkIn ,NetworkOut ,StatusCheckFailed .`	AWS DevOps

Tâche	Description	Compétences requises
Consultez les métriques personnalisées relatives à l'utilisation de la mémoire et du disque.	1. Sur la CloudWatch console, sélectionnez Tableaux de bord. 2. Dans le panneau de navigation, sélectionnez Métriques, Toutes les métriques. 3. Choisissez Espaces de noms personnalisés, CWAgent.	AWS DevOps
Afficher les alarmes relatives à l'utilisation de la mémoire et du disque.	1. Sur la CloudWatch console, dans le volet de navigation, choisissez Dashboards. 2. Sélectionnez All alarms (Toutes les alarmes).	AWS DevOps
Vérifiez la règle du cycle de vie des instantanés.	1. Ouvrez la EC2 console Amazon. 2. Dans le panneau de navigation, sélection nez Lifecycle Manager (Gestionnaire de cycle de vie). 3. Vérifiez les paramètres du cycle de vie de l'AMI.	AWS DevOps

Supprimer l'environnement (facultatif)

Tâche	Description	Compétences requises
Supprimez les piles.	Lorsque votre PoC ou votre projet pilote sera terminé, nous vous recommandons de	AWS DevOps

Tâche	Description	Compétences requises
	supprimer les piles que vous avez créées pour vous assurer que ces ressources ne vous seront pas facturées. 1. Ouvrez la CloudFormation console AWS. 2. Dans le volet de navigation, choisissez Stacks, puis sélectionnez l'une ou les deux piles que vous souhaitez supprimer précédemment. La pile doit être en cours d'exécution. 3. Dans le volet des détails de la pile, choisissez Supprimer. 4. À l'invite, choisissez Supprimer la pile. **Important** L'opération de suppression de la pile ne peut pas être arrêtée une fois qu'elle a commencé. La pile passe à l'état `DELETE_IN_PROGRESS` . Si la suppression échoue, la pile sera dans `DELETE_FA`	

Tâche	Description	Compétences requises
	`ILED` cet état. Pour trouver des solutions, consultez la section Supprimer les échecs de pile dans la documentation de CloudFormation résolution des problèmes d'AWS. Pour plus d'informations sur la protection contre la suppressi on accidentelle de piles, consultez la section Protection d'une pile contre la suppressi on dans la CloudFormation documentation AWS.	

Résolution des problèmes

Problème	Solution
Lorsque vous déployez le modèle de EC2 provisioning Amazon, le message d'erreur suivant s'affiche : Réponse mal formée reçue de la part de transform 123xxxx : :Count.	Il s'agit d'un problème connu. (Consultez la solution personnalisée et le PR dans le référentiel de CloudFormation macros AWS.) Pour résoudre ce problème, ouvrez la console AWS Lambda et mettez-la à jour `index.py` avec le contenu du GitHub référentiel.

Ressources connexes

GitHub référentiels

- UiPath Configuration du bot RPA à l'aide de CloudFormation
- CloudFormation Macro de comptage

Références AWS

- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation)
- Résolution des problèmes CloudFormation (CloudFormation documentation)
- Surveillez les métriques relatives à la mémoire et au disque pour EC2 les instances Amazon (EC2 documentation Amazon)
- Comment puis-je utiliser l' CloudWatch agent pour consulter les mesures de Performance Monitor sur un serveur Windows ? (AWS Re:Publier un article)

Références supplémentaires

- UiPath documentation
- Configuration du nom d'hôte dans une SysPreped AMI (article de blog de Brian Beach)
- Comment faire en sorte que Cloudformation retraite un modèle à l'aide d'une macro lorsque les paramètres changent ? (Stack Overflow)

Configuration d'une PeopleSoft architecture à haute disponibilité sur AWS

Créée par Ramanathan Muralidhar (AWS)

Récapitulatif

Lorsque vous migrez vos PeopleSoft charges de travail vers AWS, la résilience est un objectif important. Cela garantit que votre PeopleSoft application est toujours hautement disponible et capable de se remettre rapidement en cas de panne.

Ce modèle fournit une architecture pour vos PeopleSoft applications sur AWS afin de garantir une haute disponibilité (HA) au niveau du réseau, de l'application et de la base de données. Il utilise une base de données Amazon Relational Database Service (Amazon RDS) pour Oracle ou Amazon RDS for SQL Server pour le niveau de base de données. Cette architecture inclut également des services AWS tels qu'Amazon Route 53, les instances Linux Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Storage (Amazon EBS), Amazon Elastic File System (Amazon EFS) et un Application Load Balancer. Elle est évolutive.

Oracle PeopleSoft fournit une suite d'outils et d'applications pour la gestion des effectifs et d'autres opérations commerciales.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un PeopleSoft environnement doté des licences nécessaires pour le configurer sur AWS
- Un cloud privé virtuel (VPC) configuré dans votre compte AWS avec les ressources suivantes :
  - Au moins deux zones de disponibilité
  - Un sous-réseau public et trois sous-réseaux privés dans chaque zone de disponibilité
  - Une passerelle NAT et une passerelle Internet
  - Tables de routage pour chaque sous-réseau afin d'acheminer le trafic
  - Listes de contrôle d'accès réseau (réseau ACLs) et groupes de sécurité définis pour garantir la sécurité de l' PeopleSoft application conformément aux normes de votre entreprise

Limites

- Ce modèle fournit une solution de haute disponibilité (HA). Il ne prend pas en charge les scénarios de reprise après sinistre (DR). Dans les rares cas où l'ensemble de la région AWS pour l'implémentation HA tombe en panne, l'application deviendra indisponible.

Versions du produit

- PeopleSoft applications exécutant PeopleTools 8.52 et versions ultérieures

Architecture

Architecture cible

Les interruptions ou pannes de votre application de PeopleSoft production ont un impact sur la disponibilité de l'application et perturbent considérablement votre activité.

Nous vous recommandons de concevoir votre application PeopleSoft de production de manière à ce qu'elle soit toujours hautement disponible. Vous pouvez y parvenir en éliminant les points de défaillance uniques, en ajoutant des points de croisement ou de basculement fiables et en détectant les défaillances. Le schéma suivant illustre une architecture HA pour PeopleSoft AWS.

Ce déploiement d'architecture utilise Amazon RDS for Oracle comme base PeopleSoft de données, EC2 ainsi que des instances exécutées sous Red Hat Enterprise Linux (RHEL). Vous pouvez également utiliser Amazon RDS for SQL Server comme base de données Peoplesoft.

Cette architecture contient les composants suivants :

- Amazon Route 53 est utilisé comme serveur de noms de domaine (DNS) pour acheminer les demandes depuis Internet vers l' PeopleSoft application.
- AWS WAF vous aide à vous protéger contre les exploits Web courants et les robots susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de consommer des ressources excessives. AWS Shield Advanced (non illustré) fournit une protection beaucoup plus étendue.
- Un Application Load Balancer équilibre la charge du trafic HTTP et HTTPS grâce à un routage avancé des requêtes ciblant les serveurs Web.
- Les serveurs Web, les serveurs d'applications, les serveurs de planificateur de processus et les serveurs Elasticsearch qui prennent en charge l' PeopleSoft application s'exécutent dans plusieurs zones de disponibilité et utilisent Amazon Auto Scaling. EC2

- La base de données utilisée par l' PeopleSoft application s'exécute sur Amazon RDS dans une configuration multi-AZ.
- Le partage de fichiers utilisé par l' PeopleSoft application est configuré sur Amazon EFS et est utilisé pour accéder aux fichiers entre les instances.
- Les Amazon Machine Images (AMI) sont utilisées par Amazon EC2 Auto Scaling pour garantir que les PeopleSoft composants sont clonés rapidement en cas de besoin.
- Les passerelles NAT connectent les instances d'un sous-réseau privé à des services extérieurs à votre VPC et garantissent que les services externes ne peuvent pas établir de connexion avec ces instances.
- La passerelle Internet est un composant VPC à échelle horizontale, redondant et hautement disponible qui permet la communication entre votre VPC et Internet.
- Les hôtes bastions du sous-réseau public permettent d'accéder aux serveurs du sous-réseau privé depuis un réseau externe, tel qu'Internet ou un réseau local. Les hôtes Bastion fournissent un accès contrôlé et sécurisé aux serveurs des sous-réseaux privés.

Détails de l'architecture

La PeopleSoft base de données est hébergée dans une base de données Amazon RDS for Oracle (ou Amazon RDS for SQL Server) dans une configuration multi-AZ. La fonctionnalité Amazon RDS Multi-AZ reproduit les mises à jour de base de données sur deux zones de disponibilité afin d'accroître la durabilité et la disponibilité. Amazon RDS bascule automatiquement vers la base de données de secours pour les opérations de maintenance planifiées et les interruptions imprévues.

Le PeopleSoft Web et le niveau intermédiaire sont installés sur les EC2 instances. Ces instances sont réparties sur plusieurs zones de disponibilité et liées par un groupe Auto Scaling. Cela garantit que ces composants sont toujours hautement disponibles. Un nombre minimum d'instances requises est maintenu afin de garantir que l'application est toujours disponible et qu'elle peut évoluer en cas de besoin.

Nous vous recommandons d'utiliser un type d' EC2 instance de génération actuelle pour les EC2 instances OEM. Les types d'instances de la génération actuelle, tels que les instances basées sur le système AWS Nitro, prennent en charge les machines virtuelles matérielles (HVMs). Les HVM AMIs sont nécessaires pour tirer parti d'une mise en réseau améliorée, et ils offrent également une sécurité accrue. Les EC2 instances qui font partie de chaque groupe Auto Scaling utilisent leur propre AMI lors du remplacement ou du dimensionnement des instances. Nous vous recommandons de sélectionner les types d' EC2 instances en fonction de la charge que vous souhaitez que votre PeopleSoft application gère et des valeurs minimales recommandées par Oracle pour votre

PeopleSoft application et votre PeopleTools version. Pour plus d'informations sur les exigences matérielles et logicielles, consultez le site Web de support d'Oracle.

Le PeopleSoft Web et le niveau intermédiaire partagent un montage Amazon EFS pour partager les rapports, les fichiers de données et (si nécessaire) le `PS_HOME` répertoire. Amazon EFS est configuré avec des cibles de montage dans chaque zone de disponibilité pour des raisons de performances et de coûts.

Un Application Load Balancer est configuré pour prendre en charge le trafic qui accède à l' PeopleSoft application et pour équilibrer la charge du trafic entre les serveurs Web des différentes zones de disponibilité. Un Application Load Balancer est un périphérique réseau qui fournit une haute disponibilité dans au moins deux zones de disponibilité. Les serveurs Web distribuent le trafic aux différents serveurs d'applications en utilisant une configuration d'équilibrage de charge. L'équilibrage de charge entre le serveur Web et le serveur d'applications garantit une répartition uniforme de la charge entre les instances et permet d'éviter les blocages et les interruptions de service dus à des instances surchargées.

Amazon Route 53 est utilisé comme service DNS pour acheminer le trafic vers l'Application Load Balancer depuis Internet. Route 53 est un service Web DNS hautement disponible et évolutif.

Détails du HA

- Bases de données : la fonctionnalité multi-AZ d'Amazon RDS gère deux bases de données dans plusieurs zones de disponibilité avec réplication synchrone. Cela crée un environnement hautement disponible avec basculement automatique. Amazon RDS détecte les événements de basculement et lance un basculement automatique lorsque ces événements se produisent. Vous pouvez également lancer un basculement manuel via l'API Amazon RDS. Pour une explication détaillée, consultez le billet de blog Amazon RDS Under The Hood : Multi-AZ. Le basculement est fluide et l'application se reconnecte automatiquement à la base de données lorsque cela se produit. Cependant, toute tâche du planificateur de processus pendant le basculement génère des erreurs et doit être soumise à nouveau.
- PeopleSoft serveurs d'applications : les serveurs d'applications sont répartis sur plusieurs zones de disponibilité et un groupe Auto Scaling est défini pour eux. En cas de défaillance d'une instance, le groupe Auto Scaling la remplace immédiatement par une instance saine clonée à partir de l'AMI du modèle de serveur d'applications. Plus précisément, le jolt pooling est activé. Ainsi, lorsqu'une instance de serveur d'applications tombe en panne, les sessions basculent automatiquement vers un autre serveur d'applications, et le groupe Auto Scaling lance automatiquement une autre instance, ouvre le serveur d'applications et l'enregistre dans le montage Amazon EFS. Le

serveur d'applications nouvellement créé est automatiquement ajouté aux serveurs Web à l'aide du `PSSTRSETUP.SH` script sur les serveurs Web. Cela garantit que le serveur d'applications est toujours hautement disponible et qu'il se rétablit rapidement en cas de panne.

- Planificateurs de processus : les serveurs des planificateurs de processus sont répartis sur plusieurs zones de disponibilité et un groupe Auto Scaling leur est défini. En cas de défaillance d'une instance, le groupe Auto Scaling la remplace immédiatement par une instance saine clonée à partir de l'AMI du modèle de serveur de planificateur de processus. Plus précisément, lorsqu'une instance du planificateur de processus tombe en panne, le groupe Auto Scaling lance automatiquement une autre instance et ouvre le planificateur de processus. Toutes les tâches en cours d'exécution lorsque l'instance a échoué doivent être soumises à nouveau. Cela garantit que le planificateur de processus est toujours hautement disponible et qu'il se rétablit rapidement en cas de panne.
- Serveurs Elasticsearch : un groupe Auto Scaling est défini pour les serveurs Elasticsearch. En cas de défaillance d'une instance, le groupe Auto Scaling la remplace immédiatement par une instance saine clonée à partir de l'AMI du modèle de serveur Elasticsearch. Plus précisément, lorsqu'une instance Elasticsearch tombe en panne, l'Application Load Balancer qui répond aux demandes détecte la défaillance et arrête de lui envoyer du trafic. Le groupe Auto Scaling lance automatiquement une autre instance et fait apparaître l'instance Elasticsearch. Lorsque l'instance Elasticsearch est sauvegardée, l'Application Load Balancer détecte qu'elle est saine et recommence à lui envoyer des requêtes. Cela garantit que le serveur Elasticsearch est toujours hautement disponible et qu'il se rétablit rapidement en cas de panne.
- Serveurs Web : un groupe Auto Scaling est défini pour les serveurs Web. En cas de défaillance d'une instance, le groupe Auto Scaling la remplace immédiatement par une instance saine clonée à partir de l'AMI du modèle de serveur Web. Plus précisément, lorsqu'une instance de serveur Web tombe en panne, l'Application Load Balancer qui répond aux demandes détecte la défaillance et arrête de lui envoyer du trafic. Le groupe Auto Scaling lance automatiquement une autre instance et fait apparaître l'instance du serveur Web. Lorsque l'instance du serveur Web est sauvegardée, l'Application Load Balancer détecte qu'elle est saine et recommence à lui envoyer des requêtes. Cela garantit que le serveur Web est toujours hautement disponible et qu'il se rétablit rapidement en cas de panne.

Outils

Services AWS

- Les équilibreurs de charge des applications distribuent le trafic applicatif entrant sur plusieurs cibles, telles que EC2 les instances, dans plusieurs zones de disponibilité.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.

Bonnes pratiques

Bonnes pratiques opérationnelles

- Lorsque vous utilisez PeopleSoft AWS, utilisez Route 53 pour acheminer le trafic depuis Internet et localement. Utilisez l'option failover pour rediriger le trafic vers le site de reprise après sinistre (DR) si l'instance de base de données principale n'est pas disponible.
- Utilisez toujours un Application Load Balancer devant l' PeopleSoft environnement. Cela garantit l'équilibrage de charge du trafic vers les serveurs Web de manière sécurisée.
- Dans les paramètres du groupe cible Application Load Balancer, assurez-vous que l'adhérence est activée à l'aide d'un cookie généré par l'équilibreur de charge.

> **Note**
>
> Vous devrez peut-être utiliser un cookie basé sur une application si vous utilisez l'authentification unique (SSO) externe. Cela garantit la cohérence des connexions entre les serveurs Web et les serveurs d'applications.

- Pour une application PeopleSoft de production, le délai d'inactivité de l'Application Load Balancer doit correspondre à celui défini dans le profil Web que vous utilisez. Cela empêche les sessions utilisateur d'expirer au niveau de la couche d'équilibrage de charge.
- Pour une application PeopleSoft de production, définissez le taux de recyclage du serveur d'applications sur une valeur qui minimise les fuites de mémoire.

- Si vous utilisez une base de données Amazon RDS pour votre application de PeopleSoft production, comme décrit dans ce modèle, exécutez-la au format Multi-AZ pour une haute disponibilité.
- Si votre base de données est exécutée sur une EC2 instance de votre application PeopleSoft de production, assurez-vous qu'une base de données de secours est exécutée sur une autre zone de disponibilité pour garantir une haute disponibilité.
- Pour la reprise après sinistre, assurez-vous que votre base de données ou EC2 instance Amazon RDS dispose d'une instance de secours configurée dans une région AWS distincte de celle de la base de données de production. Cela garantit qu'en cas de sinistre dans la région, vous pouvez transférer l'application vers une autre région.
- Pour la reprise après sinistre, utilisez Amazon Elastic Disaster Recovery pour configurer les composants au niveau de l'application dans une région distincte de celle des composants de production. Cela garantit qu'en cas de sinistre dans la région, vous pouvez transférer l'application vers une autre région.
- Utilisez Amazon EFS (pour les exigences d'E/S modérées) ou Amazon FSx (pour les exigences d'E/S élevées) pour stocker vos PeopleSoft rapports, pièces jointes et fichiers de données. Cela garantit que le contenu est stocké dans un emplacement central et qu'il est accessible depuis n'importe quel endroit de l'infrastructure.
- Utilisez Amazon CloudWatch (de base et détaillé) pour surveiller les ressources du cloud AWS utilisées par votre PeopleSoft application en temps quasi réel. Cela garantit que vous êtes immédiatement alerté des problèmes et que vous pouvez les résoudre rapidement avant qu'ils n'affectent la disponibilité de l'environnement.
- Si vous utilisez une base de données Amazon RDS comme base de données, utilisez Enhanced Monitoring. PeopleSoft Cette fonctionnalité permet d'accéder à plus de 50 indicateurs, notamment le processeur, la mémoire, les E/S du système de fichiers et les E/S du disque.
- Utilisez AWS CloudTrail pour surveiller les appels d'API sur les ressources AWS utilisées par votre PeopleSoft application. Cela vous permet d'effectuer une analyse de sécurité, un suivi des modifications des ressources et un audit de conformité.

Bonnes pratiques de sécurité

- Pour protéger votre PeopleSoft application contre les exploits courants tels que l'injection SQL ou le cross-site scripting (XSS), utilisez AWS WAF. Envisagez d'utiliser AWS Shield Advanced pour des services de détection et d'atténuation personnalisés.

- Ajoutez une règle à l'Application Load Balancer pour rediriger automatiquement le trafic du protocole HTTP vers le protocole HTTPS afin de sécuriser votre PeopleSoft application.
- Configurez un groupe de sécurité distinct pour l'Application Load Balancer. Ce groupe de sécurité doit autoriser uniquement le trafic entrant HTTPS/HTTP et aucun trafic sortant. Cela garantit que seul le trafic prévu est autorisé et contribue à sécuriser votre application.
- Utilisez des sous-réseaux privés pour les serveurs d'applications, les serveurs Web et les bases de données, et utilisez des passerelles NAT pour le trafic Internet sortant. Cela garantit que les serveurs qui prennent en charge l'application ne sont pas accessibles au public, tout en fournissant un accès public uniquement aux serveurs qui en ont besoin.
- Utilisez différents VPCs pour exécuter vos environnements PeopleSoft de production et de non-production. Utilisez AWS Transit Gateway, le peering VPC, le réseau ACLs et les groupes de sécurité pour contrôler le flux de trafic entre les VPC et, si nécessaire, votre centre de données sur site.
- Respectez le principe du moindre privilège. N'accordez l'accès aux ressources AWS utilisées par l' PeopleSoft application qu'aux utilisateurs qui en ont absolument besoin. Accordez uniquement les privilèges minimaux requis pour effectuer une tâche. Pour plus d'informations, consultez le pilier de sécurité d'AWS Well-Architected Framework.
- Dans la mesure du possible, utilisez AWS Systems Manager pour accéder aux EC2 instances utilisées par l' PeopleSoft application.

Bonnes pratiques en matière de fiabilité

- Lorsque vous utilisez un Application Load Balancer, enregistrez une cible unique pour chaque zone de disponibilité activée. Cela rend l'équilibreur de charge le plus efficace possible.
- Nous vous recommandons d'en utiliser trois distinctes URLs pour chaque environnement de PeopleSoft production : une URL pour accéder à l'application, une pour servir le courtier d'intégration et une pour consulter les rapports. Dans la mesure du possible, chaque URL doit disposer de ses propres serveurs Web et serveurs d'applications dédiés. Cette conception contribue à renforcer la sécurité de votre PeopleSoft application, car chaque URL possède une fonctionnalité distincte et un accès contrôlé. Cela minimise également l'ampleur de l'impact en cas de défaillance des services sous-jacents.
- Nous vous recommandons de configurer des contrôles de santé sur les groupes cibles de l'équilibreur de charge pour votre PeopleSoft application. Les contrôles de santé doivent être effectués sur les serveurs Web plutôt que sur les EC2 instances qui exécutent ces serveurs. Cela

garantit que si le serveur Web tombe en panne ou si l' EC2 instance qui héberge le serveur Web tombe en panne, l'Application Load Balancer reflète correctement ces informations.

- Pour une application PeopleSoft de production, nous vous recommandons de répartir les serveurs Web sur au moins trois zones de disponibilité. Cela garantit que l' PeopleSoft application est toujours hautement disponible même si l'une des zones de disponibilité tombe en panne.
- Pour une application PeopleSoft de production, activez jolt pooling (`joltPooling=true`). Cela garantit que votre application bascule vers un autre serveur d'applications si un serveur est en panne pour des raisons de correction ou en raison d'une défaillance d'une machine virtuelle.
- Pour une application PeopleSoft de production, définissez cette `DynamicConfigReload` valeur sur 1. Ce paramètre est pris en charge dans les PeopleTools versions 8.52 et ultérieures. Il ajoute de nouveaux serveurs d'applications au serveur Web de manière dynamique, sans redémarrer les serveurs.
- Pour minimiser les temps d'arrêt lorsque vous appliquez des PeopleTools correctifs, utilisez la méthode de déploiement bleu/vert pour les configurations de lancement de votre groupe Auto Scaling pour le Web et les serveurs d'applications. Pour plus d'informations, consultez le livre blanc Présentation des options de déploiement sur AWS.
- Utilisez AWS Backup pour sauvegarder votre PeopleSoft application sur AWS. AWS Backup est un service rentable, entièrement géré et basé sur des politiques qui simplifie la protection des données à grande échelle.

Bonnes pratiques en matière de performances

- Mettez fin au protocole SSL au niveau de l'Application Load Balancer pour optimiser les performances de l' PeopleSoft environnement, sauf si votre entreprise a besoin d'un trafic chiffré dans l'ensemble de l'environnement.
- Créez des points de terminaison VPC d'interface pour les services AWS tels qu'Amazon Simple Notification Service (Amazon SNS) CloudWatchafin que le trafic soit toujours interne. Cette solution est rentable et contribue à la sécurité de votre application.

Bonnes pratiques en matière d'optimisation des coûts

- Marquez toutes les ressources utilisées par votre PeopleSoft environnement et activez les balises de répartition des coûts. Ces balises vous aident à visualiser et à gérer les coûts de vos ressources.

- Pour une application PeopleSoft de production, configurez des groupes Auto Scaling pour les serveurs Web et les serveurs d'applications. Cela permet de maintenir un nombre minimal de serveurs Web et d'applications pour prendre en charge votre application. Vous pouvez utiliser les politiques de groupe Auto Scaling pour augmenter ou diminuer les serveurs selon les besoins.
- Utilisez les alarmes de facturation pour recevoir des alertes lorsque les coûts dépassent le seuil budgétaire que vous spécifiez.

Bonnes pratiques en matière de durabilité

- Utilisez l'infrastructure en tant que code (IaC) pour gérer vos PeopleSoft environnements. Cela vous permet de créer des environnements cohérents et de garder le contrôle des modifications.

Épopées

Migrez votre PeopleSoft base de données vers Amazon RDS

Tâche	Description	Compétences requises
Créez un groupe de sous-réseaux de base de données.	Sur la console Amazon RDS, dans le volet de navigation, choisissez Subnet groups, puis créez un groupe de sous-réseaux de base de données Amazon RDS avec des sous-réseaux dans plusieurs zones de disponibilité. Cela est nécessaire pour que la base de données Amazon RDS s'exécute dans une configuration multi-AZ.	Administrateur du cloud
Créez la base de données Amazon RDS.	Créez une base de données Amazon RDS dans une zone de disponibilité de la région AWS que vous avez sélectionnée pour l'environnement PeopleSoft HA. Lorsque vous	Administrateur cloud, administrateur de base de données Oracle

Tâche	Description	Compétences requises
	créez la base de données Amazon RDS, assurez-vous de sélectionner l'option Multi-AZ (Créer une instance de secours) et le groupe de sous-réseaux de base de données que vous avez créé à l'étape précédente. Pour plus d'informations, consultez la documentation Amazon RDS.	
Migrez votre PeopleSoft base de données vers Amazon RDS.	Migrez votre PeopleSoft base de données existante vers la base de données Amazon RDS à l'aide d'AWS Database Migration Service (AWS DMS). Pour plus d'informations, consultez la documentation AWS DMS et le billet de blog AWS intitulé Migration de bases de données Oracle avec un temps d'arrêt quasi nul à l'aide d'AWS DMS.	Administrateur cloud, PeopleSoft DBA

Configuration de votre système de fichiers Amazon EFS

Tâche	Description	Compétences requises
Créez un système de fichiers.	Sur la console Amazon EFS, créez un système de fichiers et montez des cibles pour chaque zone de disponibilité. Pour obtenir des instructions, consultez la documentation Amazon EFS. Lorsque le	Administrateur du cloud

Tâche	Description	Compétences requises
	système de fichiers a été créé, notez son nom DNS. Vous utiliserez ces informations lors du montage du système de fichiers.	

Configurez votre PeopleSoft application et votre système de fichiers

Tâche	Description	Compétences requises
Lancez une EC2 instance.	Lancez une EC2 instance pour votre PeopleSoft application. Pour obtenir des instructions, consultez la EC2 documentation Amazon. • Pour Nom, saisissez `APP_TEMPLATE` . • Pour les images du système d'exploitation, choisissez Red Hat. • Dans Type d'instance, choisissez le type d'instance adapté à votre PeopleSoft application. Pour plus d'informations, consultez la section Détails de l'architecture dans la section Architecture.	Administrateur du cloud, PeopleSoft administrateur
Installez PeopleSoft sur l'instance.	Installez votre PeopleSoft application et PeopleTools sur l' EC2 instance que vous avez créée. Pour obtenir	Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises
	des instructions, consultez la documentation Oracle.	
Créez le serveur d'applications.	Créez le serveur d'applications pour le modèle d'AMI et assurez-vous qu'il se connecte correctement à la base de données Amazon RDS.	Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises

Montage d’un système de fichiers Amazon EFS	Connectez-vous à l' EC2 instance en tant qu'utilis ateur root et exécutez les commandes suivantes pour monter le système de fichiers Amazon EFS dans un dossier appelé PSFTMNT sur le serveur.
	`sudo su -`
	`mkdir /psftmnt`
	`cat /etc/fstab`
	Ajoutez la ligne suivante au `/etc/fstab` fichier. Utilisez le nom DNS que vous avez indiqué lors de la création du système de fichiers.
	`fs-09e064308f11453 88.efs.us-east-1.a mazonaws.com:/ / psftmnt nfs4 nfsvers=4 .1,rsize=1048576,w size=1048576,hard, timeo=600,retrans= 2,noresvport,_netdev 0 0`
	`mount -a`
		Administrateur du cloud, PeopleSoft administrateur

Vérifiez les autorisations.	Assurez-vous que le PSFTMNT dossier dispose des autorisat ions appropriées afin que l' PeopleSoft utilisateur puisse y accéder correctement.	Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises
Créez des instances supplémentaires.	Répétez les étapes précédentes de cette épopée pour créer des instances de modèles pour le planificateur de processus, le serveur Web et le serveur Elasticsearch. Nommez ces instances `PRCS_TEMPLATE` `WEB_TEMPLATE` , et`SRCH_TEMPLATE` . Pour le serveur Web, définissez `joltPooling=true` et`DynamicConfigReload=1` .	Administrateur du cloud, PeopleSoft administrateur

Création de scripts pour configurer les serveurs

Tâche	Description	Compétences requises

Créez un script pour installer le serveur d'applications.	Dans l' EC2 `APP_TEMPLATE` instance Amazon, en tant qu' PeopleSoft utilisateur, créez le script suivant. Nommez-le `appstart.sh` et placez-le dans le `PS_HOME` répertoire. Vous allez utiliser ce script pour ouvrir le serveur d'applications et enregistrer le nom du serveur sur le support Amazon EFS.
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/.profile.`
		PeopleSoft administrateur

Tâche	Description	Compétences requises

	`psadmin -c configure -d HCMDEMO`
	`psadmin -c parallelboot -d HCMDEMO`
	`touch /psftmnt/`echo $HOSTNAME`	

Créez un script pour installer le serveur du planificateur de processus.	Dans l' EC2 `PRCS_TEMPLATE` instance Amazon, en tant qu' PeopleSoft utilisateur, créez le script suivant. Nommez-le `prcsstart.sh` et placez-le dans le `PS_HOME` répertoire. Vous allez utiliser ce script pour ouvrir le serveur du planificateur de processus.
	`#!/bin/ksh`
	`. /usr/homes/hcmdemo/.profile`
	`/* The following line ensures that the process scheduler always has a unique name during replacement or scaling activity. */`
	`sed -i "s/.*PrcsServerName.*/`hostname -I | awk -F. '{print "PrcsServerName=PSUNX"$3$4}'`/" $HOME/appserv/prcs/*/psprcs.cfg`
	`psadmin -p configure -d HCMDEMO`
	`psadmin -p start -d HCMDEMO`
		PeopleSoft administrateur

Tâche	Description	Compétences requises

Créez un script pour installer le serveur Elasticsearch.	Dans l' EC2 `SRCH_TEMP LATE` instance Amazon, en tant qu'utilisateur d'Elastic search, créez le script suivant. Nommez-le `srchstart.sh` et placez-le dans le `HOME` répertoire.
	`#!/bin/ksh`
	`/* The following line ensures that the correct IP is indicated in the elasticse arch.yaml file. */`
	`sed -i "s/.*netw ork.host.*/`hostna me -I | awk '{print "host:"$0}'`/" $ES_HOME_DIR/config/ elasticsearch.yaml`
	`nohup $ES_HOME_DIR/bin/ elasticsearch &`
		PeopleSoft administrateur

Tâche	Description	Compétences requises
Créez un script pour installer le serveur Web.	Dans l' EC2 `WEB_TEMPLATE` instance Amazon, en tant qu'utilisateur du serveur Web, créez les scripts suivants dans le `HOME` répertoire. `renip.sh`: Ce script garantit que le serveur Web possède l'adresse IP correcte lorsqu'il est cloné à partir de l'AMI. `#!/bin/ksh` `hn=`hostname`` `/* On the following line, change the IP with the hostname with the hostname of the web template. */` `for text_file in `find * -type f -exec grep -l '<hostname-of-the-web-template>' {} \;`` `do` `sed -e 's/<hostname-of-the-web-template>/'$hn'/g' $text_file > temp` `mv -f temp $text_file` `done` `psstrsetup.sh` : ce script garantit que le serveur Web utilise le bon serveur IPs d'applications actuellement en cours d'exécution. Il essaie de se connecter à chaque serveur d'applications sur le	PeopleSoft administrateur

Tâche	Description	Compétences requises
	port jolt et l'ajoute au fichier de configuration. `#!/bin/ksh` `c2=""` `for ctr in `ls -1 /psftmnt/*.internal`` `do` `c1=`echo $ctr | awk -F "/" '{print $3}'`` `/* In the following lines, 9000 is the jolt port. Change it if necessary. */` `if nc -z $c1 9000 2> /dev/null; then` `if [[ $c2 = "" ]]; then` `c2="psserver="`echo $c1`":9000"` `else` `c2=`echo $c2`","`echo $c1`":9000"` `fi` `fi` `done` `webstart.sh` : Ce script exécute les deux scripts précédents et démarre les serveurs Web. `#!/bin/ksh` `/* Change the path in the following if necessary. */` `cd /usr/homes/hcmdemo` `./renip.sh` `./psstrsetup.sh`	

Tâche	Description	Compétences requises
	`webserv/peoplesoft/bin/startPIA.sh`	
Ajoutez une entrée crontab.	Dans l' EC2 `WEB_TEMPLATE` instance Amazon, en tant qu'utilisateur du serveur Web, ajoutez la ligne suivante à crontab. Modifiez l'heure et le chemin pour refléter les valeurs dont vous avez besoin. Cette entrée garantit que votre serveur Web dispose toujours des entrées de serveur d'applications correctes dans le `configuration.properties` fichier. `* * * * * /usr/homes/hcmdemo/psstrsetup.sh`	PeopleSoft administrateur

Modèles de groupe Create AMIs et Auto Scaling

Tâche	Description	Compétences requises
Créez une AMI pour le modèle de serveur d'applications.	Sur la EC2 console Amazon, créez une image AMI de l' EC2 `APP_TEMPLATE` instance Amazon. Nommez l'AMI`PSAPPSRV-SCG-VER1` . Pour obtenir des instructions, consultez la EC2 documentation Amazon.	Administrateur du cloud, PeopleSoft administrateur
Créez AMIs pour les autres serveurs.	Répétez l'étape précédent e AMIs pour créer pour le	Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises
	planificateur de processus, le serveur Elasticsearch et le serveur Web.	

Créez un modèle de lancement pour le groupe Auto Scaling du serveur d'applications.	Créez un modèle de lancement pour le groupe Auto Scaling du serveur d'applications. Nommez le modèle `PSAPPSRV_TEMPLATE`. Dans le modèle, choisissez l'AMI que vous avez créée pour l'`APP_TEMPLATE` instance. Pour obtenir des instructions, consultez la EC2 documentation Amazon.
	• Dans le modèle de lancement, sélectionnez le type d'instance en fonction de vos besoins.
	• Dans le champ Données utilisateur de la section Détails avancés, ajoutez les entrées suivantes. Assurez-vous que le chemin et les informations utilisateur sont corrects. Vous avez créé le `appstart.sh` script lors d'une étape précédente.
	`#! /bin/ksh`
	`su -c “/usr/homes/hcmdemo/appstart.sh” - hcmdemo`
		Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises

Créez un modèle de lancement pour le groupe Auto Scaling du serveur de planificateur de processus.	Répétez l'étape précédente pour créer un modèle de lancement pour le groupe Auto Scaling du serveur de planificateur de processus. Nommez le modèle`PSPRCS_TEMPLATE` . Dans le modèle, choisissez l'AMI que vous avez créée pour le planificateur de processus.
	• Dans le champ Données utilisateur de la section Détails avancés, ajoutez les entrées suivantes. Assurez-vous que le chemin et les informations utilisateur sont corrects. Vous avez créé le `prcsstart.sh` script lors d'une étape précédente.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/hcmdemo/prcssta`
	`rt.sh” - hcmdemo`
		Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises

Créez un modèle de lancement pour le groupe Auto Scaling du serveur Elasticse arch.	Répétez les étapes précédent es pour créer un modèle de lancement pour le groupe Auto Scaling du serveur Elasticsearch. Nommez le modèle`SRCH_TEMPLATE` . Dans le modèle, choisissez l'AMI que vous avez créée pour le serveur de recherche.
	• Dans le champ Données utilisateur de la section Détails avancés, ajoutez les entrées suivantes. Assurez-vous que le chemin et les informations utilisateur sont corrects. Vous avez créé le `srchstart.sh` script lors d'une étape précédente.
	`#! /bin/ksh`
	`su -c “/usr/hom`
	`es/essearch/srchst`
	`art.sh” - essearch`
		Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises

Créez un modèle de lancement pour le groupe Auto Scaling du serveur Web.	Répétez les étapes précédentes pour créer un modèle de lancement pour le groupe Auto Scaling du serveur Web. Nommez le modèle`WEB_TEMPLATE` . Dans le modèle, choisissez l'AMI que vous avez créée pour le serveur Web.
	• Dans le champ Données utilisateur de la section Détails avancés, ajoutez les entrées suivantes. Assurez-vous que le chemin et les informations utilisateur sont corrects. Vous avez créé le `webstart.sh` script lors d'une étape précédente.
	`#! /bin/ksh`
	`su -c “/usr/homes/hcmdemo/webstart.sh” - hcmdemo`
		Administrateur du cloud, PeopleSoft administrateur

Création de groupes Auto Scaling

Tâche	Description	Compétences requises
Créez un groupe Auto Scaling pour le serveur d'applications.	Sur la EC2 console Amazon, créez un groupe Auto Scaling appelé `PSAPPSRV_ASG` pour le serveur d'applications en utilisant le `PSAPPSRV_`	Administrateur du cloud, PeopleSoft administrateur

Tâche	Description	Compétences requises
	`TEMPLATE` modèle. Pour obtenir des instructions, consultez la EC2 documentation Amazon. • Sur la page Choisir les options de lancement de l'instance, sélectionnez le VPC approprié, puis sélectionnez plusieurs sous-réseaux provenant de différentes zones de disponibilité. • Sur la page Configurer les options avancées, ne sélectionnez pas d'équilibreur de charge. • Sur la page Configurer la taille du groupe et les politiques de dimensionnement, choisissez les paramètres en fonction de la charge pour laquelle vous souhaitez concevoir votre système et de l'utilisation d'une politique de dimensionnement. Nous vous recommandons de définir la capacité minimale souhaitée sur 2 au minimum afin qu'au moins une instance soit disponible pour traiter le trafic à tout moment. Pour plus d'informations sur les politiques d'Auto	

Tâche	Description	Compétences requises
	Scaling, consultez la EC2 documentation Amazon.	
Créez des groupes Auto Scaling pour les autres serveurs.	Répétez l'étape précédente pour créer des groupes Auto Scaling pour le planificateur de processus, le serveur Elasticsearch et le serveur Web.	Administrateur du cloud, PeopleSoft administrateur

Création et configuration de groupes cibles

Tâche	Description	Compétences requises
Créez un groupe cible pour le serveur Web.	Sur la EC2 console Amazon, créez un groupe cible pour le serveur Web. Pour obtenir des instructions, consultez la documentation d'Elastic Load Balancing. Définissez le port sur le port sur lequel le serveur Web écoute.	Administrateur du cloud
Configurez les contrôles de santé.	Vérifiez que les valeurs des bilans de santé correspondent aux exigences de votre entreprise. Pour de plus amples informations, veuillez consulter la documentation relative à Elastic Load Balancing.	Administrateur du cloud
Créez un groupe cible pour le serveur Elasticsearch.	Répétez les étapes précédentes pour créer un groupe cible appelé PSFTSRCH pour	Administrateur du cloud

Tâche	Description	Compétences requises
	le serveur Elasticsearch et définissez le port Elasticse arch approprié.	
Ajoutez des groupes cibles aux groupes Auto Scaling.	Ouvrez le groupe Auto Scaling du serveur Web appelé `PSPIA_ASG` que vous avez créé précédemment. Dans l'onglet Load balancing, choisissez Edit, puis ajoutez le groupe `PSFTWEB` cible au groupe Auto Scaling. Répétez cette étape pour que le groupe Elasticse arch Auto Scaling ajoute le groupe `PSSRCH_ASG` cible `PSFTSRCH` que vous avez créé précédemment.	Administrateur du cloud
Définissez le caractère collant de la session.	Dans le groupe cible`PSFTWEB`, choisissez l'onglet Attributs , choisissez Modifier et définissez le caractère permanent de la session. Pour le type d'adhérence, choisisse z le cookie généré par l'équilib reur de charge et définissez la durée sur 1. Pour de plus amples informations, veuillez consulter la documenta tion relative à Elastic Load Balancing. Répétez cette étape pour le groupe cible`PSFTSRCH`.	Administrateur du cloud

Création et configuration d'équilibreurs de charge d'applications

Tâche	Description	Compétences requises
Créez un équilibreur de charge pour les serveurs Web.	Créez un Application Load Balancer nommé PSFTLB pour équilibrer la charge du trafic vers les serveurs Web. Pour obtenir des instructions, consultez la documentation d'Elastic Load Balancing. • Indiquez le nom de l'équilibreur de charge. • Pour Méthodes, choisissez Accessible sur Internet. • Dans la section Cartographie du réseau, sélectionnez le VPC approprié et au moins deux sous-réseaux publics provenant de différentes zones de disponibilité. • Dans la section Écouteurs et routage, sélectionnez le groupe cible PSFTWEB et spécifiez le protocole et le numéro de port appropriés.	Administrateur du cloud
Créez un équilibreur de charge pour les serveurs Elasticsearch.	Créez un Application Load Balancer nommé PSFTSCH pour équilibrer la charge du trafic vers les serveurs Elasticsearch. • Indiquez le nom de l'équilibreur de charge.	Administrateur du cloud

Tâche	Description	Compétences requises
	• Pour Schéma, choisissez Internal. • Dans la section Cartograp hie du réseau, sélectionnez le VPC et les sous-réseaux privés appropriés. • Dans la section Écouteurs et routage, sélectionnez le groupe cible PSFTSRCH et spécifiez le protocole et le numéro de port appropriés.	
Configurez la Route 53.	Sur la console Amazon Route 53, créez un enregistrement dans la zone hébergée qui servira l' PeopleSoft applicati on. Pour obtenir des instructi ons, consultez la documenta tion Amazon Route 53. Cela garantit que tout le trafic passe par l'équilibreur PSFTLB de charge.	Administrateur du cloud

Ressources connexes

- PeopleSoft Site Web d'Oracle
- Documentation AWS

Configurer la reprise après sinistre pour Oracle JD Edwards EnterpriseOne avec AWS Elastic Disaster Recovery

Créée par Thanigaivel Thirumalai (AWS)

Récapitulatif

Les catastrophes provoquées par des catastrophes naturelles, des défaillances d'applications ou une interruption des services nuisent aux revenus et entraînent des interruptions de service pour les applications d'entreprise. Pour réduire les répercussions de tels événements, la planification de la reprise après sinistre (DR) est essentielle pour les entreprises qui adoptent les systèmes de planification des ressources EnterpriseOne d'entreprise (ERP) de JD Edwards et d'autres logiciels critiques et critiques.

Ce modèle explique comment les entreprises peuvent utiliser AWS Elastic Disaster Recovery comme option de reprise après sinistre pour leurs EnterpriseOne applications JD Edwards. Il décrit également les étapes à suivre pour utiliser le basculement et le retour en arrière d'Elastic Disaster Recovery pour élaborer une stratégie de reprise après sinistre interrégionale pour les bases de données hébergées sur une instance Amazon Elastic Compute Cloud (Amazon EC2) dans le cloud AWS.

> **Note**
>
> Ce modèle nécessite que les régions principale et secondaire pour la mise en œuvre de la reprise après sinistre interrégionale soient hébergées sur AWS.

Oracle JD Edwards EnterpriseOne est une solution logicielle ERP intégrée pour les moyennes et grandes entreprises dans un large éventail de secteurs.

AWS Elastic Disaster Recovery minimise les temps d'arrêt et les pertes de données grâce à une restauration rapide et fiable des applications sur site et dans le cloud en utilisant un stockage abordable, un calcul et point-in-time une restauration minimaux.

AWS fournit quatre modèles d'architecture de base pour la reprise après sinistre. Ce document se concentre sur l'installation, la configuration et l'optimisation à l'aide de la stratégie d'éclairage pilote. Cette stratégie vous permet de créer un environnement de reprise après sinistre à moindre coût dans lequel vous configurez initialement un serveur de réplication pour répliquer les données de la base de données source, et vous approvisionnez le serveur de base de données proprement dit uniquement

lorsque vous lancez une analyse de reprise après sinistre. Cette stratégie élimine les dépenses liées à la maintenance d'un serveur de base de données dans la région DR. Au lieu de cela, vous payez pour une EC2 instance plus petite qui sert de serveur de réplication.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une EnterpriseOne application JD Edwards exécutée sur Oracle Database ou Microsoft SQL Server avec une base de données prise en charge en cours d'exécution sur une EC2 instance gérée. Cette application doit inclure tous les composants de EnterpriseOne base de JD Edwards (serveur d'entreprise, serveur HTML et serveur de base de données) installés dans une région AWS.
- Rôle AWS Identity and Access Management (IAM) pour configurer le service Elastic Disaster Recovery.
- Le réseau utilisé pour exécuter Elastic Disaster Recovery est configuré conformément aux paramètres de connectivité requis.

Limites

- Vous pouvez utiliser ce modèle pour répliquer tous les niveaux, sauf si la base de données est hébergée sur Amazon Relational Database Service (Amazon RDS), auquel cas nous vous recommandons d'utiliser la fonctionnalité de copie interrégionale d'Amazon RDS.
- Elastic Disaster Recovery n'est pas compatible avec CloudEndure Disaster Recovery, mais vous pouvez effectuer une mise à niveau depuis CloudEndure Disaster Recovery. Pour plus d'informations, consultez la FAQ de la documentation d'Elastic Disaster Recovery.
- Amazon Elastic Block Store (Amazon EBS) limite la fréquence à laquelle vous pouvez prendre des instantanés. Vous pouvez répliquer un maximum de 300 serveurs dans un seul compte AWS à l'aide d'Elastic Disaster Recovery. Pour répliquer davantage de serveurs, vous pouvez utiliser plusieurs comptes AWS ou plusieurs régions AWS cibles. (Vous devrez configurer Elastic Disaster Recovery séparément pour chaque compte et région.) Pour plus d'informations, consultez les meilleures pratiques dans la documentation d'Elastic Disaster Recovery.
- Les charges de travail sources (l' EnterpriseOne application et la base de données JD Edwards) doivent être hébergées sur EC2 des instances. Ce modèle ne prend pas en charge les charges de travail sur site ou dans d'autres environnements cloud.

- Ce modèle se concentre sur les EnterpriseOne composants de JD Edwards. Un plan complet de reprise après sinistre et de continuité des activités (BCP) doit inclure d'autres services essentiels, notamment :
  - Mise en réseau (cloud privé virtuel, sous-réseaux et groupes de sécurité)
  - Active Directory
  - Amazon WorkSpaces
  - Elastic Load Balancing
  - Un service de base de données géré tel qu'Amazon Relational Database Service (Amazon RDS)

Pour plus d'informations sur les prérequis, les configurations et les limites, consultez la documentation d'Elastic Disaster Recovery.

Versions du produit

- Oracle JD Edwards EnterpriseOne (versions prises en charge par Oracle et SQL Server selon les exigences techniques minimales d'Oracle)

Architecture

Pile technologique cible

- Une seule région et un seul cloud privé virtuel (VPC) pour la production et la non-production, et une deuxième région pour la reprise après sinistre
- Zones de disponibilité uniques pour garantir une faible latence entre les serveurs
- Application Load Balancer qui répartit le trafic réseau afin d'améliorer l'évolutivité et la disponibilité de vos applications sur plusieurs zones de disponibilité
- Amazon Route 53 fournira la configuration du système de noms de domaine (DNS)
- Amazon WorkSpaces va offrir aux utilisateurs une expérience de bureau dans le cloud
- Amazon Simple Storage Service (Amazon S3) pour le stockage de sauvegardes, de fichiers et d'objets
- Amazon CloudWatch pour la journalisation, la surveillance et les alarmes des applications
- Amazon Elastic Disaster Recovery pour la reprise après sinistre

Architecture cible

Le schéma suivant montre l'architecture de reprise après sinistre interrégionale de JD Edwards à l' EnterpriseOne aide d'Elastic Disaster Recovery.

Procédure

Voici un aperçu de haut niveau du processus. Pour plus de détails, consultez la section Epics.

- La réplication d'Elastic Disaster Recovery commence par une synchronisation initiale. Lors de la synchronisation initiale, l'agent de réplication AWS réplique toutes les données des disques sources vers la ressource appropriée dans le sous-réseau de la zone de transit.
- La réplication continue indéfiniment une fois la synchronisation initiale terminée.
- Vous passez en revue les paramètres de lancement, qui incluent les configurations spécifiques au service et un modèle de EC2 lancement Amazon, une fois l'agent installé et la réplication démarrée. Lorsque le serveur source est indiqué comme étant prêt pour la restauration, vous pouvez démarrer des instances.
- Lorsqu'Elastic Disaster Recovery émet une série d'appels d'API pour démarrer l'opération de lancement, l'instance de restauration est immédiatement lancée sur AWS conformément à vos paramètres de lancement. Le service lance automatiquement un serveur de conversion au démarrage.
- La nouvelle instance est lancée sur AWS une fois la conversion terminée et est prête à être utilisée. L'état du serveur source au moment du lancement est représenté par les volumes associés à l'instance lancée. Le processus de conversion implique des modifications des pilotes, du réseau et de la licence du système d'exploitation afin de garantir le démarrage natif de l'instance sur AWS.
- Après le lancement, les volumes nouvellement créés ne sont plus synchronisés avec les serveurs sources. L'agent de réplication AWS continue de répliquer régulièrement les modifications apportées à vos serveurs sources vers les volumes de la zone de transit, mais les instances lancées ne reflètent pas ces modifications.
- Lorsque vous démarrez une nouvelle instance de forage ou de restauration, les données sont toujours reflétées dans l'état le plus récent qui a été répliqué depuis le serveur source vers le sous-réseau de la zone de transit.
- Lorsque le serveur source est marqué comme étant prêt pour la restauration, vous pouvez démarrer des instances.

> **Note**
>
> Le processus fonctionne dans les deux sens : pour le basculement d'une région AWS principale vers une région DR, et pour revenir au site principal, une fois celui-ci restauré. Vous pouvez vous préparer au retour en arrière en inversant le sens de la réplication des données de la machine cible vers la machine source de manière entièrement orchestrée.

Les avantages de ce processus décrit dans ce modèle incluent :

- Flexibilité : les serveurs de réplication sont évolutifs et évolutifs en fonction du jeu de données et du temps de réplication, afin que vous puissiez effectuer des tests de reprise après sinistre sans perturber les charges de travail source ou la réplication.
- Fiabilité : la réplication est robuste, continue et sans interruption.
- Automatisation : cette solution fournit un processus unifié et automatisé pour les tests, la restauration et le retour en panne.
- Optimisation des coûts : vous pouvez uniquement répliquer les volumes nécessaires et les payer, et payer les ressources de calcul sur le site de reprise après sinistre uniquement lorsque ces ressources sont activées. Vous pouvez utiliser une instance de réplication optimisée en termes de coûts (nous vous recommandons d'utiliser un type d'instance optimisé pour le calcul) pour plusieurs sources ou une source unique avec un volume EBS important.

Automatisation et mise à l'échelle

Lorsque vous effectuez une reprise après sinistre à grande échelle, les EnterpriseOne serveurs JD Edwards dépendent des autres serveurs de l'environnement. Par exemple :

- Les serveurs EnterpriseOne d'applications JD Edwards qui se connectent à une base de données EnterpriseOne prise en charge par JD Edwards au démarrage dépendent de cette base de données.
- EnterpriseOne Les serveurs JD Edwards qui nécessitent une authentification et doivent se connecter à un contrôleur de domaine au démarrage pour démarrer les services dépendent du contrôleur de domaine.

C'est pourquoi nous vous recommandons d'automatiser les tâches de basculement. Par exemple, vous pouvez utiliser AWS Lambda ou AWS Step Functions pour automatiser les scripts de

EnterpriseOne démarrage de JD Edwards et les modifications apportées à l'équilibreur de charge afin d'automatiser le end-to-end processus de basculement. Pour plus d'informations, consultez le billet de blog Création d'un plan de reprise après sinistre évolutif avec AWS Elastic Disaster Recovery.

Outils

Services AWS

- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances. EC2
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Elastic Disaster Recovery minimise les temps d'arrêt et les pertes de données grâce à une restauration rapide et fiable des applications sur site et dans le cloud à l'aide d'un stockage abordable, d'un calcul et point-in-time d'une restauration minimaux.
- Amazon Virtual Private Cloud (Amazon VPC) vous donne le contrôle total de votre environnement réseau virtuel, y compris le placement des ressources, la connectivité et la sécurité.

Bonnes pratiques

Bonnes pratiques générales

- Préparez un plan écrit indiquant ce qu'il faut faire en cas de véritable rétablissement.
- Après avoir correctement configuré Elastic Disaster Recovery, créez un CloudFormation modèle AWS capable de créer la configuration à la demande, en cas de besoin. Déterminez l'ordre dans lequel les serveurs et les applications doivent être lancés, et enregistrez-le dans le plan de restauration.
- Effectuez un exercice régulier (les EC2 tarifs Amazon standard s'appliquent).
- Surveillez l'état de la réplication en cours à l'aide de la console Elastic Disaster Recovery ou par programmation.
- Protégez les point-in-time instantanés et confirmez avant de mettre fin aux instances.
- Créez un rôle IAM pour l'installation d'AWS Replication Agent.
- Activez la protection contre la résiliation pour les instances de restauration dans un scénario de reprise après sinistre réel.

- N'utilisez pas l'action Disconnect from AWS dans la console Elastic Disaster Recovery pour les serveurs pour lesquels vous avez lancé des instances de restauration, même dans le cas d'un véritable événement de restauration. L'exécution d'une déconnexion met fin à toutes les ressources de réplication associées à ces serveurs sources, y compris vos points de restauration point-in-time (PIT).
- Modifiez la politique PIT pour modifier le nombre de jours de conservation des instantanés.
- Modifiez le modèle de lancement dans les paramètres de lancement d'Elastic Disaster Recovery afin de définir le sous-réseau, le groupe de sécurité et le type d'instance appropriés pour votre serveur cible.
- Automatisez le processus de end-to-end basculement en utilisant Lambda ou Step Functions pour automatiser les scripts de démarrage de JD EnterpriseOne Edwards et les modifications de l'équilibreur de charge.

EnterpriseOne Optimisation et considérations de JD Edwards

- Accédez à PrintQueuela base de données.
- Accédez à MediaObjectsla base de données.
- Excluez les journaux et le dossier temporaire des serveurs de traitement par lots et des serveurs logiques.
- Excluez le dossier temporaire d'Oracle WebLogic.
- Créez des scripts pour le démarrage après le basculement.
- Excluez le tempdb pour SQL Server.
- Excluez le fichier temporaire pour Oracle.

Épopées

Exécuter les tâches initiales et la configuration

Tâche	Description	Compétences requises
Configurez le réseau de réplication.	Implémentez votre Enterpris eOne système JD Edwards dans la région AWS principal e et identifiez la région AWS pour DR. Suivez les étapes	Administrateur AWS

Tâche	Description	Compétences requises
	décrites dans la section Exigences relatives au réseau de réplication de la documentation Elastic Disaster Recovery pour planifier et configurer votre réseau de réplication et de reprise après sinistre.	
Déterminez le RPO et le RTO.	Identifiez l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO) pour vos serveurs d'applications et votre base de données.	Architecte cloud, architecte DR
Activez la réplication pour Amazon EFS.	Le cas échéant, activez la réplication depuis la région principale AWS vers la région DR pour les systèmes de fichiers partagés tels qu'Amazon Elastic File System (Amazon EFS) en utilisant AWS DataSync, rsync ou un autre outil approprié.	Administrateur du cloud
Gérez le DNS en cas de DR.	Identifiez le processus de mise à jour du système de noms de domaine (DNS) lors de l'exercice DR ou de la DR proprement dite	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un rôle IAM pour la configuration.	Suivez les instructions de la section Initialisation et autorisations d'Elastic Disaster Recovery de la documentation d'Elastic Disaster Recovery pour créer un rôle IAM afin d'initialiser et de gérer le service AWS.	Administrateur du cloud
Configurez le peering VPC.	Assurez-vous que la source et la cible VPCs sont homologue s et accessibles l'une à l'autre. Pour les instructions de configuration, consultez la documentation Amazon VPC.	Administrateur AWS

Configuration des paramètres de réplication d'Elastic Disaster Recovery

Tâche	Description	Compétences requises
Initialisez Elastic Disaster Recovery.	Ouvrez la console Elastic Disaster Recovery, choisisse z la région AWS cible (dans laquelle vous allez répliquer les données et lancer des instances de restauration), puis choisissez Définir les paramètres de réplication par défaut.	Administrateur AWS
Configurez des serveurs de réplication.	1. Dans le volet Configure r les serveurs de réplicati on, entrez le sous-rése au de la zone de transit et le type d'instance du	Administrateur AWS

Tâche	Description	Compétences requises
	serveur de réplication. Le type d'instance `t3.small` est sélectionné par défaut. Configurez ce paramètre en fonction de vos besoins et n'oubliez pas de tenir compte de la tarification des instances. Pour plus d'informations, consultez les EC2 tarifs Amazon. 2. Dans la section Accès au service, choisissez Afficher les détails pour consulter le rôle lié au service et les politiques supplémentaires créées lors de l'initialisation du service. 3. Choisissez Suivant.	

Tâche	Description	Compétences requises
Configurez les volumes et les groupes de sécurité.	1. Dans le volet Volumes et groupes de sécurité, sélectionnez le type de volume EBS pour le serveur de réplication et définissez le chiffrement Amazon EBS sur Default. 2. Sélectionnez Toujours utiliser le groupe de sécurité AWS Elastic Disaster Recovery afin qu'Elastic Disaster Recovery attache et surveille automatiq uement le groupe de sécurité par défaut. 3. Choisissez Suivant.	Administrateur AWS

Tâche	Description	Compétences requises
Configurez des paramètres supplémentaires.	1. Dans le volet Paramètres supplémentaires, configurez le routage et la limitation des données, la politique PIT et les balises. • Le routage et la régulation des données contrôlent la manière dont les données circulent du serveur externe vers les serveurs de réplication. Choisissez Utiliser une adresse IP privée pour la réplication des données. Dans le cas contraire, les serveurs de réplication se verront automatiquement attribuer une adresse IP publique et les données circuleront sur l'Internet public. • Dans la section Politique de point in time (PIT), configurez une politique de rétention qui détermine la durée après laquelle les instantanés ne sont plus nécessaires. La période de rétention par défaut est de sept jours. • Dans la section Tags, ajoutez des balises personnalisées aux	Administrateur AWS

Tâche	Description	Compétences requises
	ressources créées par Elastic Disaster Recovery dans votre compte AWS. 2. Choisissez Next, passez en revue les paramètres dans le volet suivant, puis choisissez Create default pour créer le modèle par défaut.	

Installation de l'agent de réplication AWS

Tâche	Description	Compétences requises
Créez un rôle IAM.	Créez un rôle IAM contenant la `AWSElasticDisasterRecoveryAgentInstallationPolicy` politique. Dans la section Sélectionner le type d'accès AWS, activez l'accès programmatique. Notez l'ID de la clé d'accès et la clé d'accès secrète. Vous aurez besoin de ces informations lors de l'installation de l'agent de réplication AWS.	Administrateur AWS
Vérifiez les exigences.	Vérifiez et remplissez les conditions requises dans la documentation d'Elastic Disaster Recovery pour installer l'agent de réplication AWS.	Administrateur AWS

Tâche	Description	Compétences requises

Installez l'agent de réplication AWS.	Suivez les instructions d'installation de votre système d'exploitation et installez l'agent de réplication AWS.
	• Pour Microsoft Windows : téléchargez les fichiers d'installation et exécutez le fichier .exe en tant qu'administrateur. Répondez aux instructions pour terminer l'installation.
	• Pour Linux : copiez les commandes suivantes (dans l'ordre indiqué) et collez-les dans votre session Secure Shell (SSH). La première commande télécharge le programme d'installation et la seconde l'exécute.
	`wget -O ./aws-replication-installer-init.py https://aws-elastic-disaster-recovery-us-west-2.s3.amazonaws.com/latest/linux/aws-replication-installer-init.py`
	`sudo python3 aws-replication-installer-init.py`
		Administrateur AWS

Tâche	Description	Compétences requises
	Répondez aux instructions pour terminer l'installation. **Note** Modifiez l'URL pour qu'elle reflète votre région. Répétez ces étapes pour le serveur restant.	
Surveillez la réplication.	Retournez dans le volet des serveurs Elastic Disaster Recovery Source pour surveiller l'état de la réplicati on. La synchronisation initiale peut prendre un certain temps en fonction de la taille du transfert de données. Lorsque le serveur source est entièrement synchronisé, l'état du serveur passe à Prêt. Cela signifie qu'un serveur de réplication a été créé dans la zone intermédiaire et que les volumes EBS ont été répliqués du serveur source vers la zone intermédiaire.	Administrateur AWS

Configuration des paramètres de lancement

Tâche	Description	Compétences requises
Modifiez les paramètres de lancement.	Pour mettre à jour les paramètres de lancement des instances de forage et de restauration, sur la console Elastic Disaster Recovery, sélectionnez le serveur source, puis choisissez Actions, Modifier les paramètres de lancement . Vous pouvez également choisir vos machines sources de réplication sur la page Serveurs source, puis choisir l'onglet Paramètre s de lancement. Cet onglet comporte deux sections : Paramètres de lancement généraux et modèle de EC2 lancement.	Administrateur AWS
Configurez les paramètres généraux de lancement.	Révisez les paramètres de lancement généraux en fonction de vos besoins. • Dimensionnement correct du type d'instance : si vous choisissez Basic, Elastic Disaster Recovery contourne le type d'instanc e que vous avez sélection né dans le modèle de EC2 lancement Amazon et choisit automatiquement le	Administrateur AWS

Tâche	Description	Compétences requises
	type d'instance en fonction du système d'exploitation, du processeur et de la RAM du serveur source. • Copier l'adresse IP privée : choisissez si vous souhaitez qu'Elastic Disaster Recovery s'assure que l'adresse IP privée utilisée par l'instance de forage ou de restauration correspond à l'adresse IP privée utilisée par le serveur source. Si vous avez choisi Oui, assurez-vous que la plage d'adresses IP du sous-réseau que vous avez définie dans le modèle de EC2 lancement Amazon inclut l'adresse IP privée. Pour plus d'informations, consultez la section Paramètres de lancement généraux dans la documentation d'Elastic Disaster Recovery.	

Tâche	Description	Compétences requises
Configurez le modèle EC2 de lancement Amazon.	Elastic Disaster Recovery utilise les modèles de EC2 lancement Amazon pour lancer des instances de forage et de restauration pour chaque serveur source. Le modèle de lancement est créé automatiq uement pour chaque serveur source que vous ajoutez à Elastic Disaster Recovery après avoir installé l'agent de réplication AWS. Vous devez définir le modèle de EC2 lancement Amazon comme modèle de lancement par défaut si vous souhaitez l'utiliser avec Elastic Disaster Recovery. Pour plus d'informations, consultez la section Modèle de EC2 lancement dans la documentation d'Elastic Disaster Recovery.	Administrateur AWS

Lancer le forage DR et le basculement

Tâche	Description	Compétences requises
Lancer un exercice	1. Sur la console Elastic Disaster Recovery, ouvrez la page Serveurs source et vérifiez que l'état du serveur source est Prêt.	Administrateur AWS

Tâche	Description	Compétences requises
	2. Sélectionnez tous les serveurs source pour lesquels vous souhaitez effectuer l'exercice DR. 3. Dans le menu Initiate recovery job, choisissez Initiate drill et sélectionnez le point-in-time cliché approprié. Cela lance une tâche de restauration pour les serveurs source sélectionnés. Vous pouvez suivre l'état de la tâche dans l'onglet Historique des tâches de restauration. L'instance de forage lancée apparaît également sur la page Instances de restauration. **Note** Les modifications ultérieures apportées au serveur source seront synchronisées avec le serveur de réplication, et non avec l'instance de forage. 4. Testez et vérifiez l'instance de forage DR.	

Tâche	Description	Compétences requises
	5. Sur la page Instances de restauration, sélection nez l'instance de forage, puis choisissez Actions, Disconnect from AWS. Cela supprime l'agent de réplicati on AWS de l'instance de restauration et supprime toutes les ressources associées à l'instance de restauration d'Elastic Disaster Recovery. 6. Choisissez Supprimer les instances de restauration. Cela supprime la représent ation de l'instance de la console Elastic Disaster Recovery et dissocie complètement l'instance du service Elastic Disaster Recovery. Elle ne supprime pas l' EC2 instance sous-jacente. 7. Mettez fin à l'instance DR Drill depuis la EC2 console Amazon. Pour plus d'informations, consultez la section Préparati on au basculement dans la documentation d'Elastic Disaster Recovery.	

Tâche	Description	Compétences requises
Validez l'exercice.	À l'étape précédente, vous avez lancé de nouvelles instances cibles dans la région DR. Les instances cibles sont des répliques des serveurs sources basées sur le snapshot pris lorsque vous avez lancé le lancement. Dans cette procédure, vous vous connectez à vos machines EC2 cibles Amazon pour vérifier qu'elles fonctionnent comme prévu. 1. Ouvrez la EC2 console Amazon. 2. Choisissez Instances (en cours d'exécution). 3. Sélectionnez l'instance cible et notez son IPv4 adresse privée. 4. Assurez-vous que vous pouvez vous connecter à l' EC2 instance et que le JD Edwards EnterpriseOne et les composants associés sont répliqués comme prévu.	

Tâche	Description	Compétences requises
Lancez un basculement.	Un basculement est la redirection du trafic d'un système principal vers un système secondaire. Elastic Disaster Recovery vous aide à effectuer un basculement en lançant des instances de restauration sur AWS. Lorsque les instances de restauration ont été lancées, vous redirigez le trafic de vos systèmes principaux vers ces instances. 1. Sur la console Elastic Disaster Recovery, ouvrez la page Serveurs source et vérifiez que la colonne Ready for recovery du serveur source indique Prêt et que la colonne État de réplication des données indique Healthy. 2. Sélectionnez le serveur source. Dans le menu Initiate recovery job, sélectionnez Initiate recovery. 3. Sélectionnez le point-in-time snapshot à partir duquel vous souhaitez lancer l'instance de restauration, puis choisissez Initiate recovery.	Administrateur AWS

Tâche	Description	Compétences requises
	Cela lance un travail de rétablissement. Vous pouvez surveiller l'état de la tâche sur la page Instances de restauration. 4. Testez et vérifiez l'instance de restauration. Si nécessaire, ajustez la configuration DNS et connectez votre Enterprise One application JD Edwards à la base de données. 5. Vous pouvez désormais déconnecter et mettre hors service le Enterprise One serveur JD Edwards source, car toutes les modifications ont été écrites dans la nouvelle instance de restauration. 6. Enregistrez l'instance de restauration en tant que serveur source dans la région DR en suivant le processus décrit dans l'épique Installation de l'agent de réplication AWS. Pour plus d'informations, consultez la section Réalisation d'un basculement dans	

Tâche	Description	Compétences requises
	la documentation d'Elastic Disaster Recovery.	

Tâche	Description	Compétences requises
Lancez un retour en arrière.	Le processus de lancement d'un retour de secours est similaire au processus de lancement d'un basculement. 1. Ouvrez la console Elastic Disaster Recovery dans la région principale. Accédez à la page Instances de restauration, sélection nez l'instance de forage, puis choisissez Actions, Déconnexion d'AWS, Supprimer les instances de restauration. 2. Ouvrez la console Elastic Disaster Recovery dans la région DR. Enregistrez votre nouveau Enterpris eOne serveur JD Edwards en tant que serveur source dans la région DR en installant l'agent de réplicati on AWS. Les données seront synchronisées avec un nouveau serveur de réplication configuré dans le nouveau sous-réseau intermédiaire. **Note** Lorsque le nouveau EnterpriseOne serveur JD Edwards	Administrateur AWS

Tâche	Description	Compétences requises
	est enregistré en tant que serveur source, vous pouvez voir deux serveurs sources apparaître dans la console Elastic Disaster Recovery : un serveur créé à partir de l' EC2 instance principal e et le nouveau serveur créé à partir de l'instance de restauration. Nous vous recommand ons de baliser correctement les serveurs pour éviter toute confusion et d'ajouter de préférence le nouveau serveur au modèle de lancement. 3. Pour redémarrer la réplicati on DR depuis la région principale, dissociez l'instance de restauration lancée de la console Elastic Disaster Recovery dans la région DR et enregistrez l'hôte en tant que serveur	

Tâche	Description	Compétences requises
	source dans la région principale. Pour plus d'informations, consultez la section Réalisation d'un retour arrière dans la documentation d'Elastic Disaster Recovery.	

Tâche	Description	Compétences requises
Démarrez les EnterpriseOne composants JD Edwards.	1. Démarrez la Enterpris eOne base de données JD Edwards en vous connectant au serveur de base de données. 2. Lorsque la base de données est en cours d'exécution, démarrez les serveurs EnterpriseOne logiques et de traitement par lots de JD Edwards. 3. Commencez WebLogic sur les serveurs Web, puis démarrez une instance JAS sur les serveurs JAS. 4. Commencez WebLogic sur le serveur de provision nement et sur le serveur de la console SM. 5. Démarrez SM Agent sur les serveurs. 6. Vérifiez que la connexion à JD Edwards EnterpriseOne fonctionne correctement. Vous devrez intégrer les modifications dans Route 53 et Application Load Balancer pour que le EnterpriseOne lien JD Edwards fonctionne. Vous pouvez automatiser ces étapes à l'aide de Lambda,	J.D. Edwards EnterpriseOne CNC

Tâche	Description	Compétences requises
	Step Functions et Systems Manager (Run Command). **Note** Elastic Disaster Recovery effectue une réplication au niveau des blocs des volumes EBS de l' EC2 instance source qui hébergent le système d'exploit ation et les systèmes de fichiers. Les systèmes de fichiers partagés créés à l'aide d'Amazon EFS ne font pas partie de cette réplication. Vous pouvez répliquer des systèmes de fichiers partagés dans la région DR à l'aide d'AWS DataSync, comme indiqué dans le premier épisode, puis monter ces systèmes de fichiers répliqués dans le système DR.	

Résolution des problèmes

Problème	Solution
L'état de réplication des données du serveur source est bloqué et la réplication est retardée. Si vous vérifiez les détails, l'état de réplication des données indique que l'agent n'a pas été détecté.	Vérifiez que le serveur source bloqué fonctionne. **Note** En cas de panne du serveur source, le serveur de réplication est automatiquement arrêté. Pour plus d'informations sur les problèmes de retard, consultez la section Problèmes de retard de réplication dans la documentation d'Elastic Disaster Recovery.
L'installation d'AWS Replication Agent dans l' EC2 instance source échoue dans RHEL 8.2 après avoir scanné les disques. `aws_replication_agent_installer.log` révèle que les en-têtes du noyau sont manquants.	Avant d'installer l'agent de réplication AWS sur RHEL 8, CentOS 8 ou Oracle Linux 8, exécutez : `sudo yum install elfutils-libelf-devel` Pour plus d'informations, consultez les exigences d'installation de Linux dans la documentation d'Elastic Disaster Recovery.
Sur la console Elastic Disaster Recovery, le serveur source indique que le serveur source est prêt avec un décalage et que l'état de réplication des données est bloqué. En fonction de la durée d'indisponibilité de l'agent de réplication AWS, le statut peut	Utilisez une commande du système d'exploitation pour confirmer que l'agent de réplication AWS est en cours d'exécution dans l' EC2 instance source ou pour confirmer que l'instance est en cours d'exécution. Une fois les problèmes corrigés, Elastic Disaster Recovery reprendra l'analyse.

Problème	Solution
indiquer un retard important, mais le problème reste le même.	Attendez que toutes les données soient synchronisées et que l'état de réplication soit sain avant de commencer un exercice de reprise après sinistre.
Réplication initiale avec un décalage élevé. Sur la console Elastic Disaster Recovery, vous pouvez constater que l'état de synchronisation initial est extrêmement lent pour un serveur source.	Vérifiez les problèmes de retard de réplicati on documentés dans la section Problèmes de retard de réplication de la documentation d'Elastic Disaster Recovery. Le serveur de réplication peut être incapable de gérer la charge en raison d'opérations de calcul intrinsèques. Dans ce cas, essayez de mettre à niveau le type d'instance après avoir consulté l'équipe du Support technique AWS.

Ressources connexes

- Guide de l'utilisateur d'AWS Elastic Disaster Recovery
- Création d'un plan de reprise après sinistre évolutif avec AWS Elastic Disaster Recovery (article de blog AWS)
- AWS Elastic Disaster Recovery : introduction technique (cours AWS Skill Builder ; connexion requise)
- Guide de démarrage rapide d'AWS Elastic Disaster Recovery

Configurer la détection des AWS CloudFormation dérives dans une organisation multirégionale et multi-comptes

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Les utilisateurs d'Amazon Web Services (AWS) recherchent souvent un moyen efficace de détecter les incohérences dans la configuration des ressources, notamment la dérive des AWS CloudFormation piles, et de les corriger dès que possible. C'est particulièrement le cas lorsqu'il AWS Control Tower est utilisé.

Ce modèle fournit une solution prescriptive qui résout efficacement le problème en utilisant des modifications de configuration des ressources consolidées et en agissant sur ces modifications pour générer des résultats. La solution est conçue pour les scénarios dans lesquels plusieurs AWS CloudFormation piles sont créées dans plusieurs comptes, ou une combinaison des deux. Région AWS Les objectifs de la solution sont les suivants :

- Simplifier le processus de détection de la dérive
- Configurer les notifications et les alertes
- Configurer des rapports consolidés

Conditions préalables et limitations

Prérequis

- AWS Config activé dans toutes les régions et tous les comptes qui doivent être surveillés

Limites

- Le rapport généré prend uniquement en charge les valeurs séparées par des virgules (CSV) et les formats de sortie JSON.

Architecture

Le schéma suivant montre la AWS Organizations configuration avec plusieurs comptes. AWS Config les règles communiquent entre les comptes.

Le flux de travail comprend les étapes suivantes :

1. La AWS Config règle détecte la dérive.
2. Les résultats de détection de dérive trouvés dans d'autres comptes sont envoyés au compte de gestion.
3. La CloudWatch règle Amazon appelle une AWS Lambda fonction.
4. La fonction Lambda interroge la AWS Config règle pour obtenir des résultats agrégés.
5. La fonction Lambda informe Amazon Simple Notification Service (Amazon SNS), qui envoie une notification par e-mail concernant la dérive.

Automatisation et mise à l'échelle

La solution présentée ici peut être adaptée à la fois à des régions et à des comptes supplémentaires.

Outils

Services AWS

- AWS Configfournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS. Elle indique comment les ressources sont liées entre elles et comment elles ont été configurées dans le passé, pour que vous puissiez observer comment les configurations et les relations changent au fil du temps.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Épopées

Détection automatique de la dérive pour AWS CloudFormation

Tâche	Description	Compétences requises
Créez l'agrégateur.	1. Connectez-vous à la AWS Config console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/config. 2. Créez un agrégateur dans le compte de gestion. 3. Assurez-vous que la réplication des données est activée afin de AWS Config pouvoir récupérer les données des comptes sources. 4. Sélectionnez toutes les régions et tous les comptes applicables. Vous pouvez sélectionner des comptes en fonction de AWS Organizations. Nous recommandons cette approche car les nouveaux comptes de l'organisation font automatiquement partie de l'agrégateur.	Architecte du cloud
Créez une règle AWS gérée.	Ajoutez la règle `cloudformation-stack-drift-detection-check` AWS gérée. La règle a besoin d'une valeur de	Architecte du cloud

Tâche	Description	Compétences requises
	paramètre :`cloudformationArn` . Entrez le rôle IAM Amazon Resource Name (ARN) autorisé à détecter la dérive de pile. Le rôle doit avoir une politique de confiance qui lui AWS Config permette d'assumer le rôle.	
Créez la section de requête avancée de l'agrégateur.	Pour récupérer des piles dérivées à partir de plusieurs sources, créez la requête suivante : `SELECT resourceId, configuration.driftInformation.stackDriftStatus WHERE resourceType = 'AWS::CloudFormation::Stack' AND configuration.driftInformation.stackDriftStatus IN ('DRIFTED')`	Architecte cloud, développeur

Tâche	Description	Compétences requises
Automatisez l'exécution de la requête et publiez.	1. Créez une fonction Lambda en utilisant le code joint. Lambda publiera les résultats dans une rubrique SNS fournie en tant que variable d'environnement dans la fonction Lambda. 2. Pour recevoir des alertes, créez un abonnement par e-mail à la rubrique SNS.	Architecte cloud, développeur
Créez une CloudWatch règle.	Créez une CloudWatch règle basée sur un calendrier pour appeler la fonction Lambda, qui est chargée des alertes.	Architecte du cloud

Ressources connexes

Ressources

- Qu'est-ce que c'est AWS Config ?
- Agrégation de données multicomptes et multirégions
- Détection des modifications de configuration non gérées apportées aux piles et aux ressources
- IAM : Transmettre un rôle IAM à une personne spécifique Service AWS
- Qu'est-ce qu'Amazon SNS ?

Informations supplémentaires

Considérations

Nous recommandons d'utiliser la solution présentée dans ce modèle plutôt que d'utiliser des solutions personnalisées qui impliquent des appels d'API à des intervalles spécifiques pour initier la détection de dérive sur chaque CloudFormation pile ou ensemble de piles. Les solutions personnalisées qui utilisent des appels d'API à des intervalles spécifiques peuvent entraîner un grand nombre d'appels

d'API et affecter les performances. En raison du nombre d'appels d'API, une régulation peut se produire. Un autre problème potentiel est le retard de détection si les modifications des ressources sont identifiées uniquement sur la base du calendrier.

Comme les ensembles de piles sont constitués de piles, vous pouvez utiliser cette solution. Les détails de l'instance Stack sont également disponibles dans le cadre de la solution.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Importation réussie d'un compartiment S3 en tant que CloudFormation stack AWS

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Si vous utilisez des ressources Amazon Web Services (AWS), telles que les compartiments Amazon Simple Storage Service (Amazon S3), et que vous souhaitez utiliser une approche d'infrastructure en tant que code (IaC), vous pouvez importer vos ressources dans CloudFormation AWS et les gérer sous forme de pile.

Ce modèle fournit les étapes à suivre pour importer avec succès un compartiment S3 en tant que CloudFormation pile AWS. En utilisant l'approche de ce modèle, vous pouvez éviter d'éventuelles erreurs susceptibles de se produire si vous importez votre compartiment S3 en une seule action.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un compartiment S3 existant et une politique de compartiment S3. Pour plus d'informations à ce sujet, consultez la section Quelle politique de compartiment S3 dois-je utiliser pour me conformer à la règle AWS Config s3- bucket-ssl-requests-only dans le centre de connaissances AWS.
- Une clé AWS Key Management Service (AWS KMS) existante et son alias. Pour plus d'informations à ce sujet, consultez la section Utilisation d'alias dans la documentation AWS KMS.
- Exemple de CloudFormation modèle `CloudFormation-template-S3-bucket` AWS (ci-joint), téléchargé sur votre ordinateur local.

Architecture

Le schéma suivant illustre le flux de travail suivant :

1. L'utilisateur crée un modèle AWS CloudFormation au format JSON ou YAML.
2. Le modèle crée une CloudFormation pile AWS pour importer le compartiment S3.
3. La CloudFormation pile AWS gère le compartiment S3 que vous avez spécifié dans le modèle.

Pile technologique

- AWS CloudFormation
- AWS Identity and Access Management (IAM)
- AWS KMS
- Amazon S3

Outils

- AWS CloudFormation — AWS vous CloudFormation aide à créer et à provisionner des déploiements d'infrastructure AWS de manière prévisible et répétée.
- AWS Identity and Access Management (IAM) — IAM est un service Web permettant de contrôler en toute sécurité l'accès aux services AWS.
- AWS KMS — AWS Key Management Service (AWS KMS) est un service de chiffrement et de gestion des clés adapté au cloud.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet.

Épopées

Importez un compartiment S3 avec chiffrement AWS KMS key basé en tant que CloudFormation stack AWS

Tâche	Description	Compétences requises

Créez un modèle pour importer le compartiment S3 et la clé KMS.	Sur votre ordinateur local, créez un modèle pour importer votre compartiment S3 et votre clé KMS à l'aide de l'exemple de modèle suivant :
	`AWSTemplateFormatVersion: 2010-09-09`
	
	`Parameters:`
		AWS DevOps

Tâche	Description	Compétences requises

	<pre> bucketName:
	
	    Type: String
	
	Resources:
	
	  S3Bucket:
	
	    Type: 'AWS::S3:
	:Bucket'
	
	    DeletionPolicy:
	 Retain
	
	    Properties:
	
	      BucketName: !Ref
	 bucketName
	
	      BucketEncryption:
	
	        ServerSid
	eEncryptionConfigu
	ration:
	
	          - ServerSid
	eEncryptionByDefault:
	
	              SSEAlgori
	thm: 'aws:kms'
	
	              KMSMaster
	KeyID: !GetAtt
	
	                -
	 KMSS3Encryption
	
	                - Arn
	
	  KMSS3Encryption:</pre>	

Tâche	Description	Compétences requises

	<pre>Type: 'AWS::KMS
	::Key'
	
	DeletionPolicy:
	Retain
	
	Properties:
	
	Enabled: true
	
	KeyPolicy: !Sub
	|-
	
	{
	
	"Id": "key-
	consolepolicy-3",
	
	"Version":
	"2012-10-17",
	
	"Statemen
	t": [
	
	{
	
	"Sid": "Enable IAM User
	Permissions",
	
	"Effect": "Allow",
	
	"Principal": {
	
	"AWS": ["arn:aws:iam::
	${AWS::AccountId}:roo
	t"]
	
	},</pre>	

Tâche	Description	Compétences requises

	<pre>"Action": "kms:*",
	
	"Resource": "*"
	}
	}
	]
	}
	
	EnableKey
	Rotation: true</pre>	

Tâche	Description	Compétences requises
Créez la pile.	1. Connectez-vous à l'AWS Management Console, ouvrez la CloudFormation console AWS, choisissez View stack, Create stack, puis With existing resources (import resources). 2. Choisissez Télécharger un fichier modèle, puis chargez le fichier modèle que vous avez créé précédemment. 3. Entrez un nom pour votre pile et configurez les options restantes en fonction de vos besoins. 4. Choisissez Create stack et attendez que le statut de la pile passe à`IMPORT_COMPLETE` .	AWS DevOps

Tâche	Description	Compétences requises

Créez l'alias de clé KMS.	1. Sur la CloudFormation console AWS, choisissez Stacks, choisissez le nom de la pile que vous avez créée précédemment, choisissez le volet Modèle, puis choisissez Afficher dans Designer.
	2. Ajoutez l'extrait suivant à la `Resource` section de votre modèle, puis choisissez Create stack et complétez l'assistant :
	
	`KMSS3EncryptionAlias:`
	
	`  Type: 'AWS::KMS ::Alias'`
	
	`  DeletionPolicy: Retain`
	
	`  Properties:`
	
	`  AliasName: alias/S3BucketKey`
	
	`  TargetKeyId: !Ref KMSS3Encryption`
	
	Pour plus d'informations à ce sujet, consultez les mises à jour du CloudFormation stack AWS dans la CloudFormation documentation AWS.
		AWS DevOps

Tâche	Description	Compétences requises

Mettez à jour la pile pour inclure la politique du compartiment S3.	1. Sur la CloudFormation console AWS, choisisse z Stacks, choisissez le nom de la pile que vous avez créée précédemment, choisissez le volet Modèle, puis choisissez Afficher dans Designer.
	2. Ajoutez l'extrait suivant à la `Resource` section du modèle, puis choisissez Create stack et complétez l'assistant :
	
	`S3BucketPolicy:`
	
	`Type: 'AWS::S3::BucketPolicy'`
	
	`Properties:`
	
	`Bucket: !Ref S3Bucket`
	
	`PolicyDocument: !Sub |-`
	
	`{`
	
	`"Version": "2008-10-17",`
	
	`"Id": "restricthttp",`
		AWS DevOps

Tâche	Description	Compétences requises

	"Statement": [
	{
	"Sid": "denyhttp",
	"Effect": "Deny",
	"Principal": {
	"AWS": "*"
	},
	"Action": "s3:*",
	"Resource": ["arn:aws:s3:::${S3Bucket}","arn:aws:s3:::${S3Bucket}/*"],
	"Condition": {
	"Bool": {
	"aws:SecureTransport": "false"
	}	

Tâche	Description	Compétences requises

	<pre>}
	}
	]
	}</pre>
	Note
	Cette politique de compartiment S3 comporte une déclaration de refus qui restreint les appels d'API non sécurisés.	

Tâche	Description	Compétences requises
Mettez à jour la politique clé.	1. Sur la CloudFormation console AWS, choisisse z Stacks, choisissez le nom de la pile que vous avez créée précédemment, choisissez le volet Modèle, puis choisissez Afficher dans Designer. 2. Modifiez la ressource KMS du modèle pour inclure la politique clé qui permet aux administrateurs d'adminis trer la clé KMS. 3. Choisissez Create stack, puis Next, puis complétez l'assistant en fonction de vos besoins. Pour plus d'informations, consultez la section Politique s clés AWS KMS de la documentation AWS KMS.	Administrateur AWS

Tâche	Description	Compétences requises

Ajoutez des balises au niveau des ressources.	1. Sur la CloudFormation console AWS, choisissez Stacks, choisissez le nom de la pile que vous avez créée précédemment, choisissez le volet Modèle, puis choisissez Afficher dans Designer.
	2. Ajoutez l'extrait suivant à la `Properties` section des ressources Amazon S3 du modèle, puis choisissez Create stack et complétez l'assistant :
	`Tags:`
	`  - Key: createdBy`
	`  Value: Cloudformation`
		AWS DevOps

Ressources connexes

- Intégrer les ressources existantes à la CloudFormation gestion d'AWS
- AWS re:Invent 2017 : présentation approfondie d'AWS CloudFormation (vidéo)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Synchronisez les données entre les systèmes de fichiers Amazon EFS dans différentes régions AWS à l'aide d'AWS DataSync

Créée par Sarat Chandra Pothula (AWS) et Aditya Ambati (AWS)

Récapitulatif

Cette solution fournit un cadre robuste pour une synchronisation des données efficace et sécurisée entre les instances Amazon Elastic File System (Amazon EFS) dans les différentes régions AWS. Cette approche est évolutive et permet une réplication contrôlée des données entre régions. Cette solution peut améliorer vos stratégies de reprise après sinistre et de redondance des données.

En utilisant l'AWS Cloud Development Kit (AWS CDK), ce modèle utilise une approche d'infrastructure en tant que code (IaC) pour déployer les ressources de la solution. L'application AWS CDK déploie les ressources essentielles d'AWS, DataSync Amazon EFS, Amazon Virtual Private Cloud (Amazon VPC) et Amazon Elastic Compute Cloud (Amazon). EC2 Cet iAC fournit un processus de déploiement reproductible et contrôlé par version qui est entièrement conforme aux meilleures pratiques d'AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI) version 2.9.11 ou ultérieure, installée et configurée
- AWS CDK version 2.114.1 ou ultérieure, installé et amorcé
- NodeJS version 20.8.0 ou ultérieure, installée

Limites

- La solution hérite des limites d' DataSync Amazon EFS, telles que les taux de transfert de données, les limites de taille et la disponibilité régionale. Pour plus d'informations, consultez les rubriques DataSync Quotas AWS et Quotas Amazon EFS.
- Cette solution prend uniquement en charge Amazon EFS. DataSync prend en charge d'autres services AWS, tels qu'Amazon Simple Storage Service (Amazon S3) et FSx Amazon for Lustre. Toutefois, cette solution nécessite des modifications pour synchroniser les données avec ces autres services.

Architecture

Cette solution déploie les piles AWS CDK suivantes :

- Pile Amazon VPC : cette pile configure les ressources du cloud privé virtuel (VPC), notamment des sous-réseaux, une passerelle Internet et une passerelle NAT dans les régions AWS principale et secondaire.
- Pile Amazon EFS : cette pile déploie les systèmes de fichiers Amazon EFS dans les régions principale et secondaire et les connecte à leurs régions respectives VPCs.
- Amazon EC2 Stack — Cette pile lance EC2 des instances dans les régions principale et secondaire. Ces instances sont configurées pour monter le système de fichiers Amazon EFS, ce qui leur permet d'accéder au stockage partagé.
- DataSync pile de localisation — Cette pile utilise une construction personnalisée appelée `DataSyncLocationConstruct` pour créer des ressources de DataSync localisation dans les régions principale et secondaire. Ces ressources définissent les points de terminaison pour la synchronisation des données.
- DataSync pile de tâches — Cette pile utilise une construction personnalisée appelée `DataSyncTaskConstruct` pour créer une DataSync tâche dans la région principale. Cette tâche est configurée pour synchroniser les données entre les régions principale et secondaire en utilisant les emplacements DataSync source et de destination.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS DataSync est un service de transfert et de découverte de données en ligne qui vous aide à déplacer des fichiers ou des données d'objets vers, depuis et entre les services de stockage AWS.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS.

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel des DataSync projets inter-régions GitHub Amazon EFS.

Bonnes pratiques

Suivez les bonnes pratiques décrites dans Bonnes pratiques d'utilisation du kit AWS CDK pour TypeScript créer des projets IaC.

Épopées

Déployez l'application AWS CDK

Tâche	Description	Compétences requises
Clonez le référentiel du projet.	Entrez la commande suivante pour cloner le référentiel du DataSync projet inter-régions Amazon EFS. `git clone https://github.com/aws-samples/aws-efs-crossregion-datasync.git`	AWS DevOps
Installez les dépendances npm.	Entrez la commande suivante. `npm ci`	AWS DevOps
Choisissez les régions principale et secondaire.	Dans le référentiel cloné, accédez au `src/infra` répertoire. Dans le	AWS DevOps

Tâche	Description	Compétences requises
	`Launcher.ts` fichier, mettez à jour les `SECONDARY_AWS_REGION` valeurs `PRIMARY_AWS_REGION` et. Utilisez les codes de région correspondants. `const primaryRegion = { account: account, region: '<PRIMARY_AWS_REGION>' }; const secondaryRegion = { account: account, region: '<SECONDARY_AWS_REGION>' };`	
Démarrez l'environnement.	Entrez la commande suivante pour démarrer le compte AWS et la région AWS que vous souhaitez utiliser. `cdk bootstrap <aws_account>/<aws_region>` Pour plus d'informations, consultez Bootstrapping dans la documentation AWS CDK.	AWS DevOps
Répertoriez les piles AWS CDK.	Entrez la commande suivante pour afficher la liste des piles AWS CDK dans l'application. `cdk ls`	AWS DevOps

Tâche	Description	Compétences requises
Synthétisez les piles AWS CDK.	Entrez la commande suivante pour produire un CloudForm ation modèle AWS pour chaque pile définie dans l'application AWS CDK. `cdk synth`	AWS DevOps
Déployez l'application AWS CDK.	Entrez la commande suivante pour déployer toutes les piles sur votre compte AWS, sans nécessiter d'approbation manuelle pour les modificat ions. `cdk deploy --all --require-approval never`	AWS DevOps

Valider le déploiement

Tâche	Description	Compétences requises
Connectez-vous à l' EC2 instance dans la région principale.	1. À l'aide du gestionnaire de session, une fonctionnalité d'AWS Systems Manager, connectez-vous à l' EC2 instance dans la région principale. Pour obtenir des instructions, consultez Connect to your Linux instance with AWS Systems Manager Session Manager.	AWS DevOps

Tâche	Description	Compétences requises
	2. Remplacez les répertoires par le chemin de montage Amazon EFS. `cd /mnt/efs`	

Créez un fichier temporaire.	Entrez la commande suivante pour créer un fichier temporaire dans le chemin de montage Amazon EFS.
	
	`sudo dd if=/dev/zero \`
	`of=tmptst.dat \`
	`bs=1G \`
	`seek=5 \`
	`count=0`
	
	`ls -lrt tmptst.dat`
		AWS DevOps

Tâche	Description	Compétences requises

Lancez la DataSync tâche.	Entrez la commande suivante pour répliquer le fichier temporaire de la région principale vers la région secondaire, où `<ARN-task>` est le nom de ressource Amazon (ARN) de votre DataSync tâche.
	`aws datasync start-task-execution \`
	`  --task-arn <ARN-task>`
	La commande renvoie l'ARN de l'exécution de la tâche au format suivant.
	`arn:aws:datasync:<region>:<account-ID>:task/task-execution/<exec-ID>`
		AWS DevOps

Tâche	Description	Compétences requises
Vérifiez l'état du transfert de données.	Entrez la commande suivante pour décrire la tâche DataSync d'exécution, où `<ARN-task-execution>` est l'ARN de l'exécution de la tâche. `aws datasync describe-task-execution \ --task-execution-arn <ARN-task-execution>` La DataSync tâche est terminée lorsque `PrepareStatus TransferStatus` , et `VerifyStatus` tous ont la valeur`SUCCESS`.	AWS DevOps
Connectez-vous à l' EC2 instance dans la région secondaire.	1. À l'aide du gestionnaire de session, une fonctionnalité d'AWS Systems Manager, connectez-vous à l' EC2 instance dans la région secondaire. Pour obtenir des instructions, consultez Connect to your Linux instance with AWS Systems Manager Session Manager. 2. Remplacez les répertoires par le chemin de montage Amazon EFS. `cd /mnt/efs`	AWS DevOps

Tâche	Description	Compétences requises
Validez la réplication.	Entrez la commande suivante pour vérifier que le fichier temporaire existe dans le système de fichiers Amazon EFS. `ls -lrt tmptst.dat`	AWS DevOps

Ressources connexes

Documentation AWS

- Référence d'API AWS CDK
- Configuration des DataSync transferts AWS avec Amazon EFS
- Résolution des problèmes liés aux DataSync transferts AWS

Autres ressources AWS

- AWS DataSync FAQs

AWS Infrastructure de test à l'aide LocalStack de tests Terraform

Créée par Ivan Girardi (AWS) et Ioannis Kalyvas (AWS)

Récapitulatif

Ce modèle vous permet de tester localement l'infrastructure sous forme de code (IaC) pour AWS Terraform sans avoir à provisionner l'infrastructure dans votre AWS environnement. Il intègre le framework Terraform Tests à. LocalStack Le conteneur LocalStack Docker fournit un environnement de développement local qui émule divers. Services AWS Cela vous permet de tester et d'itérer les déploiements d'infrastructure sans encourir de coûts. AWS Cloud

Cette solution offre les avantages suivants :

- Optimisation des coûts — L'exécution de tests permet d' LocalStack éliminer le besoin d'utilisation Services AWS. Cela vous évite d'encourir les coûts associés à la création, à l'exploitation et à la modification de ces AWS ressources.
- Rapidité et efficacité — Les tests locaux sont également généralement plus rapides que le déploiement AWS des ressources. Cette boucle de rétroaction rapide accélère le développement et le débogage. Comme il LocalStack s'exécute localement, vous pouvez développer et tester vos fichiers de configuration Terraform sans connexion Internet. Vous pouvez déboguer les fichiers de configuration Terraform localement et recevoir des commentaires immédiats, ce qui rationalise le processus de développement.
- Cohérence et reproductibilité : LocalStack fournit un environnement de test cohérent. Cette cohérence permet de garantir que les tests donnent les mêmes résultats, quels que soient les AWS changements externes ou les problèmes de réseau.
- Isolation : les tests vous LocalStack évitent d'affecter accidentellement les AWS ressources réelles ou les environnements de production. Cette isolation permet d'expérimenter et de tester différentes configurations en toute sécurité.
- Automatisation — L'intégration à un pipeline d'intégration continue et de livraison continue (CI/CD) vous permet de tester automatiquement les fichiers de configuration Terraform. Le pipeline teste minutieusement l'iAc avant le déploiement.
- Flexibilité — Vous pouvez simuler différentes Régions AWS configurations et configurations de service pour mieux correspondre à vos environnements de production. Comptes AWS

Conditions préalables et limitations

Prérequis

- Installer Docker
- Activez l'accès au socket Docker par défaut (`/var/run/docker.sock`). Pour plus d'informations, consultez la documentation LocalStack .
- Installez Docker Compose
- Installez Terraform version 1.6.0 ou ultérieure
- Installez Terraform CLI
- Configurer le fournisseur Terraform AWS
- (Facultatif) Installez et configurez le AWS Command Line Interface (AWS CLI). Pour un exemple d'utilisation du AWS CLI with LocalStack, consultez l'AWS infrastructure de GitHub test utilisant LocalStack et le référentiel de tests Terraform.

Limites

- Ce modèle fournit des exemples explicites pour tester les ressources Amazon Simple Storage Service (Amazon S3) AWS Lambda, AWS Step Functions, et Amazon DynamoDB. Toutefois, vous pouvez étendre cette solution pour inclure des AWS ressources supplémentaires.
- Ce modèle fournit des instructions pour exécuter les tests Terraform localement, mais vous pouvez intégrer les tests dans n'importe quel pipeline CI/CD.
- Ce modèle fournit des instructions pour utiliser l'image de LocalStack la communauté. Si vous utilisez l'image LocalStack Pro, consultez la documentation LocalStack Pro.
- LocalStack fournit des services d'émulation pour différents. AWS APIs Pour une liste complète, voir Couverture des fonctionnalités du AWS service. Certaines fonctionnalités avancées peuvent nécessiter un abonnement LocalStack Pro.

Architecture

Le schéma suivant montre l'architecture de cette solution. Les principaux composants sont un référentiel de code source, un pipeline CI/CD et un conteneur LocalStack Docker. Le conteneur LocalStack Docker héberge les éléments suivants Services AWS localement :

- Un compartiment Amazon S3 pour stocker des fichiers

- Amazon CloudWatch pour la surveillance et la journalisation
- Une AWS Lambda fonction pour exécuter du code sans serveur
- Une machine à AWS Step Functions états pour orchestrer des flux de travail en plusieurs étapes
- Une table Amazon DynamoDB pour stocker des données NoSQL

Le schéma suivant illustre le flux de travail suivant :

1. Vous ajoutez et validez un fichier de configuration Terraform dans le référentiel de code source.
2. Le pipeline CI/CD détecte les modifications et lance un processus de génération pour l'analyse statique du code Terraform. Le pipeline construit et exécute le conteneur LocalStack Docker. Ensuite, le pipeline lance le processus de test.
3. Le pipeline télécharge un objet dans un compartiment Amazon S3 hébergé dans le conteneur LocalStack Docker.
4. Le téléchargement de l'objet appelle une AWS Lambda fonction.
5. La fonction Lambda enregistre la notification d'événement Amazon S3 dans un CloudWatch journal.
6. La fonction Lambda démarre une machine à AWS Step Functions états.
7. La machine d'état écrit le nom de l'objet Amazon S3 dans une table DynamoDB.
8. Le processus de test dans le pipeline CI/CD vérifie que le nom de l'objet chargé correspond à l'entrée de la table DynamoDB. Il vérifie également que le compartiment S3 est déployé avec le nom spécifié et que la AWS Lambda fonction a été déployée avec succès.

Outils

Services AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et autres Services AWS pour créer des applications critiques pour l'entreprise.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- Docker Compose est un outil permettant de définir et d'exécuter des applications multi-conteneurs.
- LocalStackest un émulateur de service cloud qui s'exécute dans un conteneur unique. En utilisant LocalStack, vous pouvez exécuter des charges de travail sur votre machine locale qui l'utilise Services AWS, sans vous connecter au AWS Cloud.
- Terraform est un outil IaC HashiCorp qui vous aide à créer et à gérer des ressources sur site et dans le cloud.
- Terraform Tests vous aide à valider les mises à jour de configuration des modules Terraform par le biais de tests analogues à des tests d'intégration ou unitaires.

Référentiel de code

Le code de ce modèle est disponible dans l'AWS infrastructure de GitHub test à l'aide du LocalStack référentiel Terraform Tests.

Bonnes pratiques

- Cette solution teste AWS l'infrastructure spécifiée dans les fichiers de configuration Terraform et ne déploie pas ces ressources dans le. AWS Cloud Si vous souhaitez déployer les ressources, suivez le principe du moindre privilège (documentation IAM) et configurez correctement le backend Terraform (documentation Terraform).
- Lors de l'intégration LocalStack dans un pipeline CI/CD, nous vous recommandons de ne pas exécuter le conteneur LocalStack Docker en mode privilège. Pour plus d'informations, consultez Privilèges d'exécution et fonctionnalités Linux (documentation Docker) et Sécurité pour les coureurs autogérés (GitLab documentation).

Épopées

Déployez la solution

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Dans un shell bash, entrez la commande suivante. Cela clone l'AWS infrastructure de test à l'aide d'un référentiel LocalStack de tests Terraform à partir de : GitHub `git clone https://github.com/aws-samples/localstack-terraform-test.git`	DevOps ingénieur

Faites fonctionner le LocalStack conteneur.	1. Entrez la commande suivante pour accéder au référentiel cloné :
	`cd localstack-terraform-test`
	2. Entrez la commande suivante pour démarrer le conteneur LocalStack Docker en mode détaché :
	`docker-compose up -d`
	3. Attendez que le conteneur LocalStack Docker soit opérationnel.
		DevOps ingénieur

Initialisez Terraform.	Entrez la commande suivante pour initialiser Terraform :	DevOps ingénieur

Tâche	Description	Compétences requises
	`terraform init`	

Exécutez des tests Terraform.	1. Entrez la commande suivante pour exécuter les tests Terraform :
	`terraform test`
	2. Vérifiez que tous les tests ont été effectués avec succès. La sortie doit ressembler à ce qui suit :
	`Success! 3 passed, 0 failed.`
		DevOps ingénieur

Nettoyez les ressources.	Entrez la commande suivante pour détruire le LocalStack conteneur : `docker-compose down`	DevOps ingénieur

Résolution des problèmes

Problème	Solution
`Error: reading DynamoDB Table Item (Files|README.md): empty` résultat lors de l'exécution de la `terraform test` commande.	1. Entrez à nouveau la `terraform test` commande. 2. Si cela ne résout pas l'erreur, modifiez le fichier main.tf pour augmenter le délai de veille à une valeur supérieure à 15 secondes : `resource "time_sleep" "wait" {`

Problème	Solution

	create_duration = "15s"
	triggers = {
	s3_object = local.key_json
	}
	}

Ressources connexes

- Commencer à utiliser Terraform : conseils pour AWS CDK et AWS CloudFormation experts (conseils AWS prescriptifs)
- Meilleures pratiques d'utilisation du AWS fournisseur Terraform (directives AWS prescriptives)
- Terraform CI/CD et poursuite des tests AWS avec le nouveau Terraform Test Framework (article de blog)AWS
- Accélérer la livraison de logiciels à l'aide de LocalStack Cloud Emulator depuis AWS Marketplace (article de AWS blog)

Informations supplémentaires

Intégration avec les GitHub actions

Vous pouvez intégrer LocalStack et Terraform des tests dans un pipeline CI/CD à l'aide d'Actions. GitHub Pour plus d'informations, consultez la documentation sur GitHub les actions. Voici un exemple de fichier de configuration d' GitHub actions :

```
name: LocalStack Terraform Test

on:
  push:
    branches:
      - '**'

  workflow_dispatch: {}

jobs:
  localstack-terraform-test:
    runs-on: ubuntu-latest
```

```
    steps:
    - uses: actions/checkout@v4

    - name: Build and Start LocalStack Container
      run: |
        docker compose up -d

    - name: Setup Terraform
      uses: hashicorp/setup-terraform@v3
      with:
        terraform_version: latest

    - name: Run Terraform Init and Validation
      run: |
        terraform init
        terraform validate
        terraform fmt --recursive --check
        terraform plan
        terraform show

    - name: Run Terraform Test
      run: |
        terraform test

    - name: Stop and Delete LocalStack Container
      if: always()
      run: docker compose down
```

Mettez à niveau les clusters SAP Pacemaker de ENSA1 ENSA2

Créée par Gergely Cserdi (AWS) et Balazs Sandor Skublics (AWS)

Récapitulatif

Ce modèle explique les étapes et les considérations relatives à la mise à niveau d'un cluster SAP Pacemaker basé sur un serveur d'attente autonome () ENSA1 vers. ENSA2 Les informations contenues dans ce modèle s'appliquent à la fois aux systèmes d'exploitation SUSE Linux Enterprise Server (SLES) et Red Hat Enterprise Linux (RHEL).

Les clusters Pacemaker sur SAP NetWeaver 7.52 ou S/4HANA 1709 et versions antérieures s'exécutent sur une ENSA1 architecture et sont configurés spécifiquement pour. ENSA1 Si vous exécutez vos charges de travail SAP sur Amazon Web Services (AWS) et que vous souhaitez passer à Amazon ENSA2, vous constaterez peut-être que la documentation SAP, SUSE et RHEL ne fournit pas d'informations complètes. Ce modèle décrit les étapes techniques requises pour reconfigurer les paramètres SAP et les clusters Pacemaker à partir ENSA1 de. ENSA2 Il fournit des exemples de systèmes SUSE, mais le concept est le même pour les clusters RHEL.

> Remarques : ENSA1 et ce ENSA2 sont des concepts qui concernent uniquement les applications SAP. Les informations de ce modèle ne s'appliquent donc pas à SAP HANA ou à d'autres types de clusters.
>
> Techniquement, il ENSA2 peut être utilisé avec ou sans Enqueue Replicator 2. Cependant, la haute disponibilité (HA) et l'automatisation du basculement (via une solution de cluster) nécessite nt Enqueue Replicator 2. Ce modèle utilise le terme ENSA2 clusters pour désigner les clusters dotés de Standalone Enqueue Server 2 et Enqueue Replicator 2.

Conditions préalables et limitations

Prérequis

- Un cluster fonctionnel ENSA1 qui utilise Pacemaker et Corosync sur SLES ou RHEL.
- Au moins deux instances Amazon Elastic Compute Cloud (Amazon EC2) sur lesquelles les instances (ABAP) SAP Central Services (ASCS/SCS) et Enqueue Replication Server (ERS) sont exécutées.
- Connaissance de la gestion des applications et des clusters SAP.

- Accès à l'environnement Linux en tant qu'utilisateur root.

Limites

- ENSA1les clusters basés sur une architecture à deux nœuds ne supportent qu'une architecture à deux nœuds.
- ENSA2les clusters basés sur SAP ne peuvent pas être déployés sur les NetWeaver versions de SAP antérieures à la version 7.52.
- EC2 les instances des clusters doivent se trouver dans des zones de disponibilité AWS différentes.

Versions du produit

- SAP NetWeaver version 7.52 ou ultérieure
- À partir de S/4HANA 2020, seuls les clusters sont pris en charge ENSA2
- Kernel 7.53 ou version ultérieure, qui prend en charge ENSA2 et Enqueue Replicator 2
- SLES pour applications SAP version 12 ou ultérieure
- RHEL pour SAP avec haute disponibilité (HA) version 7.9 ou ultérieure

Architecture

Pile technologique source

- SAP NetWeaver 7.52 avec SAP Kernel 7.53 ou version ultérieure
- Système d'exploitation SLES ou RHEL

Pile technologique cible

- SAP NetWeaver 7.52 avec SAP Kernel 7.53 ou version ultérieure, y compris S/4HANA 2020 avec plate-forme ABAP
- Système d'exploitation SLES ou RHEL

Architecture cible

Le schéma suivant montre une configuration HA d'instances ASCS/SCS et ERS basée sur un cluster. ENSA2

Comparaison de ENSA2 clusters ENSA1 et de clusters

SAP a été introduit ENSA2 en tant que successeur de ENSA1. Un cluster ENSA1 basé prend en charge une architecture à deux nœuds dans laquelle l'ASCS/SCS instance fails over to ERS when an error occurs. This limitation stems from how the ASCS/SCS instance regains the lock table information from the shared memory of the ERS node after failover. ENSA2-based clusters with Enqueue Replicator 2 eliminate this limitation, because the ASCS/SCS instance can collect the lock information from the ERS instance over the network. ENSA2-based clusters can have more than two nodes, because the ASCS/SCS instance is no longer required to fail over to the ERS node. (However, in a two-node ENSA2 cluster environment, the ASCS/SCSinstance bascule toujours vers le nœud ERS car il n'y a aucun autre nœud du cluster vers lequel basculer.) ENSA2 est pris en charge à partir de SAP Kernel 7.50 avec certaines limitations. Pour une configuration HA qui prend en charge Enqueue Replicator 2, la configuration minimale requise est de NetWeaver 7,52 (voir la note SAP OSS 2630416). S/4HANA 1809 est livré avec une ENSA2 architecture recommandée par défaut, tandis que S/4HANA ne prend en charge qu'à partir de la version 2020. ENSA2

Automatisation et mise à l'échelle

Le cluster HA de l'architecture cible permet à ASCS de basculer automatiquement vers d'autres nœuds.

Scénarios de migration vers des clusters ENSA2 basés

Il existe deux scénarios principaux pour la mise à niveau vers ENSA2 des clusters basés :

- Scénario 1 : vous choisissez de passer à une version ENSA2 sans mise à niveau SAP ou conversion S/4HANA associée, en supposant que votre version SAP et votre version du noyau soient compatibles. ENSA2
- Scénario 2 : vous passez à ENSA2 SUM dans le cadre d'une mise à niveau ou d'une conversion (par exemple, vers S/4HANA 1809 ou version ultérieure).

La section Epics décrit les étapes de ces deux scénarios. Le premier scénario vous oblige à configurer manuellement les paramètres liés à SAP avant de modifier la configuration du cluster pour ENSA2. Dans le second scénario, les fichiers binaires et les paramètres liés à SAP sont déployés par SUM, et il ne vous reste plus qu'à mettre à jour la configuration du cluster pour HA. Nous vous recommandons tout de même de valider les paramètres SAP après avoir utilisé SUM. Dans la plupart des cas, la conversion S/4HANA est la principale raison d'une mise à niveau du cluster.

Outils

- Pour les gestionnaires de packages de systèmes d'exploitation, nous recommandons les outils Zypper (pour SLES) ou YUM (pour RHEL).
- Pour la gestion des clusters, nous recommandons les shells crm (pour SLES) ou pcs (pour RHEL).
- Outils de gestion des instances SAP tels que SAPControl.
- Outil SUM (facultatif) pour la mise à niveau de conversion de S/4HANA.

Bonnes pratiques

- Pour connaître les meilleures pratiques relatives à l'utilisation des charges de travail SAP sur AWS, consultez le SAP Lens for the AWS Well-Architected Framework.
- Tenez compte du nombre de nœuds de cluster (pair ou impair) dans votre architecture à ENSA2 nœuds multiples.
- Configurez le ENSA2 cluster pour SLES 15 conformément à la norme de certification SAP S/4-HA-CLU 1.0.
- Enregistrez ou sauvegardez toujours l'état de votre cluster et de votre application existants avant de procéder à la mise à niveau vers ENSA2.

Épopées

Configurer les paramètres SAP manuellement pour ENSA2 (scénario 1 uniquement)

Tâche	Description	Compétences requises
Configurez les paramètres dans le profil par défaut.	Si vous souhaitez effectuer une mise à niveau ENSA2 tout en conservant la même version SAP ou si votre version cible est la valeur par défaut ENSA1, définissez les paramètres du profil par défaut (fichier DEFAULT.PFL) sur les valeurs suivantes. `enq/enable=TRUE`	SAP

Tâche	Description	Compétences requises

	``
	enq/serverhost=sapas
	csvirt
	enq/serverinst=10
	    (instance number of
	 ASCS/SCS instance)
	enque/process_loc
	ation=REMOTESA
	enq/replicatorhost=sa
	persvirt
	enq/replicatorinst=11
	    (instance number of
	 ERS instance)
	``
	
	où `sapascsvirt` est le nom d'hôte virtuel pour les instances ASCS, et `sapersvirt` est le nom d'hôte virtuel pour les instances ERS. Vous pouvez les modifier pour les adapter à votre environnement cible.
	
	Note
	Pour utiliser cette option de mise à niveau, votre version SAP et votre version du noyau doivent prendre en charge ENSA2 Enqueue Replicator 2.	

Tâche	Description	Compétences requises
Configurez le profil d'instance ASCS/SCS.	Si vous souhaitez effectuer une mise à ENSA2 niveau vers la même version de SAP ou si votre version cible est la valeur par défaut ENSA1, définissez les paramètre s suivants dans le profil d'instance ASCS/SCS. La section du profil où ENSA1 est défini ressemble à ce qui suit. `#----------------- ----------------- ----------------- --------- Start SAP enqueue server #------------------ ----------------- ----------------- ------- _EN = en.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_04 = local rm - f $(_EN) Execute_05 = local ln - s -f $(DIR_EXECUTABLE)/ enserver$(FT_EXE) $(_EN) Start_Program_01 = local $(_EN) pf=$(_PF)` Pour reconfigurer cette section pour ENSA2 :	SAP

Tâche	Description	Compétences requises
	1. Modifiez le préfixe du `_EN` programme en `_ENQ` fonction des dernières informations de SAP (OSS Note 2501860 ; nécessite un compte utilisateur SAP ONE Support Launchpad). 2. Remplacez le binaire du serveur de file d'`enserver`attente par. `enq_server` 3. Définissez le nouveau paramètre `enq/server/replication/enable` sur`TRUE`. 4. Assurez-vous de cela`Autostart = 0`. Cette section de profil ressemblera à ce qui suit après vos modifications. `#----------------- ----------------- ----------------- --------- Start SAP enqueue server #------------------- ----------------- ----------------- ------- _ENQ = enq.sap$( SAPSYSTEMNAME)$(IN STANCE_NAME) Execute_04 = local rm - f $(_ENQ)`	

Tâche	Description	Compétences requises

	`Execute_05 = local ln -s -f $(DIR_EXECUTABLE)/enq_server$(FT_EXE) $(_ENQ)`
	`Start_Program_01 = local $(_ENQ) pf=$(_PF)`
	`...`
	`enq/server/replication/enable = TRUE`
	`Autostart = 0`
	
	⚠ Important
	_ENQl'option de redémarrage ne doit pas être activée. S'`RestartProgram_01` il est défini pour_ENQ, remplacez-le par`StartProgram_01` . Cela empêche SAP de redémarrer le service ou d'interférer avec les ressources gérées par le cluster.	

Tâche	Description	Compétences requises
Configurez le profil ERS.	Si vous souhaitez effectuer une mise à ENSA2 niveau vers la même version de SAP ou si votre version cible est par défaut ENSA1, définissez les paramètres suivants dans le profil d'instance ERS. Trouvez la section dans laquelle le réplicateur de files d'attente est défini. Ce sera similaire à ce qui suit. `#------------------ ------------------ ------------------- Start enqueue replicati on server #------------------- ------------------ ------------------ _ER = er.sap$(S APSYSTEMNAME)$(INS TANCE_NAME) Execute_03 = local rm - f $(_ER) Execute_04 = local ln - s -f $(DIR_EXECUTABLE)/ enrepserver$(FT_EXE) $(_ER) Start_Program_00 = local $(_ER) pf=$(_PF) NR=$(SCSID)` Pour reconfigurer cette section pour Enqueue Replicator 2 :	SAP

Tâche	Description	Compétences requises
	1. Modifiez le préfixe du `_ER` programme en `_ENQR` fonction des dernières notes de SAP (OSS Note 2501860 ; nécessite un compte utilisateur SAP ONE Support Launchpad). 2. Remplacez le binaire du réplicateur de file d'attente par`enq_replicator . enrepserver` 3. Assurez-vous de cela`Autostart = 0`. Cette section de profil devrait ressembler à ce qui suit après vos modifications. `#------------------ ------------------ ------------------- Start enqueue replicati on server #------------------- ------------------ ----------------- _ENQR = enqr.sap$ (SAPSYSTEMNAME)$(I NSTANCE_NAME) Execute_01 = local rm - f $(_ENQR) Execute_02 = local ln - s -f $(DIR_EXECUTABLE)/ enq_replicator$(FT _EXE) $(_ENQR)`	

Tâche	Description	Compétences requises
	`Start_Program_00 = local $(_ENQR) pf= $(_PF) NR=$(SCSID) … Autostart = 0`	
	Important _ENQRl'option de redémarrage ne doit pas être activée. S'`RestartProgram_01` il est défini pour_ENQR, remplacez-le par`StartProgram_01` . Cela empêche SAP de redémarrer le service ou d'interférer avec les services gérés par cluster.	

Tâche	Description	Compétences requises

Redémarrez SAP Start Services.	Après avoir modifié les profils décrits précédemment dans cet article épique, redémarre z SAP Start Services pour ASCS/SCS et ERS.
	
	`sapcontrol -nr 10 -function RestartSe rvice SCT`
	
	`sapcontrol -nr 11 -function RestartSe rvice SCT`
	
	où `SCT` fait référence à l'ID du système SAP, et en supposant que 10 et 11 sont les numéros d'instance pour les instances ASCS/SCS et ERS, respectiv ement.
		SAP

Reconfigurer le cluster pour ENSA2 (obligatoire pour les deux scénarios)

Tâche	Description	Compétences requises
Vérifiez les numéros de version dans les agents de ressources SAP.	Lorsque vous utilisez SUM pour mettre à niveau SAP vers S/4HANA 1809 ou une version ultérieure, SUM gère les modifications de paramètre s dans les profils SAP. Seul le cluster nécessite un réglage manuel. Toutefois, nous vous recommandons de vérifier les	Administrateur système AWS

Tâche	Description	Compétences requises
	paramètres avant d'apporter des modifications au cluster. **Note** Les exemples présentés dans cette épopée supposent que vous utilisez le système d'exploitation SUSE. Si vous utilisez RHEL, vous devrez utiliser des outils tels que YUM et le shell PCs au lieu de Zypper et CRM. Vérifiez les deux nœuds de l'architecture pour vérifier que le `resource-agents` package correspond à la version minimale recommandée par SAP. Pour SLES, consultez la note SAP OSS 2641019. Pour RHEL, consultez la note SAP OSS 2641322. (SAP Notes nécessite un compte utilisateur SAP ONE Support Launchpad.) `sapers:sctadm 23> zypper search -s -i resource-agents`	

Tâche	Description	Compétences requises
	`Loading repository data... Reading installed packages... S | Name | Type | Version | Arch | Repository --+------------ ----+---------+--- ------------------ ---------------+-- ------+----------- ------------------ i | resource-agents | package | 4.8.0+git 30.d0077df0-150300 .8.28.1 | x86_64 | SLE-Product-HA15-SP3-Updates`  Mettez à jour la `resource-agents` version si nécessaire.	
Sauvegardez la configuration du cluster.	Sauvegardez la configuration du cluster CRM comme suit. `crm configure show > /tmp/cluster_config_backup.txt`	Administrateur système AWS
Définissez le mode de maintenance.	Réglez le cluster en mode maintenance. `crm configure property maintenance-mode="true"`	Administrateur système AWS

Tâche	Description	Compétences requises

Vérifiez la configuration du cluster.	Vérifiez la configuration actuelle du cluster.
	`crm configure show`
	Voici un extrait de la sortie complète :
	`node 1: sapascs`
	`node 2: sapers`
	`...`
	`primitive rsc_sap_S`
	`CT_ASCS10 SAPInstance`
	`\`
	`operations $id=rsc_s`
	`ap_SCT_ASCS10-oper`
	`ations \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
	`params InstanceN`
	`ame=SCT_ASCS10_sap`
	`ascsvirt START_PRO`
	`FILE="/sapmnt/SCT/`
	`profile/SCT_ASCS10`
	`_sapascsvirt" \`
	`AUTOMATIC_RECOVER=`
	`false \`
	`meta resource-stickines`
	`s=5000 failure-t`
	`imeout=60 migration-`
	`threshold=1 priority=`
	`10`
	`primitive rsc_sap_S`
	`CT_ERS11 SAPInstance \`
	`operations $id=rsc_s`
	`ap_SCT_ERS11-opera`
	`tions \`
	`op monitor interval=120`
	`timeout=60 on-fail=r`
	`estart \`
		Administrateur système AWS

Tâche	Description	Compétences requises

	<pre>params InstanceN
	ame=SCT_ERS11_sape
	rsvirt START_PRO
	FILE="/sapmnt/SCT/
	profile/SCT_ERS11_
	sapersvirt" \
	   AUTOMATIC_RECOVER=
	false IS_ERS=true \
	meta priority=1000
	...
	colocation col_sap_S
	CT_no_both -5000:
	 grp_SCT_ERS11
	 grp_SCT_ASCS10
	location loc_sap_S
	CT_failover_to_ers
	 rsc_sap_SCT_ASCS10 \
	rule 2000: runs_ers_SCT
	 eq 1
	order ord_sap_S
	CT_first_start_asc
	s Optional: rsc_sap_S
	CT_ASCS10:start
	 rsc_sap_SCT_ERS11:
	stop symmetrical=false
	...</pre> où `sapascsvirt` fait référence au nom d'hôte virtuel pour les instances ASCS, `sapersvirt` fait référence au nom d'hôte virtuel pour les instances ERS et SCT fait référence à l'ID du système SAP.	

Tâche	Description	Compétences requises
Supprimez la contrainte de colocation en cas de basculement.	Dans l'exemple précédent, la contrainte de localisation `loc_sap_SCT_failover_to_ers` indique que la ENSA1 fonctionnalité d'ASCS doit toujours suivre l'instance ERS en cas de basculement. Avec ENSA2, ASCS devrait pouvoir basculer librement vers tous les nœuds participants. Vous pouvez donc supprimer cette contrainte. `crm configure delete loc_sap_SCT_failover_to_ers`	Administrateur système AWS

Tâche	Description	Compétences requises

Ajustez les primitives.	Vous devrez également apporter des modifications mineures aux SAPInstance primitives ASCS et ERS.
	
	Voici un exemple de SAPInstance primitive ASCS configurée pour ENSA1.
	
	`primitive rsc_sap_SCT_ASCS10 SAPInstance \`
	`operations $id=rsc_sap_SCT_ASCS10-operations \`
	`op monitor interval=120 timeout=60 on-fail=restart \`
	`params InstanceName=SCT_ASCS10_sapascsvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ASCS10_sapascsvirt" \`
	`AUTOMATIC_RECOVER=false \`
	`meta resource-stickiness=5000 failure-timeout=60 migration-threshold=1 priority=10`
	
	Pour effectuer une mise à niveau vers ENSA2, modifiez cette configuration comme suit.
		Administrateur système AWS

Tâche	Description	Compétences requises
	`primitive rsc_sap_S CT_ASCS10 SAPInstance \ operations $id=rsc_s ap_SCT_ASCS10-oper ations \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ASCS10_sap ascsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ASCS10 _sapascsvirt" \ AUTOMATIC_RECOVER= false \ meta resource-stickines s=3000`  Il s'agit d'un exemple de SAPInstance primitive ERS configurée pour ENSA1.  `primitive rsc_sap_S CT_ERS11 SAPInstance \ operations $id=rsc_s ap_SCT_ERS11-opera tions \ op monitor interval=120 timeout=60 on-fail=r estart \ params InstanceN ame=SCT_ERS11_sape rsvirt START_PRO FILE="/sapmnt/SCT/ profile/SCT_ERS11_ sapersvirt" \ AUTOMATIC_RECOVER= false IS_ERS=true \`	

Tâche	Description	Compétences requises

	`meta priority=1000`
	
	Pour effectuer une mise à niveau vers ENSA2, modifiez cette configuration comme suit.
	
	`primitive rsc_sap_SCT_ERS11 SAPInstance \ operations $id=rsc_sap_SCT_ERS11-operations \ op monitor interval=120 timeout=60 on-fail=restart \ params InstanceName=SCT_ERS11_sapersvirt START_PROFILE="/sapmnt/SCT/profile/SCT_ERS11_sapersvirt" \ AUTOMATIC_RECOVER=false IS_ERS=true`
	
	Vous pouvez modifier les primitives de différentes manières. Par exemple, vous pouvez les réviser dans un éditeur tel que vi, comme dans l'exemple suivant.
	
	`crm configure edit rsc_sap_SCT_ERS11`	

Tâche	Description	Compétences requises
Désactivez le mode maintenance.	Désactivez le mode maintenance sur le cluster. `crm configure property maintenance-mode="false"` Lorsque le cluster sort du mode maintenance, il tente de mettre en ligne les instances ASCS et ERS avec les nouveaux ENSA2 paramètres.	Administrateur système AWS

(Facultatif) Ajoutez des nœuds de cluster

Tâche	Description	Compétences requises
Passez en revue les meilleures pratiques.	Avant d'ajouter d'autres nœuds, assurez-vous de comprendre les meilleures pratiques, par exemple s'il faut utiliser un nombre pair ou impair de nœuds.	Administrateur système AWS
Ajoutez des nœuds.	L'ajout de nœuds supplémentaires implique une série de tâches, telles que la mise à jour du système d'exploitation, l'installation de progiciels correspondant aux nœuds existants et la mise à disposition de montages. Vous pouvez utiliser l'option Prepare Additional Host dans SAP Software Provision	Administrateur système AWS

Tâche	Description	Compétences requises
	ing Manager (SWPM) pour créer une base de référence spécifique à SAP pour l'hôte. Pour plus d'informations, consultez les guides SAP répertoriés dans la section suivante.	

Ressources connexes

Références SAP et SUSE

Pour accéder à SAP Notes, vous devez disposer d'un compte utilisateur SAP ONE Support Launchpad. Pour de plus amples informations, veuillez consulter le site web du support SAP.

- SAP Note 2501860 – Documentation du serveur d' NetWeaver applications SAP pour ABAP 7.52
- SAP Note 2641019 – Installation ENSA2 et mise à jour de ENSA1 vers ENSA2 dans l'environnement SUSE HA
- Note SAP 2641322 – Installation ENSA2 et mise à jour de ENSA1 vers ENSA2 lors de l'utilisation des solutions Red Hat HA pour SAP
- SAP Note 2711036 – Utilisation du serveur d'attente autonome 2 dans un environnement HA
- Serveur de file d'attente autonome 2 (documentation SAP)
- SAP S/4 HANA – Cluster haute disponibilité Enqueue Replication 2 - Guide de configuration (documentation SUSE)

Références AWS

- SAP HANA sur AWS : guide de configuration de haute disponibilité pour SLES et RHEL
- SAP Lens - Cadre AWS Well-Architected

Utilisez des zones de disponibilité cohérentes VPCs sur les différents comptes AWS

Créée par Adam Spicer (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), le nom d'une zone de disponibilité peut varier selon vos comptes AWS et un ID de zone de disponibilité (AZ ID) qui identifie son emplacement. Si vous utilisez AWS CloudFormation pour créer des clouds privés virtuels (VPCs), vous devez spécifier le nom ou l'ID de la zone de disponibilité lors de la création des sous-réseaux. Si vous créez VPCs plusieurs comptes, le nom de la zone de disponibilité est aléatoire, ce qui signifie que les sous-réseaux utilisent des zones de disponibilité différentes dans chaque compte.

Pour utiliser la même zone de disponibilité sur tous vos comptes, vous devez associer le nom de la zone de disponibilité de chaque compte au même AZ ID. Par exemple, le schéma suivant montre que l'ID `use1-az6` AZ est nommé `us-east-1a` dans le compte AWS A et `us-east-1c` dans le compte AWS Z.

Ce modèle permet de garantir la cohérence zonale en fournissant une solution évolutive entre comptes permettant d'utiliser les mêmes zones de disponibilité dans vos sous-réseaux. La cohérence zonale garantit que le trafic réseau entre comptes évite les chemins réseau entre zones de disponibilité, ce qui permet de réduire les coûts de transfert de données et de réduire la latence réseau entre vos charges de travail.

Ce modèle constitue une approche alternative à la CloudFormation AvailabilityZoneId propriété AWS.

Conditions préalables et limitations

Prérequis

- Au moins deux comptes AWS actifs dans la même région AWS.
- Évaluez le nombre de zones de disponibilité nécessaires pour répondre à vos besoins en matière de VPC dans la région.
- Identifiez et enregistrez l'ID AZ pour chaque zone de disponibilité que vous devez prendre en charge. Pour plus d'informations à ce sujet, consultez la section Zone IDs de disponibilité de vos ressources AWS dans la documentation d'AWS Resource Access Manager.

- Une liste ordonnée, séparée par des virgules, de votre AZ. IDs Par exemple, la première zone de disponibilité de votre liste est mappée en tant que`az1`, la seconde zone de disponibilité est mappée en tant que`az2`, et cette structure de mappage continue jusqu'à ce que votre liste séparée par des virgules soit entièrement mappée. Il n'y a pas de nombre maximum d'AZ IDs qui peuvent être mappés.
- Le `az-mapping.yaml` fichier du référentiel de mappage des zones de disponibilité GitHub multicomptes, copié sur votre machine locale

Architecture

Le schéma suivant montre l'architecture déployée dans un compte et qui crée les valeurs de l'AWS Systems Manager Parameter Store. Ces valeurs du Parameter Store sont consommées lorsque vous créez un VPC dans le compte.

Le schéma suivant illustre le flux de travail suivant :

1. La solution de ce modèle est déployée sur tous les comptes qui nécessitent une cohérence zonale pour un VPC.
2. La solution crée des valeurs de magasin de paramètres pour chaque ID AZ et stocke le nouveau nom de zone de disponibilité.
3. Le CloudFormation modèle AWS utilise le nom de la zone de disponibilité stocké dans chaque valeur du magasin de paramètres, ce qui garantit la cohérence zonale.

Le schéma suivant montre le flux de travail pour créer un VPC avec la solution de ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. Soumettez un modèle pour créer un VPC à AWS. CloudFormation
2. AWS CloudFormation résout les valeurs du magasin de paramètres pour chaque zone de disponibilité et renvoie le nom de la zone de disponibilité pour chaque ID AZ.
3. Un VPC est créé avec la bonne AZ IDs requise pour la cohérence zonale.

Après avoir déployé la solution de ce modèle, vous pouvez créer des sous-réseaux qui font référence aux valeurs du Parameter Store. Si vous utilisez AWS CloudFormation, vous pouvez référencer les valeurs des paramètres de mappage de la zone de disponibilité à partir de l'exemple de code au format YAML suivant :

```
Resources:
    PrivateSubnet1AZ1:
        Type: AWS::EC2::Subnet
        Properties:
            VpcId: !Ref VPC
            CidrBlock: !Ref PrivateSubnetAZ1CIDR
            AvailabilityZone:
                !Join
                    - ''
                    - - '{{resolve:ssm:/az-mapping/az1:1}}'
```

Cet exemple de code est contenu dans le `vpc-example.yaml` fichier du référentiel de mappage des zones de disponibilité GitHub multicomptes. Il explique comment créer un VPC et des sous-réseaux qui s'alignent sur les valeurs du Parameter Store pour garantir la cohérence zonale.

Pile technologique

- AWS CloudFormation
- AWS Lambda
- AWS Systems Manager Parameter Store

Automatisation et mise à l'échelle

Vous pouvez déployer ce modèle sur tous vos comptes AWS à l'aide d'AWS CloudFormation StackSets ou de la solution Customizations for AWS Control Tower. Pour plus d'informations, consultez Working with AWS CloudFormation StackSets dans la documentation AWS Cloudformation et Customizations for AWS Control Tower dans la bibliothèque de solutions AWS.

Après avoir déployé le CloudFormation modèle AWS, vous pouvez le mettre à jour pour utiliser les valeurs du Parameter Store et le déployer VPCs dans des pipelines ou selon vos besoins.

Outils

Services AWS

- AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.
- AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- AWS Systems Manager Parameter Store est une fonctionnalité d'AWS Systems Manager. Il fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Code

Le code de ce modèle est fourni dans le référentiel de mappage des zones de disponibilité GitHub multicomptes.

Épopées

Déployez le fichier az-mapping.yaml

Tâche	Description	Compétences requises
Déterminez les zones de disponibilité requises pour la région.	1. Déterminez l'AZ IDs qui doit être systématiquement utilisé dans votre région. 2. Enregistrez ces AZ IDs dans une liste séparée par des virgules et dans l'ordre dans lequel vous souhaitez qu'ils soient appliqués. Par exemple, la première zone de disponibilité de votre liste est mappée comme `az1` et la seconde est	Architecte du cloud

Tâche	Description	Compétences requises
	mappée comme. `az2` Il n'y a pas de nombre maximum d'AZ IDs qui peuvent être mappés.	
Déployez le fichier az-mappin g.yaml.	Utilisez le `az-mappin g.yaml` fichier pour créer une CloudFormation pile AWS dans tous les comptes AWS requis. Dans le `AZIds` paramètre, utilisez la liste séparée par des virgules que vous avez créée précédemm ent. Nous vous recommandons d'utiliser AWS CloudForm ation StackSets ou la solution Customizations for AWS Control Tower.	Architecte du cloud

Déployez le VPCs dans vos comptes

Tâche	Description	Compétences requises
Personnalisez les CloudForm ation modèles AWS.	Lorsque vous créez les sous-réseaux à l'aide d'AWS CloudFormation, personnal isez les modèles pour utiliser les valeurs du magasin de paramètres que vous avez créées précédemment. Pour un exemple de modèle, consultez le `vpc-examp`	Architecte du cloud

Tâche	Description	Compétences requises
	`le.yaml` fichier dans le référentiel de mappage des zones de disponibilité GitHub multicomptes.	
Déployez le VPCs.	Déployez les CloudFormation modèles AWS personnalisés dans vos comptes. Chaque VPC de la région possède alors une cohérence zonale dans les zones de disponibi lité utilisées pour les sous-rése aux.	Architecte du cloud

Ressources connexes

- Zone de disponibilité IDs pour vos ressources AWS (documentation AWS Resource Access Manager)
- AWS::EC2::Subnet(CloudFormation documentation AWS)

Utiliser l'utilisateur IDs dans les politiques IAM pour le contrôle d'accès et l'automatisation

Créée par Srinivas Ananda Babu (AWS) et Ram Kandaswamy (AWS)

Récapitulatif

Ce modèle explique les pièges potentiels liés à l'utilisation de politiques basées sur le nom d'utilisateur dans AWS Identity and Access Management (IAM), les avantages de l'utilisation de l'utilisateur IDs et la manière d'intégrer cette approche à l'automatisation. AWS CloudFormation

Dans le AWS Cloud, le service IAM vous aide à gérer les identités des utilisateurs et le contrôle d'accès avec précision. Cependant, le recours aux noms d'utilisateur lors de la création de politiques IAM peut entraîner des risques de sécurité imprévus et des problèmes de contrôle d'accès. Par exemple, imaginez ce scénario : un nouvel employé, John Doe, rejoint votre équipe et vous créez un compte utilisateur IAM avec le nom d'utilisateur`j.doe`, qui lui accorde des autorisations par le biais de politiques IAM faisant référence à des noms d'utilisateur. Lorsque John quitte l'entreprise, le compte est supprimé. Le problème commence lorsqu'une nouvelle employée, Jane Doe, rejoint votre équipe et que le `j.doe` nom d'utilisateur est recréé. Les politiques existantes accordent désormais à Jane Doe les mêmes autorisations qu'à John Doe. Cela crée un véritable cauchemar en matière de sécurité et de conformité.

La mise à jour manuelle de chaque politique pour refléter les informations des nouveaux utilisateurs est un processus long et sujet aux erreurs, en particulier à mesure que votre organisation se développe. La solution consiste à utiliser un identifiant utilisateur unique et immuable. Lorsque vous créez un compte utilisateur IAM, AWS attribuez à l'utilisateur IAM un ID utilisateur unique (ou ID principal). Vous pouvez utiliser ces utilisateurs IDs dans vos politiques IAM pour garantir un contrôle d'accès cohérent et fiable qui n'est pas affecté par les modifications ou la réutilisation du nom d'utilisateur.

Par exemple, une politique IAM qui utilise un ID utilisateur peut ressembler à ceci :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::example-bucket",
            "Principal": { "AWS": "arn:aws:iam::123456789012:user/abcdef01234567890" }
```

```
        }
      ]
}
```

Les avantages de l'utilisation de l'utilisateur IDs dans les politiques IAM sont les suivants :

- Unicité. IDs Les utilisateurs étant uniques Comptes AWS, ils fournissent une application d'autorisation correcte et cohérente.
- Immuabilité. L'utilisateur IDs ne pouvant pas être modifié, ils fournissent un identifiant stable pour référencer les utilisateurs dans les politiques.
- Audit et conformité. Services AWS Incluez souvent l'utilisateur IDs dans les journaux et les pistes d'audit, ce qui permet de retracer facilement les actions jusqu'à des utilisateurs spécifiques.
- Automatisation et intégration. L'utilisation de scripts user IDs in AWS APIs ou d'automatisation garantit que les processus ne sont pas affectés par les changements de nom d'utilisateur. SDKs
- À l'épreuve du futur. L'utilisation de l'utilisateur IDs dans les politiques dès le départ peut éviter d'éventuels problèmes de contrôle d'accès ou des mises à jour importantes des politiques.

Automation

Lorsque vous utilisez des outils d'infrastructure en tant que code (IaC) tels que AWS CloudFormation les pièges des politiques IAM basées sur le nom d'utilisateur peuvent toujours poser problème. La ressource utilisateur IAM renvoie le nom d'utilisateur lorsque vous appelez la fonction `Ref` intrinsèque. À mesure que l'infrastructure de votre entreprise évolue, le cycle de création et de suppression de ressources, y compris les comptes utilisateur IAM, peut entraîner des problèmes de contrôle d'accès involontaires si vous réutilisez les noms d'utilisateur.

Pour résoudre ce problème, nous vous recommandons d'intégrer l'utilisateur IDs dans vos CloudFormation modèles. Cependant, il peut être difficile IDs d'obtenir un utilisateur à cette fin. C'est là que les ressources personnalisées peuvent être utiles. Vous pouvez utiliser des ressources CloudFormation personnalisées pour étendre les fonctionnalités du service en intégrant des services externes AWS APIs ou en les intégrant. En créant une ressource personnalisée qui récupère l'ID utilisateur d'un utilisateur IAM donné, vous pouvez le rendre disponible dans vos CloudFormation modèles. Cette approche rationalise le processus de référencement des utilisateurs IDs et garantit que vos flux de travail d'automatisation restent robustes et pérennes.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Rôle IAM permettant à un administrateur du cloud d'exécuter le modèle AWS CloudFormation

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Architecture cible

Le schéma suivant montre comment AWS CloudFormation utilise une ressource personnalisée sauvegardée par AWS Lambda pour récupérer l'ID utilisateur IAM.

Automatisation et mise à l'échelle

Vous pouvez utiliser le CloudFormation modèle plusieurs fois pour différents Régions AWS comptes. Vous ne devez l'exécuter qu'une seule fois dans chaque région ou compte.

Outils

Services AWS

- IAM — AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources. Vous pouvez utiliser IAM pour contrôler les personnes qui s’authentifient (sont connectées) et sont autorisées (disposent d’autorisations) à utiliser des ressources.
- AWS CloudFormation— vous AWS CloudFormation aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur les applications qui s'exécutent sur AWS. Vous créez un modèle qui décrit les AWS ressources que vous souhaitez, et vous vous CloudFormation occupez de leur provisionnement et de leur configuration.
- AWS Lambda— AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est

nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.

Bonnes pratiques

Si vous partez de zéro ou si vous planifiez un nouveau déploiement, nous vous recommandons vivement de recourir à la gestion centralisée AWS IAM Identity Centerdes utilisateurs. IAM Identity Center s'intègre à vos fournisseurs d'identité existants (tels qu'Active Directory ou Okta) pour fédérer les identités des utilisateurs AWS, ce qui élimine le besoin de créer et de gérer directement des utilisateurs IAM. Cette approche garantit non seulement un contrôle d'accès cohérent, mais simplifie également la gestion du cycle de vie des utilisateurs et contribue à améliorer la sécurité et la conformité dans votre AWS environnement.

Épopées

Valider les autorisations

Tâche	Description	Compétences requises
Validez votre rôle Compte AWS et celui d'IAM.	Vérifiez que vous disposez d'un rôle IAM autorisé à déployer des CloudForm ation modèles dans votre Compte AWS. Si vous prévoyez d'utiliser la console AWS CLI au lieu de la CloudFormation console pour déployer le modèle lors de la dernière étape de cette procédure, vous devez également configurer des informations d'identification temporaires pour exécuter des AWS CLI commandes. Pour obtenir des instructions,	Architecte du cloud

Tâche	Description	Compétences requises
	consultez la documentation IAM.	

Création d'un CloudFormation modèle

Tâche	Description	Compétences requises
Créez un CloudFormation modèle.	1. Créez un CloudFormation modèle en suivant les instructions de la CloudFormation documentation. Vous pouvez utiliser le format JSON ou YAML. Ce modèle suppose que vous utilisez le format YAML. 2. Enregistrez le modèle sous son nom `get_unique_user_id.yaml` .	AWS DevOps, architecte du cloud

Ajoutez un paramètre d'entrée pour le nom d'utilisateur.	Ajoutez le code suivant à la `Parameters` section du CloudFormation modèle :
	`Parameters:`
	`  NewIamUserName:`
	`  Type: String`
	`  Description: Unique username for the new IAM user`
	Ce paramètre invite l'utilisateur à saisir son nom d'utilisateur.
		AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises

Ajoutez une ressource personnalisée pour créer un utilisateur IAM.	Ajoutez le code suivant à la `Resources` section du CloudFormation modèle :
	
	`Resources:`
	`  rNewIamUser:`
	`  Type: 'AWS::IAM ::User'`
	`  Properties:`
	`  UserName: !Ref NewIamUserName`
	
	Ce code ajoute une CloudFormation ressource qui crée un utilisateur IAM avec le nom fourni par le `NewIamUserName` paramètre.
		AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
Ajoutez un rôle d'exécution pour la fonction Lambda.	Au cours de cette étape, vous créez un rôle IAM qui accorde à une AWS Lambda fonction l'autorisation d'obtenir l'`UserId`IAM. Spécifiez les autorisations minimales requises suivantes pour que Lambda s'exécute : • `logs:CreateLogStream` • `logs:PutLogEvents` • `CreateLogGroup` • `iam:GetUser` • `AssumeRole` pour `lambda.amazonaws.com` Pour obtenir des instructions sur la création d'un rôle d'exécution, consultez la documentation Lambda. Vous ferez référence à ce rôle à l'étape suivante, lorsque vous créerez la fonction Lambda.	Administrateur AWS, architecte cloud

Tâche	Description	Compétences requises

Ajoutez une fonction Lambda pour obtenir l'IAM unique. `UserId`	Dans cette étape, vous définissez une fonction Lambda avec un environnement d'exécution Python pour obtenir l'IAM unique. `UserId` Pour ce faire, ajoutez le code suivant dans la `Resources` section du CloudFormation modèle. `<<ROLENAME>>` Remplacez-le par le nom du rôle d'exécution que vous avez créé lors de la dernière étape.
	
	`GetUserLambdaFunction:`
	`Type: 'AWS::Lambda::Function'`
	`Properties:`
	`Handler: index.handler`
	`Role: <<ROLENAME>>`
	`Timeout: 30`
	`Runtime: python3.11`
	`Code:`
	`ZipFile: |`
	`import cfnresponse, boto3`
	`def handler(event, context):`
	`try:`
	`print(event)`
	`user = boto3.client('iam').get_user(UserName=event['ResourceP`
		AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises
	roperties'][NewIa mUserName'])['User'] cfnrespon se.send(event, context, cfnrespon se.SUCCESS, {'NewIamU serId': user['Use rId'], 'NewIamUs erPath': user['Pat h'], 'NewIamUserArn': user['Arn']}) except Exception as e: cfnrespon se.send(event, context, cfnrespon se.FAILED, {'NewIamU ser': str(e)})	
Ajoutez une ressource personnalisée.	Ajoutez le code suivant à la `Resources` section du CloudFormation modèle : `rCustomGetUniqueUs erId: Type: 'Custom:: rCustomGetUniqueUs erIdWithLambda' Properties: ServiceToken: ! GetAtt GetUserLa mbdaFunction.Arn NewIamUserName: ! Ref NewIamUserName` Cette ressource personnalisée appelle la fonction Lambda pour obtenir l'IAM. `UserID`	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises

Définissez les CloudFormation sorties.	Ajoutez le code suivant à la `Outputs` section du CloudFormation modèle :
	
	`Outputs:`
	`  NewIamUserId:`
	`  Value: !GetAtt rCustomGetUniqueUserId.NewIamUserId`
	
	Cela affiche l'IAM du nouvel `UserID` utilisateur IAM.
		AWS DevOps, architecte du cloud

Enregistrez le modèle.	Enregistrez les modifications que vous avez apportées au CloudFormation modèle.	AWS DevOps, architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Pour déployer le `get_unique_user_id.yaml` modèle à l'aide de la CloudFormation console, suivez les instructions de la CloudFormation documentation. Vous pouvez également exécuter la AWS CLI commande suivante pour déployer le modèle : `aws cloudformation create-stack \`	AWS DevOps, architecte du cloud

Tâche	Description	Compétences requises

	`--stack-name DemoNewUser \`
	`--template-body file://get_unique_user_id.yaml \`
	`--parameters ParameterKey=NewIamUserName,ParameterValue=demouser \`
	`--capabilities CAPABILITY_NAMED_IAM`	

Ressources connexes

- Création d'une pile depuis la CloudFormation console (CloudFormation documentation)
- Ressources personnalisées soutenues par Lambda (documentation) CloudFormation
- Identifiants uniques (documentation IAM)
- Utiliser des informations d'identification temporaires avec AWS les ressources (documentation IAM)

Validez le code Account Factory pour Terraform (AFT) localement

Créée par Alexandru Pop (AWS) et Michal Gorniak (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle montre comment tester localement le code HashiCorp Terraform géré par AWS Control Tower Account Factory for Terraform (AFT). Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud. AFT met en place un pipeline Terraform qui vous aide à approvisionner et à personnaliser plusieurs Comptes AWS entrées. AWS Control Tower

Lors du développement du code, il peut être utile de tester votre infrastructure Terraform en tant que code (IaC) localement, en dehors du pipeline AFT. Ce modèle montre comment effectuer les opérations suivantes :

- Récupérez une copie locale du code Terraform stocké dans les AWS CodeCommit référentiels de votre compte de gestion AFT.
- Simulez le pipeline AFT localement en utilisant le code récupéré.

Cette procédure peut également être utilisée pour exécuter des commandes Terraform qui ne font pas partie du pipeline AFT normal. Par exemple, vous pouvez utiliser cette méthode pour exécuter des commandes telles que `terraform validateterraform plan`,`terraform destroy`, `etterraform import`.

Conditions préalables et limitations

Prérequis

- Un environnement AWS multi-comptes actif qui utilise AWS Control Tower
- Un environnement AFT entièrement déployé
- AWS Command Line Interface (AWS CLI), installé et configuré
- AWS CLI assistant d'identification pour AWS CodeCommit, installé et configuré
- Python 3.x

- Git, installé et configuré sur votre machine locale
- `git-remote-commit`utilitaire, installé et configuré
- Terraform, installé et configuré (la version du package Terraform local doit correspondre à la version utilisée dans le déploiement AFT)

Limites

- Ce modèle ne couvre pas les étapes de déploiement requises pour AWS Control Tower AFT ou tout autre module Terraform spécifique.
- La sortie générée localement au cours de cette procédure n'est pas enregistrée dans les journaux d'exécution du pipeline AFT.

Architecture

Pile technologique cible

- Infrastructure AFT déployée dans le cadre d'un AWS Control Tower déploiement
- Terraform
- Git
- AWS CLI version 2

Automatisation et mise à l'échelle

Ce modèle montre comment invoquer localement le code Terraform pour les personnalisations de comptes globaux AFT dans un seul compte géré par AFT. Compte AWS Une fois votre code Terraform validé, vous pouvez l'appliquer aux comptes restants de votre environnement multi-comptes. Pour plus d'informations, voir Réinvoquer les personnalisations dans la AWS Control Tower documentation.

Vous pouvez également utiliser un processus similaire pour exécuter des personnalisations de compte AFT dans un terminal local. Pour invoquer localement le code Terraform à partir des personnalisations de compte AFT, clonez le aft-account-customizationsréférentiel plutôt que le aft-global-account-customizationsréférentiel depuis votre compte de CodeCommit gestion AFT.

Outils

Services AWS

- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.

Autres services

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- Git est un système de contrôle de version distribué et open source.

Code

Voici un exemple de script bash qui peut être utilisé pour exécuter localement du code Terraform géré par AFT. Pour utiliser le script, suivez les instructions de la section Epics de ce modèle.

```
#! /bin/bash
# Version: 1.1 2022-06-24 Unsetting AWS_PROFILE since, when set, it interferes with
 script operation
#          1.0 2022-02-02 Initial Version
#
# Purpose: For use with AFT: This script runs the local copy of TF code as if it were
 running within AFT pipeline.
#        * Facilitates testing of what the AFT pipline will do
#           * Provides the ability to run terraform with custom arguments (like 'plan'
 or 'move') which are currently not supported within the pipeline.
#
# © 2021 Amazon Web Services, Inc. or its affiliates. All Rights Reserved.
# This AWS Content is provided subject to the terms of the AWS Customer Agreement
# available at http://aws.amazon.com/agreement or other written agreement between
# Customer and either Amazon Web Services, Inc. or Amazon Web Services EMEA SARL or
 both.
#
# Note: Arguments to this script are passed directly to 'terraform' without parsing nor
 validation by this script.
#
# Prerequisites:
#    1. local copy of ct GIT repositories
#    2. local backend.tf and aft-providers.tf filled with data for the target account
 on which terraform is to be run
```

```
#       Hint: The contents of above files can be obtain from the logs of a previous
 execution of the AFT pipeline for the target account.
#    3. 'terraform' binary is available in local PATH
#    4. Recommended: .gitignore file containing 'backend.tf', 'aft_providers.tf' so the
 local copy of these files are not pushed back to git

readonly credentials=$(aws sts assume-role \
    --role-arn arn:aws:iam::$(aws sts get-caller-identity --query "Account" --output
 text ):role/AWSAFTAdmin \
    --role-session-name AWSAFT-Session \
    --query Credentials )

unset AWS_PROFILE
export AWS_ACCESS_KEY_ID=$(echo $credentials | jq -r '.AccessKeyId')
export AWS_SECRET_ACCESS_KEY=$(echo $credentials | jq -r '.SecretAccessKey')
export AWS_SESSION_TOKEN=$(echo $credentials | jq -r '.SessionToken')
terraform "$@"
```

Épopées

Enregistrez l'exemple de code dans un fichier local

Tâche	Description	Compétences requises
Enregistrez l'exemple de code dans un fichier local.	1. Copiez l'exemple de script bash qui se trouve dans la section Code de ce modèle et collez-le dans un éditeur de code. 2. Nommez le fichier`ct_terraform.sh` , puis enregistrez-le localement dans un dossier dédié, tel que `~/scripts` ou`~/bin`.	Administrateur AWS
Rendez l'exemple de code exécutable.	Ouvrez une fenêtre de terminal et authentifiez-vous dans votre compte de gestion	Administrateur AWS

Tâche	Description	Compétences requises
	AWS AFT en effectuant l'une des opérations suivantes : • Utilisez un AWS CLI profil existant configuré avec les autorisations requises pour accéder au compte de gestion AFT. Pour utiliser le profil, vous pouvez exécuter la commande suivante : `export AWS_PROFILE=<aft account profile name>` • Si votre organisation utilise l'authentification unique pour accéder AWS, entrez les informations d'identification de votre compte de gestion AFT sur la page SSO de votre organisation. **Note** Votre organisation peut également disposer d'un outil personnalisé pour fournir des informations d'authentification à votre AWS environnement.	

Tâche	Description	Compétences requises

Vérifiez correctement l'accès au compte de gestion AFT Région AWS.	**⚠ Important**
	Assurez-vous d'utiliser la même session de terminal que celle avec laquelle vous vous êtes authentifié sur votre compte de gestion AFT.
	
	1. Accédez à votre déploiement AFT Région AWS en exécutant la commande suivante :
	`export AWS_REGION=<aft_region>`
	2. Vérifiez que vous êtes sur le bon compte.
	a. Exécutez la commande suivante :
	`aws code-commit list-repositories`
	b. Vérifiez que les référentiels répertoriés dans la sortie correspondent aux noms des référentiels présents dans votre compte de gestion AFT.
		Administrateur AWS

Tâche	Description	Compétences requises

Créez un nouveau répertoire local pour stocker le code du référentiel AFT.	Au cours de la même session de terminal, exécutez les commandes suivantes :
	`mkdir my_aft`
	`cd my_aft`
		Administrateur AWS

Tâche	Description	Compétences requises
Clonez le code du référentiel AFT distant.	1. Dans votre terminal local, exécutez la commande suivante : `git clone codecommit::$AWS_REGION://aft-global-customizations` **Note** Pour des raisons de simplicité, cette procédure et AFT utilisent uniquement une branche de code principale. Pour utiliser le branchement de code, vous pouvez également saisir des commandes de branchement de code ici. Cependant, toute modification appliquée depuis la branche non principale sera annulée lorsque l'automatisation AFT appliquera le code de la branche principale.	Administrateur AWS

Tâche	Description	Compétences requises
	2. Accédez au répertoire cloné : `cd aft-global-customizations/terraform`	

Créez les fichiers de configuration Terraform requis pour que le pipeline AFT s'exécute localement

Tâche	Description	Compétences requises
Ouvrez un pipeline AFT déjà exécuté et copiez les fichiers de configuration Terraform dans un dossier local.	**Note** Les fichiers `aft-providers.tf` de configuration `backend.tf` et créés dans cette épopée sont nécessaires au fonctionnement local du pipeline AFT. Ces fichiers sont créés automatiquement dans le pipeline AFT basé sur le cloud, mais doivent être créés manuellement pour que le pipeline s'exécute localement. L'exécution locale du pipeline AFT nécessite un ensemble de fichiers représentant l'exécution du pipeline	Administrateur AWS

Tâche	Description	Compétences requises
	au sein d'un seul Compte AWS. 1. À l'aide des informations d'identification de votre compte de AWS Control Tower gestion AWS Management Console, connectez-vous à la AWS CodePipeline console et ouvrez-la. Assurez-vous que vous êtes dans le même Région AWS endroit que celui où vous avez déployé l'AFT. 2. Dans le volet de navigation de gauche, choisissez Pipelines. 3. Choisissez ##########-customizations-pipeline. (Le ########## est l'Compte AWS ID que vous utilisez pour exécuter le code Terraform localement.) 4. Assurez-vous que l'exécution la plus récente marquée indique une valeur réussie. Si la valeur est différente, vous devez réinvoquer vos personnalisations dans le pipeline AFT. Pour plus d'informations, voir	

Tâche	Description	Compétences requises
	Réinvoquer les personnalisations dans la AWS Control Tower documentation. 5. Choisissez le moteur d'exécution le plus récent pour en afficher les détails. 6. Dans la section Apply-AFT-Global-Customizations, recherchez le stage Apply-Terraform. 7. Sélectionnez la section Détails du stage Apply-Terraform. 8. Trouvez le journal d'exécution du stage Apply-Terraform. 9. Dans le journal d'exécution, recherchez la section qui commence et se termine par les lignes suivantes : `"\n\n aft-providers.tf ... "\n \n backend.tf"` 10. Copiez la sortie entre ces deux étiquettes et enregistrez-la sous forme de fichier local nommé `aft-providers.tf` dans le dossier Terraform local (le répertoire de travail actuel de votre session de terminal).	

Tâche	Description	Compétences requises

	Exemple de déclaration providers.tf générée automatiquement
	
	`## Autogenerated providers.tf ## ## Updated on: 2022-05-31 16:27:45 ## provider "aws" { region = "us-east-2" assume_role { role_arn = "arn:aws:iam::########:role/AWSAFTExecution" } default_tags { tags = { managed_by = "AFT" } } }`
	
	11. Dans le journal d'exécution, recherchez la section qui commence et se termine par les lignes suivantes :
	
	`"\n\n tf ... "\n \n backend.tf"`
	
	12. Copiez la sortie entre ces deux étiquettes et enregistrez-la sous forme de fichier local nommé `tf` dans le	

Tâche	Description	Compétences requises
	dossier Terraform local (le répertoire de travail actuel de votre session de terminal). Exemple d'instruction backend.tf générée automatiquement ```## Autogenerated backend.tf ## ## Updated on: 2022-05-31 16:27:45 ## terraform { required_version = ">= 0.15.0" backend "s3" { region = "us-east-2" bucket = "aft-backend-#####-primary-region" key = "##########-aft-global-customizations/terraform.tfstate" dynamodb_table = "aft-backend-#####" encrypt = "true" kms_key_id = "########-####-####-####-############" role_arn = "arn:aws:iam::#########:role/AWSAFTExecution"```	

Tâche	Description	Compétences requises
	} }	

> **Note**
>
> Les `aft-providers.tf` fichiers `backend.tf` et sont liés à un déploiement et à un dossier AFT spécifiques Compte AWS. Ces fichiers sont également différents selon qu'ils se trouvent ou non dans le aft-account-customizationsréférentiel aft-global-customizationsand au sein du même déploiement AFT. Assurez-vous de générer les deux fichiers à partir de la même liste d'environnements d'exécution.

Exécutez le pipeline AFT localement en utilisant l'exemple de script bash

Tâche	Description	Compétences requises
Implémentez les modifications de configuration Terraform que vous souhaitez valider.	1. Accédez au aft-global-customizationsréférenti	Administrateur AWS

Tâche	Description	Compétences requises
	el cloné en exécutant la commande suivante : `cd aft-global-customizations/terraform` **Note** Les fichiers `backend.tf` et les fichiers `aft-providers.tf` se trouvent dans ce répertoire. Le répertoire contient également les fichiers Terraform du aft-global-customizations référentiel. 2. Incorporez les modifications de code Terraform que vous souhaitez tester localement dans les fichiers de configuration.	

Tâche	Description	Compétences requises

Exécutez le `ct_terraform.sh` script et examinez le résultat.	1. Accédez au dossier local qui contient le script sh.
	2. Pour valider votre code Terraform modifié, exécutez le `ct_terraform.sh` script en exécutant la commande suivante :
	`~/scripts/ct_terraform.sh apply`
	`terraform --help`
	Note
	Vous pouvez exécuter n'importe quelle commande Terraform au cours de cette étape. Pour voir la liste complète des commandes Terraform, exécutez la commande suivante :
	3. Passez en revue le résultat de la commande, puis déboguez les modifications de code localement avant de les valider et de les renvoyer dans le référentiel AFT.
		Administrateur AWS

Tâche	Description	Compétences requises
	⚠ Important • Toutes les modifications apportées localement et non renvoyées au référentiel distant sont temporaires et peuvent être annulées à tout moment par une automatisation du pipeline AFT en cours d'exécution. • L'automatisation AFT peut être exécutée à tout moment, car elle peut être invoquée par d'autres utilisateurs et par des déclencheurs d'automatisation AFT. • AFT appliquera toujours le code de la branche principale du référentiel, annulant ainsi toute modification non validée.	

Transférez vos modifications de code local vers le référentiel AFT

Tâche	Description	Compétences requises
Ajoutez des références aux `aft-providers.tf` fichiers `backend.tf` et à un `.gitignore` fichier.	Ajoutez les `aft-providers.tf` fichiers `backend.tf` et que vous avez créés à un `.gitignor`	Administrateur AWS

Tâche	Description	Compétences requises

	e fichier en exécutant les commandes suivantes :
	`echo backend.tf >> .gitignore`
	`echo aft-providers.tf >>.gitignore`
	Note
	Le déplacement des fichiers vers le `.gitignore` fichier garantit qu'ils ne sont pas validés et renvoyés vers le référentiel AFT distant.	

Tâche	Description	Compétences requises

Validez et transférez vos modifications de code dans le référentiel AFT distant.	1. Pour ajouter de nouveaux fichiers de configuration Terraform au référentiel, exécutez la commande suivante :
	`git add <filename>`
	2. Pour valider vos modifications et les transférer vers le référentiel AFT distant CodeCommitt, exécutez les commandes suivantes :
	`git commit -a`
	`git push`
	Important
	Les modifications de code que vous introduisez en suivant cette procédure jusqu'à présent ne sont appliquées qu'à une Compte AWS seule.
		Administrateur AWS

Déployez les modifications sur plusieurs comptes

Tâche	Description	Compétences requises
Appliquez les modifications à tous vos comptes gérés par AFT.	Pour appliquer les modifications à plusieurs Comptes AWS options gérées par AFT, suivez les instructions de la section Réinvoquer les personnalisations dans la AWS Control Tower documentation.	Administrateur AWS

Plus de modèles

- Ajoutez HA à Oracle PeopleSoft sur Amazon RDS Custom à l'aide d'une réplique en lecture
- Auditez automatiquement les groupes de AWS sécurité qui autorisent l'accès depuis des adresses IP publiques
- Automatisez la création de comptes à l'aide de l'accélérateur Landing Zone sur AWS
- Automatisez l'ajout ou la mise à jour d'entrées de registre Windows à l'aide d'AWS Systems Manager
- Automatisez l'évaluation des ressources AWS
- Automatisez le déploiement du portefeuille et des produits AWS Service Catalog à l'aide d'AWS CDK
- Automatisez le basculement et le retour en arrière entre régions à l'aide de DR Orchestrator Framework
- Automatisez la suppression des AWS CloudFormation piles et des ressources associées
- Automatisez l'ingestion et la visualisation des métriques personnalisées Amazon MWAA sur Amazon Managed Grafana à l'aide de Terraform
- Automatisez la configuration de RabbitMQ dans Amazon MQ
- Automatisez la réplication des instances Amazon RDS sur Comptes AWS
- Associez automatiquement une politique gérée par AWS pour Systems Manager aux profils d' EC2 instance à l'aide de Cloud Custodian et d'AWS CDK
- Créez automatiquement des pipelines CI/CD et des clusters Amazon ECS pour les microservices à l'aide d'AWS CDK
- Détectez automatiquement les modifications et lancez différents CodePipeline pipelines pour un monorepo dans CodeCommit
- Réactivez automatiquement AWS à l'aide CloudTrail d'une règle de correction personnalisée dans AWS Config
- Créez un pipeline de données pour ingérer, transformer et analyser les données Google Analytics à l'aide du kit de AWS DataOps développement
- Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager
- Créez et envoyez des images Docker vers Amazon ECR à l'aide d' GitHub Actions et de Terraform
- Centralisez la gestion des clés d'accès IAM dans AWS Organizations à l'aide de Terraform
- Centralisez la distribution des packages logiciels dans AWS Organizations à l'aide de Terraform

- Enchaînez les services AWS en utilisant une approche sans serveur
- Configuration d'une extension de centre de données vers le VMware cloud sur AWS à l'aide du mode Hybrid Linked
- Configurez la journalisation des appels de modèles dans Amazon Bedrock en utilisant AWS CloudFormation
- Configurer le routage en lecture seule dans un groupe de disponibilité Always On dans SQL Server sur AWS
- Configurer VMware vRealize Automation pour le provisionner VMs sur le VMware cloud sur AWS
- Créez un portail pour les micro-frontends en utilisant AWS Amplify Angular et Module Federation
- Création d'une EventBridge connexion Amazon entre comptes dans une organisation
- Créez automatiquement des pipelines CI dynamiques pour les projets Java et Python
- Déployez une API Amazon API Gateway sur un site Web interne à l'aide de points de terminaison privés et d'un Application Load Balancer
- Déploiement et débogage de clusters Amazon EKS
- Déployez et gérez AWS Control Tower les contrôles en utilisant AWS CDK et CloudFormation
- Déployez et gérez les AWS Control Tower contrôles à l'aide de Terraform
- Déployez des CloudWatch canaris Synthetics à l'aide de Terraform
- Déployez un système de fichiers Lustre pour un traitement des données performant à l'aide de Terraform et DRA
- Déployez un cas d'utilisation de RAG AWS en utilisant Terraform et Amazon Bedrock
- Déployez des ressources dans une AWS Wavelength zone à l'aide de Terraform
- Déployez des instances de cluster de basculement SQL Server sur Amazon EC2 et Amazon à l'aide FSx de Terraform
- Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform
- Détectez les instances de base de données Amazon RDS et Aurora dont les certificats CA expirent
- Documentez la conception de votre zone de landing zone AWS
- Assurez-vous qu'un profil IAM est associé à une instance EC2
- Exportez les rapports AWS Backup de l'ensemble d'une organisation dans AWS Organizations sous forme de fichier CSV
- Générez des recommandations personnalisées et reclassées à l'aide d'Amazon Personalize
- Identifiez et alertez lorsque les ressources Amazon Data Firehose ne sont pas chiffrées à l'aide d'une clé AWS KMS

- Implémentez Account Factory for Terraform (AFT) en utilisant un pipeline bootstrap
- Implémentez la gestion des versions d'API basée sur les chemins en utilisant des domaines personnalisés dans Amazon API Gateway
- Installation de l'agent SSM sur les nœuds de travail Amazon EKS à l'aide de Kubernetes DaemonSet
- Installez l'agent SSM et l' CloudWatch agent sur les nœuds de travail Amazon EKS à l'aide de preBootstrapCommands
- Intégrer VMware vRealize Network Insight au VMware cloud sur AWS
- Gérez les ensembles AWS IAM Identity Center d'autorisations sous forme de code en utilisant AWS CodePipeline
- Gérez les produits AWS Service Catalog dans plusieurs comptes AWS et régions AWS
- Gérez les applications de conteneur sur site en configurant Amazon ECS Anywhere avec le kit AWS CDK
- Gérez AWS Organizations les politiques sous forme de code en utilisant AWS CodePipeline Amazon Bedrock
- Migrer des enregistrements DNS en masse vers une zone hébergée privée Amazon Route 53
- Migrer Oracle E-Business Suite vers Amazon RDS Custom
- Migrer Oracle PeopleSoft vers Amazon RDS Custom
- Migrez les systèmes RHEL BYOL vers des instances incluses dans une licence AWS à l'aide d'AWS MGN
- Migrer VMware le SDDC vers le VMware cloud sur AWS à l'aide de HCX VMware
- Configurez un espace de données minimum viable pour partager les données entre les organisations
- Surveillez les ElastiCache clusters Amazon pour le chiffrement au repos
- Surveillez l'activité des applications à l'aide de CloudWatch Logs Insights
- Surveiller les ElastiCache clusters pour les groupes de sécurité
- Surveillez les clusters SAP RHEL Pacemaker à l'aide des services AWS
- Optimisez les déploiements multicomptes sans serveur en utilisant les flux de travail et AWS CDK Actions GitHub
- Accédez en privé à un point de terminaison de service AWS central à partir de plusieurs VPCs
- Provisionner AWS Service Catalog des produits basés sur AWS CloudFormation des modèles à l'aide d' GitHub actions

- Fournissez des rôles IAM avec le moindre privilège en déployant une solution de distribution automatique de rôles
- Supprimez EC2 les entrées Amazon Comptes AWSAWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Supprimez EC2 les entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Rotation des informations d'identification de base de données sans redémarrer les conteneurs
- Envoyer une notification lorsqu'un utilisateur IAM est créé
- Envoyez des logs depuis le VMware Cloud AWS vers Splunk en utilisant VMware Aria Operations for Logs
- Configuration d'un routeur cellulaire sans serveur pour une architecture basée sur les cellules
- Configurez un pipeline CI/CD pour les charges de travail hybrides sur Amazon ECS Anywhere à l'aide d'AWS CDK et GitLab
- Configurez une infrastructure de bureau virtuel à scalabilité automatique à l'aide de NICE EnginFrame et de NICE DCV Session Manager
- Configuration d'une architecture HA/DR pour Oracle E-Business Suite sur Amazon RDS Custom avec une base de données de secours active
- Configuration de la résolution DNS pour les réseaux hybrides dans un environnement multi-comptes AWS
- Configurez une infrastructure multi-AZ pour un SQL Server Always On FCI à l'aide d'Amazon FSx
- Configuration de la fonctionnalité Oracle UTL_FILE sur Aurora compatible avec PostgreSQL
- Simplifiez l'authentification des applications avec le protocole TLS mutuel dans Amazon ECS en utilisant Application Load Balancer
- Simplifiez la gestion des certificats privés en utilisant AWS Private CA et AWS RAM
- Rationalisez les flux de travail d'apprentissage automatique, du développement local aux expériences évolutives en utilisant l' SageMaker IA et Hydra
- Marquez automatiquement les pièces jointes à Transit Gateway à l'aide d'AWS Organizations
- Rôles de transition pour une PeopleSoft application Oracle sur Amazon RDS Custom for Oracle
- Utilisez Amazon Q Developer comme assistant de codage pour augmenter votre productivité

Applications Web et mobiles

Rubriques

- Authentifiez les utilisateurs existants de l'application React à l'aide d'Amazon Cognito et de l'interface utilisateur AWS Amplify
- Déployez en continu une application Web AWS Amplify moderne à partir d'un référentiel AWS CodeCommit
- Créez une application React à l'aide d'AWS Amplify et ajoutez l'authentification avec Amazon Cognito
- Créez un portail pour les micro-frontends en utilisant AWS Amplify Angular et Module Federation
- Déployez une application monopage basée sur React sur Amazon S3 et CloudFront
- Déployez une API Amazon API Gateway sur un site Web interne à l'aide de points de terminaison privés et d'un Application Load Balancer
- Intégrer un tableau de QuickSight bord Amazon dans une application Angular locale
- Découvrez le développement complet d'applications Web natives pour le cloud avec Green Boost
- Exécutez des tests unitaires pour une application Node.js à GitHub l'aide d'AWS CodeBuild
- Structurer un projet Python dans une architecture hexagonale à l'aide d'AWS Lambda
- Plus de modèles

Authentifiez les utilisateurs existants de l'application React à l'aide d'Amazon Cognito et de l'interface utilisateur AWS Amplify

Créée par Daniel Kozhemyako (AWS)

Récapitulatif

Ce modèle montre comment ajouter des fonctionnalités d'authentification à une application React frontale existante à l'aide d'une bibliothèque d' AWS Amplify interface utilisateur et d'un groupe d'utilisateurs Amazon Cognito.

Le modèle utilise Amazon Cognito pour fournir l'authentification, l'autorisation et la gestion des utilisateurs pour l'application. Il utilise également un composant d'Amplify UI, une bibliothèque open source qui étend les fonctionnalités de développement AWS Amplify d'interfaces utilisateur (UI). Le composant Authenticator UI gère les sessions de connexion et exécute le flux de travail connecté au cloud qui authentifie les utilisateurs via Amazon Cognito.

Après avoir implémenté ce modèle, les utilisateurs peuvent se connecter à l'aide de l'une des informations d'identification suivantes :

- Nom d'utilisateur et mot de passe
- Fournisseurs d'identité sociale, tels qu'Apple, Facebook, Google et Amazon
- Fournisseurs d'identité d'entreprise compatibles avec SAML 2.0 ou OpenID Connect (OIDC)

> **Note**
>
> Pour créer un composant d'interface utilisateur d'authentification personnalisé, vous pouvez exécuter le composant d'interface utilisateur d'authentification en mode headless.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une application Web React 18.2.0 ou version ultérieure
- Node.js et npm 6.14.4 ou version ultérieure, installés

Limites

- Ce modèle s'applique uniquement aux applications Web React.
- Ce modèle utilise un composant Amplify UI prédéfini. La solution ne couvre pas les étapes requises pour implémenter un composant d'interface utilisateur personnalisé.

Versions du produit

- Amplify UI 6.1.3 ou version ultérieure (Gen 1)
- Amplify 6.0.16 ou version ultérieure (Gen 1)

Architecture

Architecture cible

Le schéma suivant montre une architecture qui utilise Amazon Cognito pour authentifier les utilisateurs d'une application Web React.

Outils

Services AWS

- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour les applications Web et mobiles.

Autres outils

- Amplify UI est une bibliothèque d'interface utilisateur open source qui fournit des composants personnalisables que vous pouvez connecter au cloud.
- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.
- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.

Bonnes pratiques

Si vous créez une nouvelle application, nous vous recommandons d'utiliser Amplify Gen 2.

Épopées

Création d'un groupe d'utilisateurs Amazon Cognito

Tâche	Description	Compétences requises
Créez un groupe d'utilisateurs.	Créez un groupe d'utilisateurs Amazon Cognito. Configurez les options de connexion et les exigences de sécurité du groupe d'utilisateurs en fonction de votre cas d'utilisation.	Développeur d’applications
Ajoutez un client d'application.	Configurez un client d'application pour un groupe d'utilisateurs. Ce client est nécessaire pour que votre application puisse interagir avec le groupe d'utilisateurs Amazon Cognito.	Développeur d’applications

Intégrez votre groupe d'utilisateurs Amazon Cognito au composant de l'interface utilisateur Authenticator

Tâche	Description	Compétences requises
Installez les dépendances.	Pour installer les `@aws-amplify/ui-react` packages `aws-amplify` et, exécutez la commande suivante depuis le répertoire racine de votre application : `npm i @aws-amplify/ui-react aws-amplify`	Développeur d’applications

Tâche	Description	Compétences requises

Configurez le groupe d'utilisateurs.	Sur la base de l'exemple suivant, créez un `aws-exports.js` fichier et enregistrez-le dans le `src` dossier. Le fichier doit inclure les informations suivantes :
	• Région AWS dans lequel se trouve votre groupe d'utilisateurs Amazon Cognito
	• ID du groupe d'utilisateurs Amazon Cognito
	• ID du client de l'application
	
	`// replace the user pool region, id, and app client id details`
	`const awsmobile = {`
	`"aws_project_region": "put_your_region_here",`
	`"aws_cognito_region": "put_your_region_here",`
	`"aws_user_pools_id": "put_your_user_pool_id_here",`
	`"aws_user_pools_web_client_id": "put_your_user_pool_app_id_here"`
	`}`
	
	`export default awsmobile;`
		Développeur d’applications

Tâche	Description	Compétences requises

Importez et configurez le service Amplify.	1. Dans le fichier du point d'entrée de l'application (par exemple,`App.js`), importez et chargez le `aws-exports.js` fichier en saisissant les lignes de code suivantes :
	`import { Amplify } from 'aws-amplify'; import awsExports from './aws-exports';`
	2. Sur la base de l'exemple suivant, configurez le client Amplify à l'aide du `aws-exports.js` fichier :
	`// Configure Amplify in index file or root file Amplify.configure({ ...awsExports });`
	Pour plus d'informations, voir Configurer les catégories Amplify dans la documentation Amplify.
		Développeur d’applications

Tâche	Description	Compétences requises

Ajoutez le composant d'interface utilisateur Authenticator.	Pour afficher le composant d'`Authenticator` interface utilisateur, ajoutez les lignes de code suivantes au fichier de point d'entrée de l'application (`App.js`) :
	`import { Authenticator } from '@aws-amplify/ui-react';`
	`import '@aws-amplify/ui-react/styles.css';`
	Note
	L'extrait de code d'exemple importe le composant d'`Authenticator` interface utilisateur et le fichier Amplify UI styles.css, qui est requis lors de l'utilisation des thèmes prédéfinis du composant.
	Le composant d'`Authenticator` interface utilisateur fournit deux valeurs de retour :
	• Informations sur l'utilisateur
		Développeur d’applications

Tâche	Description	Compétences requises
	• Une fonction qui peut être invoquée pour déconnecter l'utilisateur Consultez l'exemple de composant suivant : `function App() { return ( <Authenticator> {({ signOut, user }) => ( <div> <p>Welcome {user.username}</p> <button onClick={signOut}>Sign out</button> </div> )} </Authenticator> ); }` **Note** Pour un exemple de `App.js` fichier, consultez la section Informations supplémentaires de ce modèle.	

Tâche	Description	Compétences requises
(Facultatif) Récupérez les informations de session.	Une fois qu'un utilisateur est authentifié, vous pouvez récupérer les données du client Amplify concernant sa session. Par exemple, vous pouvez récupérer le jeton Web JSON (JWT) à partir de la session d'un utilisateur afin d'authentifier les demandes de sa session auprès d'une API principale. Consultez l'exemple suivant d'en-tête de demande qui inclut un JWT : `import { fetchAuth Session } from 'aws-amplify/auth'; (await fetchAuth Session()).tokens? .idToken?.toString();`	Développeur d’applications

Résolution des problèmes

Problème	Solution
Les nouveaux utilisateurs ne peuvent pas s'inscrire à l'application.	Comme suit, assurez-vous que votre groupe d'utilisateurs Amazon Cognito est configuré pour permettre aux utilisateurs de s'inscrire pour faire partie du groupe d'utilisateurs : • Connectez-vous à la console Amazon Cognito AWS Management Console, puis ouvrez-la.

Problème	Solution
	• Dans le volet de navigation de gauche, sélectionnez Groupes d'utilisateurs. • Choisissez votre groupe d'utilisateurs dans la liste. • Sous Paramètres généraux, sélectionnez Politiques. • Choisissez Autoriser les utilisateurs à s'inscrire eux-mêmes.
Le composant d'authentification a cessé de fonctionner après la mise à niveau de la version 5 vers la version 6.	La `Auth` catégorie est passée à une approche fonctionnelle et a nommé les paramètres dans Amplify v6. Vous devez maintenant importer la fonctionnalité APIs directement depuis le `aws-amplify/auth` chemin. Pour plus d'informations, voir Migrer de la version 5 à la version 6 dans la documentation Amplify.

Ressources connexes

- Commencer à utiliser Amazon Cognito (site Web)AWS
- Création d'une nouvelle application React (documentation React)
- Qu'est-ce qu'Amazon Cognito ? (documentation Amazon Cognito)
- Bibliothèque d'interface utilisateur Amplify (documentation Amplify)

Informations supplémentaires

Le `App.js` fichier doit contenir le code suivant :

```
import './App.css';
import { Amplify } from 'aws-amplify';
import awsExports from './aws-exports';
import { fetchAuthSession } from 'aws-amplify/auth';
import { Authenticator } from '@aws-amplify/ui-react';
import '@aws-amplify/ui-react/styles.css';
Amplify.configure({ ...awsExports });
```

```
let token = (await fetchAuthSession()).tokens?.idToken?.toString();
function App() {
  return (
      <Authenticator>
        {({ signOut, user }) => (
            <div>
              <p>Welcome {user.username}</p>
                <p>Your token is: {token}</p>
              <button onClick={signOut}>Sign out</button>
            </div>
        )}
      </Authenticator>
  );
}

export default App;
```

Déployez en continu une application Web AWS Amplify moderne à partir d'un référentiel AWS CodeCommit

Créée par Deekshitulu Pentakota (AWS) et Sai Katakam (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus.

Les applications Web modernes sont conçues comme des applications d'une seule page (SPAs) qui regroupent tous les composants de l'application dans des fichiers statiques. En utilisant AWS Amplify Hosting, vous pouvez créer un pipeline d'intégration et de déploiement continus (CI/CD) qui crée, déploie et héberge une application Web moderne gérée dans un référentiel Git. Lorsque vous connectez Amplify Hosting au référentiel de code, chaque validation lance un flux de travail unique pour déployer le frontend et le backend de l'application. L'avantage de cette approche est que l'application Web n'est mise à jour qu'une fois le déploiement terminé avec succès, ce qui permet d'éviter les incohérences entre le frontend et le backend.

Dans ce modèle, vous utilisez un CodeCommit référentiel AWS pour gérer votre application Web moderne. L'exemple d'application Web présenté dans ces instructions utilise le framework React SPA. Cependant, Amplify Hosting prend en charge de nombreux autres frameworks SPA, tels que Angular, Vue, Next.js, et prend également en charge les générateurs à site unique, tels que Gatsby, Hugo et Jekyll.

Ce modèle est destiné aux créateurs d'AWS qui ont de l'expérience avec les services et concepts suivants :

- AWS CodeCommit
- Hébergement AWS Amplify
- React
- JavaScript
- Node.js
- npm
- Git

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Autorisations pour créer des ressources dans Amplify et. CodeCommit Pour plus d'informations, consultez Identity and Access Management pour Amplify et Identity and Access Management pour AWS. CodeCommit
- Interface de ligne de commande AWS (AWS CLI), installée et configurée.
- Un éditeur de texte ou un éditeur de code.
- CodeCommit, configuré pour les utilisateurs HTTPS à l'aide des informations d'identification Git.
- Un rôle de service IAM pour Amplify.
- npm et Node.js, installés (documentation npm).

Limites

- Ce modèle ne traite pas du développement et de l'intégration d'un backend pour l'application Amplify, tel qu'une API, une authentification ou une base de données. Pour plus d'informations sur les backends, voir Créer un backend dans la documentation Amplify.

Versions du produit

- Version 2.0 de l'interface de ligne de commande AWS
- Node.js version 16.x ou ultérieure

Architecture

Pile technologique cible

- CodeCommitRéférentiel AWS contenant un spa React
- Flux de travail d'hébergement AWS Amplify

Architecture cible

Outils

Services AWS

- AWS Amplify Hosting fournit un flux de travail basé sur Git pour héberger des applications Web sans serveur complètes avec un déploiement continu.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

Autres outils

- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.
- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.

Épopées

Création d'un CodeCommit référentiel

Tâche	Description	Compétences requises
Créer un référentiel .	Pour obtenir des instructions, consultez la section Création d'un CodeCommit référentiel AWS dans la CodeCommit documentation.	AWS DevOps
Pour cloner le référentiel.	Pour obtenir des instructions, consultez la section Se connecter au CodeCommit référentiel en clonant le référentiel dans la CodeCommit documentation. Si vous y êtes invité, fournisse	Développeur d’applications

Tâche	Description	Compétences requises
	z les informations d'identif ication Git.	

Création d'une application React

Tâche	Description	Compétences requises

Créez une nouvelle application React.	1. Entrez la commande suivante pour accéder au dépôt cloné. Remplacez `<repo name>` par le nom de votre CodeCommit dépôt.
	`$ cd <repo name>`
	2. Entrez la commande suivante pour créer une nouvelle application React dans le référentiel cloné.
	`$ npx create-react-app .`
	3. Codez l'application, puis entrez la commande suivante pour la démarrer.
	`$ npm start`
	Pour plus d'informations sur la création d'une applicati on React personnalisée, consultez les instructions de création d'une application
		Développeur d’applications

Tâche	Description	Compétences requises
	React dans la documentation de création d'une application React. Vous pouvez également déployer un exemple d'application React sur votre compte Amplify en suivant les instructions de la section Déployer un frontend dans la documentation Amplify.	

Créez une branche et insérez le code.	1. Entrez la commande suivante pour créer une nouvelle branche localement, où <branch> est le nom que vous souhaitez attribuer à la nouvelle branche.
	`$ git checkout -b <branch>`
	2. Entrez la commande suivante pour transférer la branche vers le CodeCommit référentiel, où se <branch> trouve le nom que vous avez attribué à l'étape précédente. Pour plus d'informations, consultez la section Utilisation des validations.
	`$ git push --set-upstream origin <branch>`
		Développeur d’applications

Déployez l'application dans AWS Amplify Hosting

Tâche	Description	Compétences requises
Connect Amplify au référentiel.	Pour obtenir des instructions, voir Connecter un dépôt dans la documentation d'Amplify Hosting. Sélectionnez AWS CodeCommit , le référentiel et la branche que vous avez créés précédemment.	Développeur d’applications

Définissez les paramètres de construction du frontend.	Pour obtenir des instructions, voir Confirmer les paramètres de construction du frontend dans la documentation d'Amplify Hosting. Acceptez les valeurs par défaut ou entrez ce qui suit.
	`Build settings:`
	`version: 0.1`
	`frontend:`
	`  phases:`
	`  preBuild:`
	`  commands:`
	`  - npm ci`
	`  build:`
	`  commands:`
	`  - npm run build`
	`  artifacts:`
	`  baseDirectory:`
	`  build`
	`  files:`
	`  - '**/*'`
	`  cache:`
	`  paths:`
	`  - node_modules/**/*`
		Développeur d’applications

Tâche	Description	Compétences requises
Vérifiez et déployez.	Pour obtenir des instructi ons, consultez la section Enregistrer et déployer dans la documentation d'Amplify Hosting. Attendez que le processus de déploiement soit terminé.	Développeur d’applications

Valider le déploiement continu

Tâche	Description	Compétences requises
Vérifiez le déploiement initial.	Lorsque le processus de déploiement est terminé, sous Domaine, cliquez sur le lien. Vérifiez que l'application fonctionne comme prévu.	Développeur d’applications
Appliquez une modification au référentiel de code.	Modifiez le code sur votre poste de travail local et transférez les modifications vers le CodeCommit référenti el. Amplify Hosting détecte le changement dans le référenti el et lance automatiquement le processus de création et de déploiement. Vérifiez que les mises à jour de l'application sont visibles sur le domaine.	Développeur d’applications

Ressources connexes

CodeCommit Documentation AWS

- Configuration pour AWS CodeCommit
  - Configuration pour les utilisateurs HTTPS à l'aide des informations d'identification Git
  - Étapes de configuration des connexions HTTPS aux CodeCommit référentiels AWS sous Linux, macOS ou Unix à l'aide de l'assistant d'identification de la CLI AWS
- Commencer à utiliser AWS CodeCommit

Documentation d'hébergement AWS Amplify

- Commencer avec le code existant
- Configuration de domaines personnalisés

Ressources React

- Créer le site Web de l'application React
- Création de la documentation de l'application React
- Créer un référentiel d'applications React (GitHub)

Créez une application React à l'aide d'AWS Amplify et ajoutez l'authentification avec Amazon Cognito

Créée par Rishi Singla (AWS)

Récapitulatif

Ce modèle montre comment utiliser AWS Amplify pour créer une application basée sur React et comment ajouter une authentification au frontend à l'aide d'Amazon Cognito. AWS Amplify comprend un ensemble d'outils (framework open source, environnement de développement visuel, console) et de services (hébergement d'applications Web et de sites Web statiques) destinés à accélérer le développement d'applications mobiles et Web sur AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Node.js et npm installés sur votre machine

Versions du produit

- Node.js version 10.x ou ultérieure (pour vérifier votre version, exécutez-le `node -v` dans une fenêtre de terminal)
- npm version 6.x ou version ultérieure (pour vérifier votre version, exécutez-le `npm -v` dans une fenêtre de terminal)

Architecture

Pile technologique cible

- AWS Amplify
- Amazon Cognito

Outils

- Amplify Command Line Interface (CLI)

- Amplify Libraries (bibliothèques clientes open source)
- Amplify Studio (interface visuelle)

Épopées

Installation de l'interface de ligne de commande AWS Amplify

Tâche	Description	Compétences requises

Installez la CLI Amplify.	L'Amplify CLI est une chaîne d'outils unifiée permettant de créer des services cloud AWS pour votre application React. Pour installer la CLI Amplify, exécutez :
	`npm install -g @aws-amplify/cli`
	npm vous informera si une nouvelle version majeure est disponible. Si tel est le cas, utilisez la commande suivante pour mettre à niveau votre version de npm :
	`npm install -g npm@9.8.0`
	où 9.8.0 fait référence à la version que vous souhaitez installer.
		Développeur d’applications

Création d'une application React

Tâche	Description	Compétences requises

Créez une application React.	Pour créer une nouvelle application React, utilisez la commande :
	`npx create-react-app amplify-react-application`
	où `amplify-react-application` est le nom de l'application.
	Lorsque l'application a été créée avec succès, le message suivant s'affiche :
	`Success! Created amplify-react-application`
	Un répertoire avec différents sous-dossiers sera créé pour l'application React.
		Développeur d’applications

Lancez l'application sur votre ordinateur local.	Accédez au répertoire `amplify-react-application` créé à l'étape précédente et exécutez la commande : `amplify-react-application% npm start`	Développeur d’applications

Tâche	Description	Compétences requises
	Cela lance l'application React sur votre machine locale.	

Configuration de la CLI Amplify

Tâche	Description	Compétences requises
Configurez Amplify pour vous connecter à votre compte AWS.	Configurez Amplify en exécutant la commande : `amplify-react-application % amplify configure` La CLI Amplify vous demande de suivre ces étapes pour configurer l'accès à votre compte AWS : 1. Connectez-vous à votre compte d'administrateur AWS. 2. Spécifiez la région AWS que vous souhaitez utiliser. 3. Créez un utilisateur AWS Identity and Access Management (IAM) doté d'un accès programmatique et associez la politique d'`AdministratorAccess-Amplify` autorisation à l'utilisateur.	AWS général, développeur d'applications

Tâche	Description	Compétences requises
	4. Créez puis copiez l'ID de clé d'accès et la clé d'accès secrète. 5. Entrez ces informations dans le terminal. 6. Créez un nom de profil ou utilisez le profil par défaut. ⚠ Warning Ce scénario nécessite que les utilisateurs IAM disposent d'un accès programmatique et d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires. Les clés d'accès peuvent être mises à jour si nécessaire. Pour plus d'informations, consultez la section	

Tâche	Description	Compétences requises

	Mise à jour des clés d'accès dans le guide de l'utilisateur IAM.
	
	Ces étapes apparaissent dans le terminal comme suit.
	
	`Follow these steps to set up access to your AWS account:`
	`Sign in to your AWS administrator account: https://console.aws.amazon.com/`
	`Press Enter to continue`
	`Specify the AWS Region`
	`? region: us-east-1`
	`Follow the instructions at https://docs.amplify.aws/cli/start/install/#configure-the-amplify-cli`
	`to complete the user creation in the AWS console`
	`https://console.aws.amazon.com/iamv2/home#/users/create`
	`Press Enter to continue`
	`Enter the access key of the newly created user:`
	`? accessKeyId: ********************`
	`? secretAccessKey: ********************`
	`****`	

Tâche	Description	Compétences requises

	`This would update/cr eate the AWS Profile in your local machine ? Profile Name: new`
	
	`Successfully set up the new user.`
	
	Pour plus d'informations sur ces étapes, consultez la documentation du centre de développement Amplify.	

Initialiser Amplify

Tâche	Description	Compétences requises

Initialisez Amplify.	1. Pour initialiser Amplify dans le nouveau répertoire, exécutez :
	
	`amplify init`
	
	Amplify vous demande le nom du projet et les paramètres de configuration
	2. Spécifiez tous les paramètres, puis appuyez sur Y pour initialiser le projet avec la configuration spécifiée.
	
	`Project information | Name: amplifyre actproject`
		Développeur d'applications, AWS général

Tâche	Description	Compétences requises

	<pre>| Environment: dev
	
	| Default editor:
	Visual Studio Code
	
	| App type: javascrip
	t
	
	| Javascript
	framework: react
	
	| Source Directory
	Path: src
	
	| Distribution
	Directory Path: build
	
	| Build Command: npm
	run-script build
	
	| Start Command: npm
	run-script start</pre> 3. Sélectionnez le profil que vous avez créé à l'étape précédente. Les ressources seront déployées dans l'devenvironnement du projet Amplify que vous avez créé.
	4. Pour confirmer que les ressources ont été créées, vous pouvez ouvrir la console AWS Amplify et consulter le CloudFormation modèle AWS utilisé pour créer les ressources ainsi que les détails.	

Tâche	Description	Compétences requises

	<pre>Deploying root stack
	 amplifyreactproject
	 [==========
	==========
	----] 2/4
	amplify-amplif
	yreactproject-d…
	 AWS::CloudFormatio
	n::Stack
	 CREATE_IN_PROGRESS
	
	UnauthRole
	  AWS::IAM:
	:Role
	 CREATE_COMPLETE
	
	DeploymentBucket
	  AWS::S3::
	Bucket
	 CREATE_IN_PROGRESS
	
	AuthRole
	  AWS::IAM:
	:Role
	 CREATE_COMPLETE</pre>	

Ajouter l'authentification au frontend

Tâche	Description	Compétences requises
Ajout de l'authentification.	Vous pouvez utiliser la `amplify add <category>` commande pour ajouter des fonctionnalités telles qu'un	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	identifiant utilisateur ou une API principale. Au cours de cette étape, vous allez utiliser la commande pour ajouter l'authentification. Amplify fournit un service d'authentification principal avec Amazon Cognito, des bibliothèques frontales et un composant d'interface utilisateur d'authentification intégré. Les fonctionnalités incluent l'inscription des utilisateurs, la connexion des utilisateurs, l'authentification multifactorielle, la déconnexion des utilisateurs et la connexion sans mot de passe. Vous pouvez également authentifier les utilisateurs en intégrant des fournisseurs d'identité fédérés tels qu'Amazon, Google et Facebook. La catégorie d'authentification Amplify s'intègre parfaitement aux autres catégories Amplify telles que les API, les analyses et le stockage, afin que vous puissiez définir des règles d'autorisation pour les utilisateurs authentifiés et non authentifiés.	

Tâche	Description	Compétences requises

	1. Pour configurer l'authentification pour votre application React, exécutez la commande :
	
	`amplify-react-application1 % amplify add auth`
	
	Cela affiche les informations et les instructions suivantes. Vous pouvez choisir la configuration appropriée en fonction de votre activité et de vos exigences en matière de sécurité.
	
	`Using service: Cognito, provided by: awscloudformation The current configured provider is Amazon Cognito. Do you want to use the default authentication and security configuration? (Use arrow keys)`
	
	`# Default configuration`
	
	`Default configuration with Social Provider (Federation)`	

Tâche	Description	Compétences requises

	<pre> Manual configura
	tion
	
	  I want to learn
	 more.</pre>
	2. Pour un exemple simple, choisissez la configuration par défaut, puis sélection nez le mécanisme de connexion pour les utilisate urs (dans ce cas, e-mail) :
	<pre>How do you want users
	 to be able to sign
	 in?
	 Username
	
	# Email
	
	  Phone Number
	
	  Email or Phone
	 Number
	
	  I want to learn
	 more.</pre>
	3. Contournez les paramètre s avancés pour terminer l'ajout de ressources d'authentification :
	<pre>Do you want to
	 configure advanced
	 settings? (Use arrow
	 keys)
	# No, I am done.</pre>	

Tâche	Description	Compétences requises
	<pre> Yes, I want to make some additional changes.</pre>	

	4. Développez vos ressources de backend locales et provisionnez-les dans le cloud :
	<pre>amplify-react-application1 % amplify push</pre>Cette commande apporte les modifications appropriées aux groupes d'utilisateurs Conbito de votre compte.
	5. Appuyez sur Y pour configurer la `auth` ressource en utilisant CloudFormation.
	Cela permet de configurer les ressources suivantes :
	<pre>UserPool
	           AWS::Cognito::UserPool
	  CREATE_COMPLETE
	UserPoolClientWeb
	            AWS::Cognito::UserPoolClient
	   CREATE_COMPLETE
	
	UserPoolClientWeb
	            AWS::Cognito::UserPoolClient</pre>	

Tâche	Description	Compétences requises

	<pre>CREATE_COMPLETE
	
	UserPoolClientRole
	AWS::IAM::Role
	CREATE_COMPLETE
	
	UserPoolClientLambda
	AWS::Lambda::Function
	CREATE_COMPLETE
	UserPoolClientLambdaPolicy
	AWS::IAM::Policy
	CREATE_COMPLETE
	
	UserPoolClientLogPolicy
	AWS::IAM::Policy
	CREATE_IN_PROGRESS</pre>
	Vous pouvez également utiliser la console AWS Cognito pour consulter ces ressources (recherchez les groupes d'utilisateurs et les groupes d'identités Cognito).
	
	Cette étape met à jour le `aws-exports.js` fichier du `src` dossier de votre application React avec les configurations du groupe	

Tâche	Description	Compétences requises
	d'utilisateurs et du pool d'identités Cognito.	

Modifiez le fichier App.js

Tâche	Description	Compétences requises
Modifiez le fichier App.js.	Dans le `src` dossier, ouvrez le `App.js` fichier et modifiez-le. Le fichier modifié doit ressembler à ceci : `{ App.Js File after modifications: import React from 'react'; import logo from './logo.svg'; import './App.css'; import { Amplify } from 'aws-amplify'; import { withAuthenticator, Button, Heading } from '@aws-amplify/ui-react'; import awsconfig from './aws-exports'; Amplify.configure(awsconfig); function App({ signOut }) { return (<div> <h1>Thankyou for doing verification</h1> <h2>My Content</h2>`	Développeur d’applications

Tâche	Description	Compétences requises
	<button onClick={ signOut}>Sign out</ button>); } export default withAuthenticator(App);	
Importez des packages React.	Le `App.js` fichier importe deux packages React. Installez ces packages à l'aide de la commande : `amplify-react-appl ication1 % npm install --save aws-amplify @aws-amplify/ui-react`	Développeur d'applications

Lancez l'application React et vérifiez l'authentification

Tâche	Description	Compétences requises
Lancez l'application.	Lancez l'application React sur votre machine locale : `amplify-react-appl ication1 % npm start`	Développeur d'applications, AWS général
Vérifiez l'authentification.	Vérifiez si l'application demande des paramètre s d'authentification. (Dans notre exemple, nous avons configuré le courrier électroni	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	que comme méthode de connexion.) L'interface utilisateur du frontend doit vous demander vos informations de connexion et vous proposer la possibilité de créer un compte. Vous pouvez également configurer le processus de génération d'Amplify pour ajouter le backend dans le cadre d'un flux de travail de déploiement continu. Cependant, ce modèle ne couvre pas cette option.	

Ressources connexes

- Mise en route (documentation npm)
- Création d'un compte AWS autonome (documentation sur la gestion des comptes AWS)
- Documentation AWS Amplify
- Documentation Amazon Cognito

Créez un portail pour les micro-frontends en utilisant AWS Amplify Angular et Module Federation

Créée par Milena Godau (AWS) et Pedro Garcia (AWS)

Récapitulatif

Une architecture micro-frontend permet à plusieurs équipes de travailler indépendamment sur différentes parties d'une application frontale. Chaque équipe peut développer, créer et déployer un fragment du frontend sans interférer avec les autres parties de l'application. Du point de vue de l'utilisateur final, il semble s'agir d'une application unique et cohérente. Cependant, ils interagissent avec plusieurs applications indépendantes publiées par différentes équipes.

Ce document décrit comment créer une architecture de micro-frontend en utilisant AWS Amplifyle framework d'interface Angular et la fédération de modules. Dans ce modèle, les micro-frontends sont combinés côté client par une application shell (ou parent). L'application shell agit comme un conteneur qui récupère, affiche et intègre les micro-frontends. L'application shell gère le routage global, qui charge différents micro-frontends. Le plugin @angular -architects/module-federation intègre Module Federation à Angular. Vous déployez l'application shell et les micro-frontends à l'aide de. AWS Amplify Les utilisateurs finaux accèdent à l'application via un portail Web.

Le portail est divisé verticalement. Cela signifie que les micro-frontends sont des vues entières ou des groupes de vues, et non des parties de la même vue. Par conséquent, l'application shell ne charge qu'un seul micro-frontend à la fois.

Les micro-frontends sont implémentés sous forme de modules distants. L'application shell charge paresseusement ces modules distants, ce qui reporte l'initialisation du micro-frontend jusqu'à ce qu'elle soit requise. Cette approche optimise les performances des applications en chargeant uniquement les modules nécessaires. Cela réduit le temps de chargement initial et améliore l'expérience utilisateur globale. De plus, vous partagez des dépendances communes entre les modules via le fichier de configuration du pack Web (webpack.config.js). Cette pratique favorise la réutilisation du code, réduit les doublons et rationalise le processus de regroupement.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS

- Node.js et npm, installés
- Amplify CLI, installée
- CLI angulaire, installée
- Autorisations d'utilisation AWS Amplify
- Connaissance d'Angular

Versions du produit

- Angular CLI version 13.1.2 ou ultérieure
- @angular -architects/module-federation version 14.0.1 ou ultérieure
- webpack version 5.4.0 ou ultérieure
- AWS Amplify 1re génération

Limites

Une architecture micro-frontend est une approche puissante pour créer des applications Web évolutives et résilientes. Cependant, il est essentiel de comprendre les défis potentiels suivants avant d'adopter cette approche :

- Intégration — L'un des principaux défis est l'augmentation potentielle de la complexité par rapport aux interfaces monolithiques. L'orchestration de plusieurs micro-frontends, la gestion des communications entre elles et la gestion des dépendances partagées peuvent s'avérer plus complexes. De plus, il peut y avoir une surcharge de performance associée à la communication entre les micro-frontends. Cette communication peut augmenter le temps de latence et réduire les performances. Cela doit être résolu par des mécanismes de messagerie efficaces et des stratégies de partage de données.
- Duplication de code — Chaque micro-frontend étant développé indépendamment, il existe un risque de duplication de code pour des fonctionnalités communes ou des bibliothèques partagées. Cela peut augmenter la taille globale de l'application et poser des problèmes de maintenance.
- Coordination et gestion — La coordination des processus de développement et de déploiement sur plusieurs micro-frontends peut s'avérer difficile. Dans une architecture distribuée, il est de plus en plus essentiel de garantir un versionnement cohérent, de gérer les dépendances et de maintenir la compatibilité entre les composants. L'établissement d'une gouvernance claire, de directives et de pipelines de test et de déploiement automatisés est essentiel pour une collaboration et une livraison fluides.

- Tests — Il peut être plus complexe de tester des architectures de micro-frontend que de tester des frontends monolithiques. Cela nécessite des efforts supplémentaires et des stratégies de test spécialisées pour effectuer des tests et end-to-end des tests d'intégration entre composants, et pour valider des expériences utilisateur cohérentes sur plusieurs micro-frontends.

Avant de vous engager dans l'approche micro-frontend, nous vous recommandons de consulter Comprendre et implémenter les micro-frontends sur. AWS

Architecture

Dans une architecture micro-frontend, chaque équipe développe et déploie des fonctionnalités de manière indépendante. L'image suivante montre comment plusieurs DevOps équipes travaillent ensemble. L'équipe du portail développe l'application shell. L'application shell agit comme un conteneur. Il récupère, affiche et intègre les applications micro-frontend publiées par d'autres équipes. DevOps Vous l'utilisez AWS Amplify pour publier l'application shell et les applications micro-frontend.

Le schéma d'architecture montre le flux de travail suivant :

1. L'équipe du portail développe et gère l'application shell. L'application shell orchestre l'intégration et le rendu des micro-frontends afin de composer l'ensemble du portail.
2. Les équipes A et B développent et maintiennent une ou plusieurs micro-interfaces ou fonctionnalités intégrées au portail. Chaque équipe peut travailler indépendamment sur ses micro-frontends respectifs.
3. L'utilisateur final s'authentifie à l'aide d'Amazon Cognito.
4. L'utilisateur final accède au portail et l'application shell est chargée. Pendant que l'utilisateur navigue, l'application shell s'occupe du routage et récupère le micro-frontend demandé pour charger son bundle.

Outils

Services AWS

- AWS Amplifyest un ensemble d'outils et de fonctionnalités spécialement conçus pour aider les développeurs Web et mobiles frontaux à créer rapidement des applications complètes. AWS Dans ce modèle, vous utilisez la CLI Amplify pour déployer les applications du micro-frontend Amplify.

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.

Autres outils

- @angular -architects/module-federation est un plugin qui intègre Angular à Module Federation.
- Angular est un framework d'applications Web open source permettant de créer des applications d'une seule page modernes, évolutives et testables. Il suit une architecture modulaire basée sur des composants qui favorise la réutilisation et la maintenance du code.
- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.
- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.
- Webpack Module Federation vous aide à charger du code compilé et déployé indépendamment, tel que des micro-frontends ou des plugins, dans une application.

Référentiel de code

Le code de ce modèle est disponible sur le portail Micro-frontend à l'aide du référentiel Angular et Module Federation GitHub . Ce dépôt contient les deux dossiers suivants :

- `shell-app`contient le code de l'application shell.
- `feature1-app`contient un exemple de micro-frontend. L'application shell récupère ce micro-frontend et l'affiche sous forme de page dans l'application portail.

Bonnes pratiques

Les architectures micro-frontend offrent de nombreux avantages, mais elles introduisent également de la complexité. Voici quelques bonnes pratiques pour un développement fluide, un code de haute qualité et une expérience utilisateur exceptionnelle :

- Planification et communication — Pour rationaliser la collaboration, investissez dans la planification initiale, la conception et dans des canaux de communication clairs.
- Cohérence de conception : appliquez un style visuel cohérent sur les micro-frontends à l'aide de systèmes de conception, de guides de style et de bibliothèques de composants. Cela permet d'offrir une expérience utilisateur cohérente et d'accélérer le développement.

- Gestion des dépendances : les micro-frontends évoluant de manière indépendante, adoptez des contrats standardisés et des stratégies de gestion des versions pour gérer efficacement les dépendances et éviter les problèmes de compatibilité.
- Architecture micro-frontend — Pour permettre un développement et un déploiement indépendants, chaque micro-frontend doit avoir une responsabilité claire et bien définie pour une fonctionnalité encapsulée.
- Intégration et communication — Pour faciliter l'intégration et minimiser les conflits, définissez des contrats et des protocoles de communication clairs entre les micro-interfaces APIs, y compris les événements et les modèles de données partagés.
- Tests et assurance qualité — Mettez en œuvre l'automatisation des tests et des pipelines d'intégration continue pour les micro-frontends. Cela améliore la qualité globale, réduit les efforts de test manuel et valide les fonctionnalités entre les interactions entre les micro-frontend.
- Optimisation des performances — Surveillez en permanence les indicateurs de performance et suivez les dépendances entre les micro-frontends. Cela vous permet d'identifier les goulots d'étranglement et de maintenir des performances applicatives optimales. Utilisez des outils de surveillance des performances et d'analyse des dépendances à cette fin.
- Expérience du développeur : concentrez-vous sur l'expérience du développeur en fournissant une documentation, des outils et des exemples clairs. Cela vous permet de rationaliser le développement et d'intégrer de nouveaux membres à l'équipe.

Épopées

Création de l'application shell

Tâche	Description	Compétences requises
Créez l'application shell.	1. Dans la CLI angulaire , entrez la commande suivante : `ng new shell --routing` 2. Entrez la commande suivante pour accéder au dossier du projet :	Développeur d’applications

Tâche	Description	Compétences requises
	`cd shell` **Note** La structure des dossiers et des projets pour les applications shell et micro-frontend peut être totalemen t indépendante. Ils peuvent être gérés comme des applicati ons angulaires indépendantes.	
Installez le plug-in .	Dans la CLI angulaire, entrez la commande suivante pour installer le plugin @angular - architects/module-federation : `ng add @angular-architects/module-federation --project shell --port 4200`	Développeur d’applications

Tâche	Description	Compétences requises
Ajoutez l'URL du micro-frontend en tant que variable d'environnement.	1. Ouvrez le fichier environment.ts. 2. Ajoutez `mfe1URL: 'http://localhost:5000'` à l'`environment` objet : `export const environment = { production: false, mfe1URL: 'http://localhost:5000', };` 3. Enregistrez et fermez le fichier environment.ts.	Développeur d’applications

Tâche	Description	Compétences requises

Définissez le routage.	1. Ouvrez le fichier app-routing.module.ts.
	2. Dans la CLI angulaire, entrez la commande suivante pour importer le `loadRemoteModule` module depuis le plugin @angular -architects/module-federation :
	`import { loadRemoteModule } from '@angular-architects/module-federation';`
	3. Définissez l'itinéraire par défaut comme suit :
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	4. Définissez l'itinéraire pour le micro-frontend :
	`{ path: 'mfe1', loadChildren: () => loadRemoteModule({ type: 'module',`
		Développeur d’applications

Tâche	Description	Compétences requises
	<pre>remoteEntry: `${environment.mfe1URL}/remoteEntry.js`, exposedModule: './Module' }) .then(m => m.Mfe1Module) },</pre> 5. Enregistrez et fermez le fichier app-routing.module.ts.	
Déclarez le `mfe1` module.	1. Dans le `src` dossier, créez un nouveau fichier nommé decl.d.ts. 2. Ouvrez le fichier decl.d.ts. 3. Ajoutez ce qui suit au fichier : <pre>declare module 'mfe1/Module';</pre> 4. Enregistrez et fermez le fichier decl.d.ts.	Développeur d’applications

Tâche	Description	Compétences requises

Préparez le préchargement pour le micro-frontend.	Le préchargement du micro-frontend aide le webpack à négocier correctement les bibliothèques et les packages partagés.
	1. Ouvrez le fichier main.ts.
	2. Remplacez le contenu par le suivant :
	`import { loadRemoteEntry } from '@angular-architects/module-federation';`
	`Promise.all([ loadRemoteEntry(`${environment.mfe1URL}/remoteEntry.js`, 'mfe1'), ]) .catch(err => console.error('Error loading remote entries', err)) .then(() => import('./bootstrap')) .catch(err => console.error(err) );`
	3. Enregistrez et fermez le fichier main.ts.
		Développeur d’applications

Tâche	Description	Compétences requises
Ajustez le contenu HTML.	1. Ouvrez le fichier app.component.html. 2. Remplacez le contenu par le suivant : `<h1>Shell application is running!</h1><router-outlet></router-outlet>` 3. Enregistrez et fermez le fichier app.component.html.	Développeur d’applications

Création de l'application micro-frontend

Tâche	Description	Compétences requises

Créez le micro-frontend.	1. Dans la CLI angulaire , entrez la commande suivante :
	`ng new mfe1 --routing`
	2. Entrez la commande suivante pour accéder au dossier du projet :
	`cd mfe1`
		Développeur d’applications

Installez le plug-in .	Entrez la commande suivante pour installer le plugin @angular -architects/module-federation : `ng add @angular-architects/module-`	Développeur d’applications

Tâche	Description	Compétences requises
	`federation --project mfe1 --port 5000`	

Créez un module et un composant.	Entrez les commandes suivantes pour créer un module et un composant et les exporter en tant que module de saisie à distance :
	`ng g module mfe1 --routing`
	`ng g c mfe1`
		Développeur d'applications

Définissez le chemin de routage par défaut.	1. Ouvrez le fichier mfe-routing.module.ts. 2. Définissez l'itinéraire par défaut comme suit : `{ path: '', component: Mfe1Component },` 3. Enregistrez et fermez le fichier mfe-routing.module.ts.	Développeur d'applications

Tâche	Description	Compétences requises

Ajoutez l'`mfe1`itinéraire.	1. Ouvrez le fichier app-routing.module.ts.
	2. Définissez l'itinéraire par défaut comme suit :
	`{ path: '', pathMatch: 'full', redirectTo: 'mfe1' },`
	3. Ajoutez l'`mfe1`itinéraire suivant :
	`{ path: 'mfe1', loadChildren: () => import('./mfe1/mfe1.module').then((m) => m.Mfe1Module), },`
	4. Enregistrez et fermez le fichier app-routing.module.ts.
		Développeur d’applications

Tâche	Description	Compétences requises

Modifiez le fichier webpack.config.js.	1. Ouvrez le fichier webpack.config.js.
	2. Modifiez la `For remotes` section pour qu'elle corresponde à ce qui suit :
	`// For remotes (please adjust)`
	`name: "mfe1",`
	`filename: "remoteEntry.js",`
	`exposes: {`
	`'./Module': './src/app/mfe1/mfe1.module.ts',`
	`},`
	3. Dans la `shared` section, ajoutez les dépendances que l'`mfe1`application partage avec l'application shell :
	`shared: share({`
	`"@angular/core": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
	`"@angular/common": { singleton: true, strictVersion: true, requiredVersion: 'auto' },`
	`"@angular/common/http": { singleton: true, strictVersion: true,`
		Développeur d’applications

Tâche	Description	Compétences requises
	requiredVersion: 'auto' }, "@angular/router": { singleton: true, strictVersion: true, requiredVersion: 'auto' }, ...sharedMappings.getDescriptors() }) 4. Enregistrez et fermez le fichier webpack.config.js.	
Ajustez le contenu HTML.	1. Ouvrez le fichier app.component.html. 2. Remplacez le contenu par le suivant : `<router-outlet></router-outlet>` 3. Enregistrez et fermez le fichier app.component.html.	Développeur d'applications

Exécutez les applications localement

Tâche	Description	Compétences requises
Lancez l'`mfe1`application.	1. Entrez la commande suivante pour démarrer l'`mfe1`application : `npm start`	Développeur d'applications

Tâche	Description	Compétences requises
	2. Dans un navigateur Web, accédez à`http://localhost:5000`. 3. Vérifiez que le micro-frontend peut être exécuté de manière autonome. L'`mfe1`application doit s'afficher correctement sans aucune erreur.	
Exécutez l'application shell.	1. Entrez la commande suivante pour démarrer l'application shell : `npm start` 2. Dans un navigateur Web, accédez à`http://localhost:4200/mfe1`. 3. Vérifiez que le `mfe1` micro-frontend est intégré à l'application shell. L'application du portail doit s'afficher correctement, sans aucune erreur, et l'`mfe1`application doit y être intégrée.	Développeur d’applications

Refactoriser l'application shell pour gérer une erreur de chargement du micro-frontend

Tâche	Description	Compétences requises
Créez un module et un composant.	Dans le dossier racine de l'application shell, entrez les commandes suivantes pour créer un module et un	Développeur d’applications

Tâche	Description	Compétences requises

	composant pour une page d'erreur :
	`ng g module error-page --routing`
	`ng g c error-page`	

Ajustez le contenu HTML.	1. Ouvrez le fichier error-page.component.html. 2. Remplacez le contenu par le suivant : `<p>Sorry, this page is not available.</p>` 3. Enregistrez et fermez le fichier error-page.component.html.	Développeur d’applications
Définissez le chemin de routage par défaut.	1. Ouvrez le fichier error-page-routing.module.ts. 2. Définissez l'itinéraire par défaut comme suit : `{ path: '', component: ErrorPageComponent },` 3. Enregistrez et fermez le error-page-routing fichier .module.ts.	Développeur d’applications

Tâche	Description	Compétences requises

Créez une fonction pour charger les micro-frontends.	1. Ouvrez le fichier app-routing.module.ts.
	2. Créez la fonction suivante :
	`function loadMFE(url: string) { return loadRemoteModule({ type: 'module', remoteEntry: `${url}/remoteEntry.js`, exposedModule: './Module' }) .then(m => m.Mfe1Module) .catch( () => import('./error-page/error-page.module').then(m => m.ErrorPageModule) ); }`
	3. Modifiez l'`mfe1`itinéraire comme suit :
	`{ path: 'mfe1', loadChildren: () => loadMFE(environment.mfe1URL) },`
		Développeur d'applications

Tâche	Description	Compétences requises
	4. Enregistrez et fermez le fichier app-routing.module .ts.	

Testez la gestion des erreurs.	1. Si ce n'est pas déjà fait, entrez la commande suivante pour démarrer l'application shell :
	`npm start`
	2. Dans un navigateur Web, accédez à`http://localhost:4200/mfe1` .
	3. Vérifiez que la page d'erreur est affichée. Vous devriez voir le texte suivant :
	`Sorry, this page is not available.`
		Développeur d’applications

Déployez les applications en utilisant AWS Amplify

Tâche	Description	Compétences requises
Déployez le micro-frontend.	1. Dans la CLI Amplify, accédez au dossier racine de l'application micro-frontend. 2. Entrez la commande suivante pour initialiser Amplify :	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises

	`amplify init`
	3. Lorsque vous êtes invité à saisir un nom pour votre projet Amplify, appuyez sur Entrée. Cela réutilise le nom du fichier package.json.
	4. Lorsque vous êtes invité à initialiser le projet avec la configuration ci-dessus, entrez`Yes`.
	5. Lorsque vous êtes invité à sélectionner une méthode d'authentification, choisissez`AWS Profile`.
	6. Sélectionnez le profil que vous souhaitez utiliser.
	7. Attendez qu'Amplify initialise le projet. Lorsque ce processus est terminé, vous recevez un message de confirmation dans le terminal.
	8. Entrez la commande suivante pour ajouter une catégorie d'hébergement Amplify au micro-frontend :
	`amplify add hosting`
	9. Lorsque vous êtes invité à sélectionner le module du	

Tâche	Description	Compétences requises

	plugin, choisissezHosting with Amplify Console.
	10. Lorsque vous êtes invité à choisir un type, choisisse zManual deployment .
	11. Installez les dépendances npm du projet en saisissant la commande suivante :
	`npm install`
	12. Publiez l'application sur la console Amplify en saisissant la commande suivante :
	`amplify publish -y`
	Lorsque la publication est terminée, Amplify renvoie l'URL du micro-frontend.
	13. Copiez l'URL. Vous avez besoin de cette valeur pour mettre à jour l'application shell.	

Tâche	Description	Compétences requises

Déployez l'application shell.	1. Dans le src/app/environments dossier, ouvrez le fichier environments.prod.ts.
	2. Remplacez la `mfe1URL` valeur par l'URL du micro-frontend déployé :
	`export const environment = { production: true, mfe1URL: 'https://<env>.<Amplify-app-ID>.amplifyapp.com' };`
	3. Enregistrez et fermez le fichier environments.prod.ts.
	4. Dans la CLI Amplify, accédez au dossier racine de l'application shell.
	5. Entrez la commande suivante pour initialiser Amplify :
	`amplify init`
	6. Lorsque vous êtes invité à saisir un nom pour votre projet Amplify, appuyez sur Entrée. Cela réutilise le nom du fichier package.json.
	7. Lorsque vous êtes invité à initialiser le projet avec
		Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises

	la configuration ci-dessus, entrezYes.
	8. Lorsque vous êtes invité à sélectionner une méthode d'authentification, choisissez`AWS Profile`.
	9. Sélectionnez le profil que vous souhaitez utiliser.
	10 Attendez qu'Amplify initialise le projet. Lorsque ce processus est terminé, vous recevez un message de confirmation dans le terminal.
	11 Ajoutez une catégorie d'hébergement Amplify à l'application shell :
	`amplify add hosting`
	12 Lorsque vous êtes invité à sélectionner le module du plugin, choisissez`Hosting with Amplify Console`.
	13 Lorsque vous êtes invité à choisir un type, choisissez`Manual deployment` .
	14 Installez les dépendances npm du projet en saisissant la commande suivante :
	`npm install`
	15 Publiez l'application shell sur la console Amplify en	

Tâche	Description	Compétences requises
	saisissant la commande suivante : `amplify publish -y` Lorsque la publication est terminée, Amplify renvoie l'URL de l'application shell déployée. 16. Prenez note de l'URL de l'application shell.	

Tâche	Description	Compétences requises
Activez CORS.	Les applications shell et micro-frontend étant hébergées indépendamment sur des domaines différents, vous devez activer le partage de ressources entre origines (CORS) sur le micro-frontend. Cela permet à l'application shell de charger le contenu depuis une autre origine. Pour activer CORS, vous devez ajouter des en-têtes personnalisés. 1. Dans la CLI Amplify, accédez au dossier racine du micro-frontend. 2. Entrez la commande suivante : `amplify configure hosting` 3. Lorsque vous êtes invité à configurer des paramètres personnalisés, entrezY. 4. Connectez-vous à la console Amplify AWS Management Console, puis ouvrez-la. 5. Choisissez le micro-frontend. 6. Dans le volet de navigation, choisissez Hosting, puis Custom headers.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises

	7. Choisissez Modifier.
	8. Dans la fenêtre Modifier les en-têtes personnalisés, entrez ce qui suit :
	`customHeaders:`
	`  - pattern: '*.js'`
	`  headers:`
	`  - key: Access-Control-Allow-Origin`
	`  value: '*'`
	`  - key: Access-Control-Allow-Methods`
	`  value: 'GET, OPTIONS'`
	`  - key: Access-Control-Allow-Headers`
	`  value: '*'`
	9. Choisissez Enregistrer.
	10. Redéployez le micro-frontend pour appliquer les nouveaux en-têtes personnalisés.	

Tâche	Description	Compétences requises
Créez une règle de réécriture sur l'application shell.	L'application Angular Shell est configurée pour utiliser HTML5 le routage. Si l'utilisateur effectue une actualisation complète, Amplify essaie de charger une page à partir de l'URL actuelle. Cela génère une erreur 403. Pour éviter cela, vous devez ajouter une règle de réécriture dans la console Amplify. Pour créer la règle de réécriture, procédez comme suit : 1. Dans la CLI Amplify, accédez au dossier racine de l'application shell. 2. Entrez la commande suivante : `amplify configure hosting` 3. Lorsque vous êtes invité à configurer des paramètres personnalisés, entrezY. 4. Ouvrez la console Amplify. 5. Choisissez l'application shell. 6. Dans le volet de navigation, choisissez Hosting, puis Rewrites and redirections.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	7. Sur la page Réécritures et redirections, choisissez Gérer les redirections. 8. Choisissez Ouvrir un éditeur de texte. 9. Dans l'éditeur JSON, entrez la redirection suivante : `[ { "source": "/<*>", "target": "/index.html", "status": "404-200", "condition": null } ]` 10. Choisissez Enregistrer.	
Testez le portail Web.	1. Dans un navigateur Web, entrez l'URL de l'application shell déployée. 2. Vérifiez que l'application shell et le micro-frontend se chargent correctement.	Développeur d’applications

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez les applications.	Si vous n'avez plus besoin du shell et des applications micro-	AWS général

Tâche	Description	Compétences requises
	frontend, supprimez-les. Cela permet d'éviter de facturer des ressources que vous n'utilisez pas. 1. Connectez-vous à la console Amplify AWS Management Console, puis ouvrez-la. 2. Choisissez le micro-fro ntend. 3. Dans le volet de navigatio n, choisissez Paramètre s de l'application, puis Paramètres généraux. 4. Choisissez Delete app (Supprimer l'appli). 5. Dans la fenêtre de confirmation, entrez`delete`, puis choisissez Supprimer l'application. 6. Répétez ces étapes pour supprimer l'application shell.	

Résolution des problèmes

Problème	Solution
Aucun AWS profil disponible lors de l'exécution de la `amplify init` commande	Si aucun AWS profil n'est configuré, vous pouvez toujours exécuter la `amplify init` commande. Toutefois, vous devez sélection

Problème	Solution
	ner l'`AWS access keys`option lorsque vous êtes invité à saisir la méthode d'authentification. Ayez votre clé AWS d'accès et votre clé secrète à portée de main. Vous pouvez également configurer un profil nommé pour AWS CLI. Pour obtenir des instructions, consultez la section Configuration et paramètres des fichiers d'identification dans la AWS CLI documentation.
Erreur lors du chargement des entrées distantes	Si vous rencontrez une erreur lors du chargement des entrées distantes dans le fichier main.ts de l'application shell, assurez-vous que la `environment.mfe1URL` variable est correctement définie. La valeur de cette variable doit être l'URL du micro-frontend.
Erreur 404 lors de l'accès au micro-frontend	Si vous obtenez une erreur 404 lorsque vous essayez d'accéder au micro-frontend local, par exemple à`http://localhost:4200/mfe1`, vérifiez les points suivants : • Pour l'application shell, assurez-vous que la configuration de routage dans le fichier app-routing.module.ts est correctement configuré e et que la fonction appelle correctement le micro-frontend. `loadRemoteModule` • Pour le micro-frontend, vérifiez que le fichier webpack.config.js est correctement **exposes** configuré et que le fichier remoteEntry.js est correctement généré.

Informations supplémentaires

AWS documentation

- Comprendre et implémenter des micro-frontends sur AWS(directivesAWS prescriptives)
- Amplify CLI (documentation Amplify)
- Hébergement Amplify (documentation Amplify)

Autres références

- Fédération de modules
- Node.js
- Angulaire
- @angular -architects/module-federation

Déployez une application monopage basée sur React sur Amazon S3 et CloudFront

Créée par Jean-Baptiste Guillois (AWS)

Récapitulatif

Une application monopage (SPA) est un site Web ou une application Web qui met à jour dynamiquement le contenu d'une page Web affichée en utilisant JavaScript APIs. Cette approche améliore l'expérience utilisateur et les performances d'un site Web car elle ne met à jour que les nouvelles données au lieu de recharger l'intégralité de la page Web depuis le serveur.

Ce modèle fournit une step-by-step approche pour coder et héberger un SPA écrit dans React sur Amazon Simple Storage Service (Amazon S3) et Amazon. CloudFront Dans ce modèle, le SPA utilise une API REST configurée dans Amazon API Gateway et exposée via une CloudFront distribution Amazon afin de simplifier la gestion du partage de ressources entre origines (CORS).

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Node.js et`npm`, installé et configuré. Pour plus d'informations, consultez la section Téléchargements de la documentation Node.js.
- Yarn, installé et configuré. Pour plus d'informations, consultez la documentation Yarn.
- Git, installé et configuré. Pour plus d'informations, consultez la documentation Git.

Architecture

Cette architecture est automatiquement déployée en utilisant AWS CloudFormation (infrastructure en tant que code). Il utilise des services régionaux tels qu'Amazon S3 pour stocker les actifs statiques et Amazon CloudFront avec Amazon API Gateway pour exposer les points de terminaison d'API régionaux (REST). Les journaux des applications sont collectés à l'aide d'Amazon CloudWatch. Tous les appels AWS d'API sont audités dans AWS CloudTrail. Toute la configuration de sécurité (par exemple, les identités et les autorisations) est gérée dans AWS Identity and Access Management (IAM). Le contenu statique est diffusé via le réseau de diffusion de CloudFront contenu (CDN) Amazon et les requêtes DNS sont gérées par Amazon Route 53.

Outils

Services AWS

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- Amazon CloudFront accélère la diffusion de votre contenu Web en le diffusant via un réseau mondial de centres de données, ce qui réduit le temps de latence et améliore les performances.
- AWS CloudTrailvous aide à auditer la gouvernance, la conformité et le risque opérationnel de votre Compte AWS
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

L'exemple de code d'application de ce modèle est disponible dans le référentiel d'applications d'une seule page CORS GitHub basé sur React.

Bonnes pratiques

En utilisant le stockage d'objets Amazon S3, vous pouvez stocker les actifs statiques de votre application de manière sécurisée, hautement résiliente, performante et rentable. Il n'est pas nécessaire d'utiliser un conteneur dédié ou une instance Amazon Elastic Compute Cloud (Amazon EC2) pour cette tâche.

En utilisant le réseau de diffusion de CloudFront contenu Amazon, vous pouvez réduire la latence que vos utilisateurs peuvent rencontrer lorsqu'ils accèdent à votre application. Vous pouvez également associer un pare-feu d'application Web (AWS WAF) pour protéger vos actifs contre les attaques malveillantes.

Épopées

Créez et déployez votre application localement

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Exécutez la commande suivante pour cloner le référentiel de l'exemple d'application : `git clone https://github.com/aws-samples/react-cors-spa react-cors-spa && cd react-cors-spa`	Développeur d'applications, AWS DevOps
Déployez l'application localement.	1. Dans le répertoire du projet, exécutez la `npm install` commande pour initier les dépendances de l'application. 2. Exécutez la `yarn dev` commande pour démarrer l'application localement.	Développeur d'applications, AWS DevOps
Accédez à l'application localement.	Ouvrez une fenêtre de navigateur et entrez l'`http://localhost:3000` URL pour accéder à l'application.	Développeur d'applications, AWS DevOps

Déployer l'application

Tâche	Description	Compétences requises
Déployez le AWS CloudFormation modèle.	1. Connectez-vous à la AWS CloudFormation console AWS Management Console, puis ouvrez-la. 2. Choisissez Create Stack, puis choisissez Avec de nouvelles ressources (standard). 3. Choisissez Charger un fichier de modèle. 4. Choisissez Choisir un fichier, choisissez le `react-cors-spa-stack.yaml` fichier dans le référentiel cloné, puis cliquez sur Suivant. 5. Entrez un nom pour votre pile, puis choisissez Next. 6. Conservez toutes les options par défaut, puis choisissez Next. 7. Passez en revue les paramètres finaux de votre pile, puis choisissez Create stack.	Développeur d'applications, AWS DevOps
Personnalisez les fichiers source de votre application.	1. Une fois votre stack déployé, ouvrez l'onglet Output et identifiez le `Bucket` nom et `APIDomain` la valeur.	Développeur d’applications

Tâche	Description	Compétences requises
	2. Copiez le domaine de CloudFront distribution pour l'API REST. 3. Accédez à ce domaine`<project_root>/src/pages/index.tsx` , puis insérez-le ou collez-le dans la valeur de la `APIEndPoint` variable à la ligne 13 du `index.tsx` fichier.	
Créez le package d'application.	Dans le répertoire de votre projet, exécutez la `yarn build` commande pour créer le package d'application.	Développeur d’applications

Tâche	Description	Compétences requises
Déployez le package d'application.	1. Ouvrez la console Amazon S3. 2. Identifiez et choisissez le compartiment S3 créé précédemment par la CloudFormation pile. 3. Choisissez Télécharger, puis Ajouter des fichiers. 4. Choisissez le contenu de votre `out` dossier. 5. Choisissez Ajouter un dossier, puis sélectionnez le `_next` répertoire. **Important** Choisissez le `_next` répertoire, pas le contenu. 6. Choisissez Upload pour télécharger les fichiers et le répertoire dans votre compartiment S3.	Développeur d'applications, AWS DevOps

Tester l'application

Tâche	Description	Compétences requises
Accédez à l'application et testez-la.	Ouvrez une fenêtre de navigateur, puis collez le domaine de CloudFront distribution (le `SPADomain` résultat de la CloudFormation	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	pile que vous avez déployée précédemment) pour accéder à l'application.	

Nettoyez les ressources

Tâche	Description	Compétences requises
Supprimez le contenu du compartiment S3.	1. Ouvrez la console Amazon S3 et choisissez le compartiment créé précédemment par la pile (le premier compartiment dont le nom commence par `react-cors-spa-`). 2. Choisissez Empty pour supprimer le contenu du compartiment. 3. Choisissez le deuxième compartiment créé précédemment par la pile (le deuxième compartiment dont le nom commence par `react-cors-spa-` et se termine par `-logs`). 4. Choisissez Empty pour supprimer le contenu du compartiment.	AWS DevOps, développeur d'applications
Supprimez la AWS CloudFormation pile.	1. Ouvrez la AWS CloudFormation console et choisissez la pile que vous avez créée précédemment.	AWS DevOps, développeur d'applications

Tâche	Description	Compétences requises
	2. Choisissez Supprimer pour supprimer la pile et toutes les ressources associées.	

Ressources connexes

Pour déployer et héberger votre application Web, vous pouvez également utiliser AWS Amplify Hosting, qui fournit un flux de travail basé sur Git pour héberger des applications Web complètes sans serveur avec un déploiement continu. Amplify Hosting en fait partie AWS Amplify, qui fournit un ensemble d'outils et de fonctionnalités spécialement conçus pour permettre aux développeurs Web et mobiles de créer rapidement et facilement des applications complètes. AWS

Informations supplémentaires

Pour traiter les URLs demandes non valides de l'utilisateur susceptibles de générer 403 erreurs, une page d'erreur personnalisée configurée dans la CloudFront distribution détecte 403 erreurs et les redirige vers le point d'entrée de l'application (`index.html`).

Pour simplifier la gestion de CORS, l'API REST est exposée par le biais d'une CloudFront distribution.

Déployez une API Amazon API Gateway sur un site Web interne à l'aide de points de terminaison privés et d'un Application Load Balancer

Créée par Saurabh Kothari (AWS)

Récapitulatif

Ce modèle vous montre comment déployer une API Amazon API Gateway sur un site Web interne accessible depuis un réseau sur site. Vous apprenez à créer un nom de domaine personnalisé pour une API privée en utilisant une architecture conçue avec des points de terminaison privés, un Application Load Balancer, PrivateLink AWS et Amazon Route 53. Cette architecture évite les conséquences imprévues de l'utilisation d'un nom de domaine personnalisé et d'un serveur proxy pour faciliter le routage basé sur le domaine sur une API. Par exemple, si vous déployez un point de terminaison de cloud privé virtuel (VPC) dans un sous-réseau non routable, votre réseau ne peut pas atteindre API Gateway. Une solution courante consiste à utiliser un nom de domaine personnalisé, puis à déployer l'API dans un sous-réseau routable, mais cela peut perturber d'autres sites internes lorsque la configuration du proxy transmet le trafic (`execute-api.{region}.vpce.amazonaws.com`) à AWS Direct Connect. Enfin, ce modèle peut vous aider à répondre aux exigences organisationnelles relatives à l'utilisation d'une API privée inaccessible depuis Internet et d'un nom de domaine personnalisé.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un certificat SNI (Server Name Indication) pour votre site Web et votre API
- Une connexion depuis un environnement sur site vers un compte AWS configuré à l'aide d'AWS Direct Connect ou d'AWS VPN Site-to-Site
- Une zone hébergée privée avec un domaine correspondant (par exemple, domain.com) qui est résolue à partir d'un réseau local et qui transmet les requêtes DNS à Route 53
- Un sous-réseau privé routable accessible depuis un réseau local

Limites

Pour plus d'informations sur les quotas (anciennement appelés limites) pour les équilibreurs de charge, les règles et les autres ressources, consultez la section Quotas pour vos équilibreurs de charge d'application dans la documentation Elastic Load Balancing.

Architecture

Pile technologique

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS Certificate Manager
- AWS PrivateLink

Architecture cible

Le schéma suivant montre comment un Application Load Balancer est déployé dans un VPC qui dirige le trafic Web vers un groupe cible de sites Web ou un groupe cible d'API Gateway en fonction des règles d'écoute d'Application Load Balancer. Le groupe cible API Gateway est une liste d'adresses IP pour le point de terminaison VPC dans API Gateway. API Gateway est configuré pour rendre l'API privée avec sa politique de ressources. La politique refuse tous les appels qui ne proviennent pas d'un point de terminaison VPC spécifique. Les noms de domaine personnalisés dans API Gateway sont mis à jour pour utiliser api.domain.com pour l'API et sa phase. Les règles Application Load Balancer sont ajoutées pour acheminer le trafic en fonction du nom d'hôte.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur d'un réseau local tente d'accéder à un site Web interne. La demande est envoyée à ui.domain.com et api.domain.com. La demande est ensuite résolue vers l'Application Load Balancer interne du sous-réseau privé routable. Le SSL est résilié au niveau de l'Application Load Balancer pour ui.domain.com et api.domain.com.
2. Les règles du récepteur, configurées sur l'Application Load Balancer, vérifient la présence de l'en-tête de l'hôte.

   a. Si l'en-tête de l'hôte est api.domain.com, la demande est transmise au groupe cible API Gateway. L'Application Load Balancer initie une nouvelle connexion à API Gateway via le port 443.

b. Si l'en-tête de l'hôte est ui.domain.com, la demande est transmise au groupe cible du site Web.

3. Lorsque la demande atteint API Gateway, le mappage de domaine personnalisé configuré dans API Gateway détermine le nom d'hôte et l'API à exécuter.

Automatisation et mise à l'échelle

Les étapes de ce modèle peuvent être automatisées à l'aide d'AWS CloudFormation ou de l'AWS Cloud Development Kit (AWS CDK). Pour configurer le groupe cible des appels d'API Gateway, vous devez utiliser une ressource personnalisée pour récupérer l'adresse IP du point de terminaison du VPC. Appels d'API vers describe-vpc-endpointset describe-network-interfacesrenvoyant les adresses IP et le groupe de sécurité, qui peuvent être utilisés pour créer le groupe cible d'adresses IP de l'API.

Outils

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- Amazon Route 53 est un service Web DNS hautement disponible et évolutif.
- AWS Certificate Manager (ACM) vous aide à créer, stocker et renouveler les certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et applications AWS.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS vous PrivateLink aide à créer des connexions privées unidirectionnelles VPCs à partir de vos services situés en dehors du VPC.

Épopées

Création d'un certificat SNI

Tâche	Description	Compétences requises
Créez un certificat SNI et importez-le dans ACM.	1. Créez un certificat SNI pour ui.domain.com et api.domain.com. Pour plus d'informations, consultez Choisir le mode CloudFront de	Administrateur réseau

Tâche	Description	Compétences requises
	traitement des requêtes HTTPS dans la CloudFront documentation Amazon. 2. Importez les certificats SNI dans AWS Certificate Manager (ACM). Pour plus d'informations, consultez la section Importation de certificats dans AWS Certificate Manager dans la documentation ACM.	

Déployer un point de terminaison VPC dans un sous-réseau privé non routable

Tâche	Description	Compétences requises
Créez un point de terminaison VPC d'interface dans API Gateway.	Pour créer un point de terminaison VPC d'interface, suivez les instructions de la section Accéder à un service AWS à l'aide d'un point de terminaison VPC d'interface dans la documentation Amazon Virtual Private Cloud (Amazon VPC).	Administrateur du cloud

Configuration de l'Application Load Balancer

Tâche	Description	Compétences requises
Créez un groupe cible pour votre application.	Créez un groupe cible pour les ressources d'interface utilisateur de votre application.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez un groupe cible pour le point de terminaison API Gateway.	1. Créez un groupe cible avec un type d'adresse IP, puis ajoutez l'adresse IP du point de terminaison VPC du point de terminaison API Gateway au groupe cible. 2. Configurez les contrôles de santé pour vos groupes cibles avec le code de réussite 403. 403 est obligatoire car le point de terminaison VPC pour l'API Gateway renvoie un code 403 lorsqu'il est invoqué sans aucun en-tête par le contrôle de santé du groupe cible.	Administrateur du cloud
Créez un Application Load Balancer.	1. Créez un Application Load Balancer (interne) dans un sous-réseau privé routable. 2. Ajoutez l'écouteur 443 à l'Application Load Balancer, puis choisissez le certificat auprès d'ACM.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez des règles pour les auditeurs.	Créez des règles d'écoute pour effectuer les opérations suivantes : 1. Transférer l'hôte api.domain.com vers le groupe cible API Gateway 2. Transférez l'hôte ui.domain.com au groupe cible pour les ressources de l'interface utilisateur	Administrateur du cloud

Configuration de la Route 53

Tâche	Description	Compétences requises
Créez une zone hébergée privée.	Créez une zone hébergée privée pour domain.com.	Administrateur du cloud
Créez des enregistrements de domaine.	Créez des enregistrements CNAME pour les éléments suivants : • Une API dont la valeur est définie sur le nom DNS de l'Application Load Balancer • Une interface utilisateur dont la valeur est définie sur le nom DNS de l'Application Load Balancer	Administrateur du cloud

Création d'un point de terminaison d'API privé dans API Gateway

Tâche	Description	Compétences requises
Créez et configurez un point de terminaison d'API privé.	1. Pour créer un point de terminaison d'API privé, suivez les instructions de la section Création d'une API privée dans Amazon API Gateway dans la documentation d'API Gateway. 2. Configurez la politique de ressources pour autoriser uniquement les appels à l'API depuis le point de terminaison du VPC. Pour plus d'informations, consultez la section Contrôle de l'accès à une API à l'aide des politiques de ressources d'API Gateway dans la documentation d'API Gateway.	Développeur d'applications, administrateur cloud
Créez un nom de domaine personnalisé.	1. Créez un nom de domaine personnalisé pour api.domain.com. Pour plus d'informations, consultez la section Configuration de noms de domaine personnalisés pour REST APIs dans la documentation d'API Gateway. 2. Sélectionnez l'API et le stage créés. Pour plus	Administrateur du cloud

Tâche	Description	Compétences requises
	d'informations, consultez la section Utilisation des mappages d'API pour REST APIs dans la documentation d'API Gateway.	

Ressources connexes

- Amazon API Gateway
- Amazon Route 53
- Application Load Balancer
- AWS PrivateLink
- AWS Certificate Manager

Intégrer un tableau de QuickSight bord Amazon dans une application Angular locale

Créée par Sean Griffin (AWS) et Milena Godau (AWS)

Récapitulatif

Ce modèle fournit des conseils pour intégrer un tableau de QuickSight bord Amazon dans une application Angular hébergée localement à des fins de développement ou de test. La fonctionnalité d'analyse intégrée QuickSight ne prend pas en charge cette fonctionnalité de manière native. Cela nécessite un QuickSight compte avec un tableau de bord existant et une connaissance d'Angular.

Lorsque vous travaillez avec des QuickSight tableaux de bord intégrés, vous devez généralement héberger votre application sur un serveur Web pour afficher le tableau de bord. Cela complique le développement, car vous devez continuellement transférer vos modifications sur le serveur Web pour vous assurer que tout fonctionne correctement. Ce modèle montre comment exécuter un serveur hébergé localement et utiliser des outils d'analyse QuickSight intégrés pour simplifier et rationaliser le processus de développement.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- Un QuickSight compte actif avec tarification de la capacité de session
- QuickSight SDK d'intégration installé
- CLI angulaire installée
- Connaissance d'Angular
- mkcert installé

Limites

- Ce modèle fournit des conseils sur l'intégration d'un QuickSight tableau de bord à l'aide du type d'authentification `ANONYMOUS` (accessible au public). Si vous utilisez AWS Identity and Access Management (IAM) ou QuickSight l'authentification avec vos tableaux de bord intégrés, le code fourni ne s'applique pas. Cependant, les étapes d'hébergement de l'application Angular dans la section Epics sont toujours valides.

- L'utilisation de l'GetDashboardEmbedUrlAPI avec le type `ANONYMOUS` d'identité nécessite un plan QuickSight de tarification des capacités.

Versions

- CLI angulaire version 13.3.4
- QuickSight Intégration de la version 2.3.1 du SDK

Architecture

Pile technologique

- Frontend angulaire
- Backend AWS Lambda et Amazon API Gateway

Architecture

Dans cette architecture, le protocole HTTP APIs in API Gateway permet à l'application Angular locale d'appeler la fonction Lambda. La fonction Lambda renvoie l'URL d'intégration du tableau de bord. QuickSight

Automatisation et mise à l'échelle

Vous pouvez automatiser le déploiement du backend en utilisant AWS CloudFormation ou AWS Serverless Application Model (AWS Serverless Application Model) (AWS SAM).

Outils

Outils

- Angular CLI est un outil d'interface de ligne de commande que vous utilisez pour initialiser, développer, échafauder et gérer des applications Angular directement à partir d'un shell de commande.
- QuickSight Le SDK d'intégration est utilisé pour intégrer des QuickSight tableaux de bord dans votre code HTML.

- mkcert est un outil simple pour créer des certificats de développement fiables localement. Il ne nécessite aucune configuration. mkcert est requis car seules les requêtes HTTPS sont autorisées pour QuickSight intégrer des tableaux de bord.

Services AWS

- Amazon API Gateway est un service AWS permettant de créer, de publier, de gérer, de surveiller et de sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- Amazon QuickSight est un service d'analyse commerciale permettant de créer des visualisations, d'effectuer des analyses ad hoc et d'obtenir des informations commerciales à partir de vos données.

Épopées

Générer une URL incorporée

Tâche	Description	Compétences requises
Créez une EmbedUrl politique.	Créez une stratégie IAM nommée QuicksightGetDashboardEmbedUrlqui possède les propriétés suivantes. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [`	Administrateur AWS

Tâche	Description	Compétences requises

	<pre>"quicksight:GetDashboardEmbedUrl",
	
	"quickSight:GetAnonymousUserEmbedUrl"
	],
	
	"Resource": "*"
	}
	]
	}</pre>	

Tâche	Description	Compétences requises

Créez la fonction Lambda.	1. Sur la console Lambda, ouvrez la page Fonctions.
	
	2. Choisissez Créer une fonction.
	
	3. Choisissez Créer à partir de zéro.
	
	4. Sous Nom de la fonction, saisissez `get-qs-embed-url`.
	
	5. Pour Runtime (Environn ement d'exécution), choisissez Python 3.9.
	
	6. Choisissez Créer une fonction.
	
	7. Dans l'onglet Code, copiez le code suivant dans la fonction Lambda.
	
	`import json`
	`import boto3`
	`from botocore.`
	`exceptions import`
	`ClientError`
	`import time`
	`from os import environ`
	
	`qs = boto3.client('quic`
	`ksight',region_nam`
	`e='us-east-1')`
	`sts = boto3.cli`
	`ent('sts')`
		Développeur d’applications

Tâche	Description	Compétences requises

	ACCOUNT_ID = boto3.client('sts').get_caller_identity().get('Account')
	DASHBOARD_ID = environ['DASHBOARD_ID']
	
	def getDashboardURL(accountId, dashboardId, quicksightNamespace, resetDisabled, undoRedoDisabled):
	  try:
	  response = qs.get_dashboard_embed_url(
	  AwsAccountId = accountId,
	  DashboardId = dashboardId,
	  Namespace = quicksightNamespace,
	  IdentityType = 'ANONYMOUS',
	  SessionLifetimeInMinutes = 600,
	  UndoRedoDisabled = undoRedoDisabled,
	  ResetDisabled = resetDisabled
	  )
	  return response
	
	  except ClientError as e:
	  print(e)
	  return "Error generating embeddedURL: " + str(e)	

Tâche	Description	Compétences requises

	``
	def lambda_handler(eve
	nt, context):
	  url = getDashbo
	ardURL(ACCOUNT_ID,
	 DASHBOARD_ID,
	 "default", True, True)
	['EmbedUrl']
	  return {
	  'statusCode':
	 200,
	  'url': url
	  }
	``
	
	8. Choisissez Déployer.	

Tâche	Description	Compétences requises
Ajoutez l'ID du tableau de bord en tant que variable d'environnement.	Ajoutez `DASHBOARD_ID` en tant que variable d'environnement à votre fonction Lambda : 1. Dans l'onglet Configuration, choisissez Variables d'environnement, Modifier, Ajouter une variable d'environnement. 2. Ajoutez une variable d'environnement à l'aide de la clé `DASHBOARD_ID`. 3. Pour obtenir la valeur de `DASHBOARD_ID`, accédez à votre tableau de bord QuickSight et copiez l'UUID à la fin de l'URL dans votre navigateur. Par exemple, si l'URL est `https://us-east-1.quicksight.aws.amazon.com/sn/dashboards/<dashboard-id>`, spécifiez la `<dashboard-id>` partie de l'URL comme valeur clé. 4. Choisissez Enregistrer.	Développeur d'applications

Tâche	Description	Compétences requises
Ajoutez des autorisations pour la fonction Lambda.	Modifiez le rôle d'exécution de la fonction Lambda et ajoutez-y la QuicksightGetDashboardEmbedUrlpolitique. 1. Dans l'onglet Configuration, sélectionnez Autorisations, puis choisissez le nom du rôle. 2. Choisissez Joindre des politiques, recherche `zQuicksightGetDashboardEmbedUrl` , cochez la case correspondante, puis choisissez Joindre une politique.	Développeur d’applications

Tâche	Description	Compétences requises
Testez la fonction Lambda.	Créez et exécutez un événement de test. Vous pouvez utiliser le modèle « Hello World », car la fonction n'utilisera aucune des données de l'événement de test. 1. Choisissez l'onglet Test. 2. Donnez un nom à votre événement de test, puis choisissez Enregistrer. 3. Pour tester votre fonction Lambda, choisissez Test. La réponse devrait être similaire à ce qui suit. `{ "statusCode": 200, "url": "\"https://us-east-1.quicksight.aws.amazon.com/embed/f1acc0786687783b9a4543a05ba929b3a/dashboards/... }` **Note** Comme indiqué dans la section Conditions préalables et limites, votre QuickSigh t compte doit être soumis à un plan	Développeur d'applications

Tâche	Description	Compétences requises
	tarifaire relatif à la capacité de session. Dans le cas contraire , cette étape affichera un message d'erreur.	

Tâche	Description	Compétences requises
Créez une API dans API Gateway.	1. Sur la console API Gateway, choisissez Create API, puis choisissez REST API, Build. • Pour le nom de l'API, entrez`qs-embed-api` . • Sélectionnez Create API (Créer une API). 2. Dans Actions, choisissez Create Method. • Choisissez GET et confirmez en cochant la case. • Choisissez Lambda Function comme type d'intégration. • Pour Lambda Function, entrez. `get-qs-embed-url` • Choisissez Enregistrer. • Dans la zone Ajouter une autorisation à la fonction Lambda, cliquez sur OK. 3. Activez CORS. • Dans Actions, sélectionnez Activer CORS. • Pour Access-Control-Allow-Origin, entrez. `'https://my-qs-app.net:4200'` • Choisissez Activer le CORS, remplacez les en-	Développeur d'applications

Tâche	Description	Compétences requises
	têtes CORS existants, puis confirmez. 4. Déployez l'API. • Pour Actions, choisissez Deploy API. • Dans Deployment stage (Étape de déploiement), sélectionnez [New Stage] [Nouvelle étape]. • Sous Stage name (Nom de l'étape), entrez `dev`. • Choisissez Deploy (Déployer). • Copiez l'URL Invoke. **Note** `my-qs-app.net` peut être n'importe quel domaine. Si vous souhaitez utiliser un autre nom de domaine, veillez à mettre à jour les informations Access-Control-Allow-Origin à l'étape 3 et à les modifier lors des étapes suivantes. `my-qs-app.net`	

Création de l'application Angular

Tâche	Description	Compétences requises

Créez l'application avec la CLI angulaire.	1. Créez l'application.
	`ng new quicksight-app --defaults`
	`cd quicksight-app/src/app`
	2. Créez le composant du tableau de bord.
	`ng g c dashboard`
	3. Accédez à votre `src/environments/environment.ts` fichier et ajoutez-le `apiUrl: '<Invoke URL from previous steps>'` à l'objet d'environnement.
	`export const environment = { production: false, apiUrl: '<Invoke URL from previous steps>', };`
		Développeur d’applications

Ajoutez le SDK QuickSight d'intégration.	1. Installez le SDK QuickSight d'intégration en exécutant la commande suivante dans le dossier racine de votre projet.	Développeur d’applications

Tâche	Description	Compétences requises
	``` npm i amazon-qu icksight-embedding- sdk ``` 2. Créez un nouveau `decl.d.ts` fichier dans le `src` dossier avec le contenu suivant. ``` declare module 'amazon-quicksight- embedding-sdk'; ```	

Tâche	Description	Compétences requises

Ajoutez du code à votre fichier dashboard.component.ts.	`import { Component, OnInit } from '@angular/core';`
	`import { HttpClient } from '@angular/common/http';`
	`import * as QuicksightEmbedding from 'amazon-quicksight-embedding-sdk';`
	`import { environment } from "../../environments/environment";`
	`import { take } from 'rxjs';`
	`import { EmbeddingContext } from 'amazon-quicksight-embedding-sdk/dist/types';`
	`import { createEmbeddingContext } from 'amazon-quicksight-embedding-sdk';`
	
	`@Component({`
	`  selector: 'app-dashboard',`
	`  templateUrl: './dashboard.component.html',`
	`  styleUrls: ['./dashboard.component.scss']`
	`})`
	`export class DashboardComponent implements OnInit {`
	
	`  constructor(private http: HttpClient) { }`
		Développeur d'applications

Tâche	Description	Compétences requises

	`  loadingError = false;`
	`  dashboard: any;`
	
	`  ngOnInit() {`
	`  this.GetDashboardU`
	`RL();`
	`  }`
	
	`  public GetDashbo`
	`ardURL() {`
	`  this.http.get(envi`
	`ronment.apiUrl)`
	`  .pipe(`
	`  take(1),`
	`  )`
	`  .subscribe((data:`
	` any) => this.Dash`
	`board(data.url));`
	`  }`
	
	`  public async Dashboard`
	`(embeddedURL: any) {`
	`  var containerDiv`
	` = document.getElemen`
	`tById("dashboardCo`
	`ntainer") || '';`
	`  const frameOptions`
	` = {`
	`  url: embeddedURL,`
	`  container:`
	` containerDiv,`
	`  height: "850px",`
	`  width: "100%",`
	`  resizeHei`
	`ghtOnSizeChangedEv`
	`ent: true,`
	`  }`
	`  const embedding`
	`Context: Embedding`
	`Context = await`
	` createEmbeddingCon`
	`text();`	

Tâche	Description	Compétences requises

	`this.dashboard = embeddingContext.embedDashboard(frameOptions);`
	`}`
	`}`	

Ajoutez du code à votre fichier dashboard.component.html.	Ajoutez le code suivant à votre `src/app/dashboard/dashboard.component.html` fichier. `<div id="dashboardContainer"></div>`	Développeur d'applications
Modifiez votre fichier app.component.html pour charger le composant de votre tableau de bord.	1. Supprimez le contenu du `src/app/app.component.html` fichier. 2. Ajoutez ce qui suit. `<app-dashboard></app-dashboard>`	Développeur d'applications
Importez HttpClientModule dans votre fichier app.module.ts.	1. En haut du `src/app/app.module.ts` fichier, ajoutez ce qui suit. `import { HttpClientModule } from '@angular/common/http';` 2. Ajoutez `HttpClientModule` le **`imports`**tableau correspondant à votre`AppModule` .	Développeur d'applications

Héberger l'application Angular

Tâche	Description	Compétences requises

Configurez mkcert.	**Note**
	Les commandes suivantes sont destinées aux machines Unix ou macOS. Si vous utilisez Windows, consultez la section Informations supplémentaires pour la commande echo équivalente.
	
	1. Créez une autorité de certification (CA) locale sur votre machine.
	`mkcert -install`
	2. Configurez `my-qs-app.net` pour toujours être redirigé vers votre PC local.
	`echo "127.0.0.1 my-qs-app.net" | sudo tee -a /private/etc/hosts`
	3. Assurez-vous que vous êtes dans le `src` répertoire du projet Angular.
		Développeur d’applications

Tâche	Description	Compétences requises
	`mkcert my-qs-app.net 127.0.0.1`	
Configurez QuickSight pour autoriser votre domaine.	1. Dans QuickSight, choisissez votre nom dans le coin supérieur droit, puis choisissez Gérer Quicksight. 2. Accédez à Domaines et intégration. 3. Ajouter `https://my-qs-app.net:4200` en tant que domaine autorisé.	Administrateur AWS

Tâche	Description	Compétences requises
Testez la solution.	Démarrez un serveur de développement Angular local en exécutant la commande suivante. `ng serve --host my-qs-app.net --port 4200 --ssl --ssl-key "./src/my-qs-app.net-key.pem" --ssl-cert "./src/my-qs-app.net.pem" -o` Cela active le protocole SSL (Secure Sockets Layer) avec le certificat personnalisé que vous avez créé précédemment. Lorsque la construction est terminée, une fenêtre de navigateur s'ouvre et vous pouvez consulter votre tableau de QuickSight bord intégré hébergé localement dans Angular.	Développeur d'applications

Ressources connexes

- Site Web angulaire
- Intégration de tableaux de bord de QuickSight données pour les utilisateurs anonymes (non enregistrés) (documentation) QuickSight
- QuickSight SDK d'intégration
- outil mkcert

Informations supplémentaires

Si vous utilisez Windows, exécutez la fenêtre d'invite de commande en tant qu'administrateur et configurez `my-qs-app.net` pour toujours être redirigé vers votre PC local à l'aide de la commande suivante.

```
echo 127.0.0.1 my-qs-app.net >> %WINDIR%\System32\Drivers\Etc\Hosts
```

Découvrez le développement complet d'applications Web natives pour le cloud avec Green Boost

Créée par Ben Stickley (AWS) et Amiin Samatar (AWS)

Récapitulatif

En réponse à l'évolution des besoins des développeurs, Amazon Web Services (AWS) reconnaît la nécessité d'adopter une approche efficace du développement d'applications Web natives pour le cloud. L'objectif d'AWS est de vous aider à surmonter les obstacles courants associés au déploiement d'applications Web sur le cloud AWS. En exploitant les capacités des technologies modernes telles qu' TypeScriptAWS Cloud Development Kit (AWS CDK), React et Node.js, ce modèle vise à rationaliser et à accélérer le processus de développement.

S'appuyant sur le kit d'outils Green Boost (GB), le modèle propose un guide pratique pour créer des applications Web qui utilisent pleinement les fonctionnalités étendues d'AWS. Il constitue une feuille de route complète qui vous guide tout au long du processus de déploiement d'une application Web CRUD (Create, Read, Update, Delete) fondamentale intégrée à Amazon Aurora PostgreSQL Compatible Edition. Ceci est réalisé en utilisant l'interface de ligne de commande Green Boost (CLI Green Boost) et en établissant un environnement de développement local.

Après le déploiement réussi de l'application, le modèle explore les composants clés de l'application Web, notamment la conception de l'infrastructure, le développement du backend et du frontend, ainsi que les outils essentiels tels que cdk-dia pour la visualisation, facilitant ainsi une gestion de projet efficace.

Conditions préalables et limitations

Prérequis

- Git installé
- Visual Studio Code (VS Code) installé
- Interface de ligne de commande (AWS CLI) (AWS CLI) installée
- AWS CDK Toolkit installé
- Node.js 18 installé, ou Node.js 18 avec pnpm activé
- pnpm installé, s'il ne fait pas partie de votre installation de Node.js
- Connaissance de base d'AWS CDK TypeScript, de Node.js et de React

- Un compte AWS actif
- Un compte AWS a démarré à l'aide d'AWS CDK dans. `us-east-1` La région `us-east-1` AWS est requise pour le support des fonctions Amazon CloudFront Lambda @Edge.
- Informations d'identification de sécurité AWS`AWS_ACCESS_KEY_ID`, y compris celles correctement configurées dans votre environnement de terminal
- Pour les utilisateurs de Windows, un terminal en mode administrateur (pour s'adapter à la façon dont pnpm gère les modules de nœuds)

Versions du produit

- SDK AWS pour JavaScript version 3
- AWS CDK version 2
- Version 2.2 de l'interface de ligne de commande AWS
- Version 18 de Node.js
- Version 18 de React

Architecture

Pile technologique cible

- Amazon Aurora PostgreSQL-Compatible Edition
- Amazon CloudFront
- Amazon CloudWatch
- Amazon Elastic Compute Cloud (Amazon EC2)
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS WAF

Architecture cible

Le schéma suivant montre que les demandes des utilisateurs passent par Amazon CloudFront, AWS WAF et AWS Lambda avant d'interagir avec un compartiment S3, une base de données Aurora, EC2

une instance et d'atteindre finalement les développeurs. Les administrateurs, quant à eux, utilisent Amazon SNS et Amazon à des CloudWatch fins de notification et de surveillance.

Pour obtenir un aperçu plus approfondi de l'application après le déploiement, vous pouvez créer un diagramme à l'aide de cdk-dia, comme indiqué dans l'exemple suivant.

Ces diagrammes présentent l'architecture de l'application Web sous deux angles distincts. Le diagramme cdk-dia offre une vue technique détaillée de l'infrastructure AWS CDK, en mettant en évidence des services AWS spécifiques tels que la compatibilité avec Amazon Aurora PostgreSQL et AWS Lambda. En revanche, l'autre diagramme adopte une perspective plus large, mettant l'accent sur le flux logique des données et les interactions avec les utilisateurs. La principale différence réside dans le niveau de détail : le cdk-dia explore les subtilités techniques, tandis que le premier schéma fournit une vue plus centrée sur l'utilisateur.

La création du diagramme cdk-dia est abordée dans le livre épique Comprendre l'infrastructure des applications à l'aide d'AWS CDK.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon CloudFront accélère la diffusion de votre contenu Web en le diffusant via un réseau mondial de centres de données, ce qui réduit le temps de latence et améliore les performances.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.

- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- AWS Systems Manager vous aide à gérer vos applications et votre infrastructure exécutées dans le cloud AWS. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos ressources AWS en toute sécurité à grande échelle. Ce modèle utilise le gestionnaire de session AWS Systems Manager.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données. Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les demandes HTTP et HTTPS qui sont transférées vers les ressources protégées de votre application Web

Autres outils

- Git est un système de contrôle de version distribué et open source.
- Green Boost est une boîte à outils permettant de créer des applications Web sur AWS.
- Next.js est un framework React permettant d'ajouter des fonctionnalités et des optimisations.
- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.
- pnpm est un gestionnaire de paquets pour les dépendances du projet Node.js.

Bonnes pratiques

Consultez la section Epics pour plus d'informations sur les recommandations suivantes :

- Surveillez l'infrastructure à l'aide des CloudWatch tableaux de bord et des alarmes Amazon.

- Appliquez les meilleures pratiques d'AWS en utilisant cdk-nag pour exécuter une analyse statique de l'infrastructure sous forme de code (IaC).
- Établissez la redirection de port de base de données via le tunneling SSH (Secure Shell) avec le gestionnaire de session Systems Manager, qui est plus sécurisé que le fait d'avoir une adresse IP exposée publiquement.
- Gérez les vulnérabilités en exécutant`pnpm audit`.
- Appliquez les meilleures pratiques en utilisant ESLintpour effectuer une analyse de TypeScript code statique et Prettier pour standardiser le formatage du code.

Épopées

Déployer une application Web CRUD compatible avec Aurora PostgreSQL

Tâche	Description	Compétences requises
Installez la CLI Green Boost.	Pour installer Green Boost CLI, exécutez la commande suivante. `pnpm add -g gboost`	Développeur d’applications
Créez une application GB.	1. Pour créer une application à l'aide de Green Boost, exécutez la commande`gboost create`. 2. Choisissez le modèle `CRUD App with Aurora PostgreSQL` .	Développeur d’applications
Installez les dépendances et déployez l'application.	1. Accédez au répertoire du projet :`cd <your directory>` . 2. Pour installer les dépendances, exécutez la commande`pnpm i`.	Développeur d’applications

Tâche	Description	Compétences requises
	3. Accédez au répertoire infra :`cd infra`. 4. Pour déployer l'application localement, exécutez la commande`pnpm deploy:local` . Il s'agit d'un alias pour une `cdk deploy ...` commande définie dans`infra/package.json` . Attendez la fin du déploiement (environ 20 minutes). Pendant que vous attendez, surveillez les CloudFormation piles AWS dans la CloudFormation console. Remarquez comment les constructions définies dans le code correspondent à la ressource déployée. Passez en revue l'arborescence de CDK Construct dans la CloudFormation console.	

Tâche	Description	Compétences requises
Accédez à l'application.	Après avoir déployé votre application GB localement, vous pouvez y accéder à l'aide de l' CloudFront URL. L'URL est imprimée dans la sortie du terminal, mais elle peut être un peu difficile à trouver. Pour le trouver plus rapidement, procédez comme suit : 1. Ouvrez le terminal sur lequel vous avez exécuté la `pnpm deploy:local` commande. 2. Recherchez une section dans la sortie du terminal qui ressemble au texte suivant. `myapp5stickbui9C39A55A.CloudFrontDomainName = d1q16n5pof924c.cloudfront.net` L'URL sera propre à votre déploiement. Vous pouvez également trouver l' CloudFront URL en accédant à la CloudFront console Amazon : 1. Connectez-vous à l'AWS Management Console et	Développeur d’applications

Tâche	Description	Compétences requises
	accédez au CloudFront service. 2. Recherchez la dernière distribution déployée dans la liste. Copiez le nom de domaine associé à la distribution. Cela ressemblera à`your-unique-id.cloudfront.net` .	

Surveillez en utilisant Amazon CloudWatch

Tâche	Description	Compétences requises
Consultez le CloudWatch tableau de bord.	1. Ouvrez la CloudWatch console et choisissez Dashboards. 2. Sélectionnez le tableau de bord qui porte le nom - -dashboard <appId><stageName>. 3. Consultez le tableau de bord. Quelles sont les ressources surveillées ? Quels indicateurs sont enregistrés ? Ce tableau de bord est rendu possible grâce à la construction cdk-monitoring-constructsopen source.	Développeur d’applications

Tâche	Description	Compétences requises

Activez les alertes.	Un CloudWatch tableau de bord vous permet de surveille r activement votre applicati on Web. Pour surveiller passivement votre application Web, vous pouvez activer les alertes.
	1. Accédez à`/infra/src/app/stateless/mo nitor-stack.ts` , qui définit la pile de moniteurs.
	2. Décommentez la ligne suivante et remplacez-la `admin@example.com` par votre adresse e-mail.
	`onAlarmTopic.addSu bscription(new EmailSubscription( "admin@example.com "));`
	3. Ajoutez les informations d'importation suivantes en haut du fichier.
	`import { EmailSubs cription } from "aws-cdk-lib/aws-sns-subscriptions";`
	4. À l'intérieur`infra/`, exécutez la commande suivante.
		Développeur d’applications

Tâche	Description	Compétences requises
	`cdk deploy "*/monitor" --exclusively.` 5. Pour confirmer votre abonnement à la rubrique SNS qui s'affiche lorsqu'une alarme de surveillance est déclenchée, cliquez sur le lien contenu dans le message électronique.	

Découvrez l'infrastructure des applications à l'aide d'AWS CDK

Tâche	Description	Compétences requises
Créez un schéma d'architecture.	Générez un schéma d'architecture de votre application Web à l'aide de cdk-dia. La visualisation de l'architecture permet d'améliorer la compréhension et la communication entre les membres de l'équipe. Il fournit une vue d'ensemble claire des composants du système et de leurs relations. 1. Installez Graphviz. 2. À l'intérieur`infra/`, exécutez la commande`pnpm cdk-dia`. 3. Consultez votre`infra/diagram.png` .	Développeur d’applications

Tâche	Description	Compétences requises
Utilisez cdk-nag pour appliquer les meilleures pratiques.	Utilisez cdk-nag pour vous aider à maintenir une infrastructure sécurisée et conforme en appliquant les meilleures pratiques, en réduisant le risque de vulnérabilités de sécurité et de mauvaises configurations. 1. Découvrez l'application des meilleures pratiques de cdk-nag dans sa section sur les règles, y compris les vérifications issues du pack de règles de la bibliothèque de solutions AWS. 2. Pour voir comment cdk-nag applique les règles, modifiez le code. Par exemple, dans `infra/src/app/stateful/data-stacks.ts` , remplacez `storageEncrypted: true` par `storageEncrypted: false` . 3. À l'intérieur `infra/`, exécutez la commande `cdk synth "*/data"`. Au cours de la synthèse, vous rencontrerez une erreur de compilation indiquant une violation des règles. `AwsSolutions-RDS2: The RDS instance or`	Développeur d’applications

Tâche	Description	Compétences requises

	`Aurora DB cluster does not have storage encryption enabled.`
	
	Cette erreur montre en quoi cdk-nag est un mécanisme de sécurité destiné à appliquer les meilleure s pratiques en matière d'infrastructure et à prévenir les erreurs de configuration en matière de sécurité.
	4. Si nécessaire, vous pouvez également supprimer des règles de différentes étendues. Par exemple, pour supprimer AwsSoluti ons -RDS2, ajoutez le code suivant sous l'instanciation de. `DbIamCluster`
	
	`NagSuppressions.ad dResourceSuppressi ons( cluster.node.findC hild("Resource"), [ { id: "AwsSolut ions-RDS2", reason: "Customer requireme nt necessitates having unencrypted DB storage", }, ],`	

Tâche	Description	Compétences requises
	```); ``` 5. Après la suppression, exécutez `cdk synth "*/data"` à nouveau. Votre application AWS CDK devrait maintenant être synthétisée correctement. Vous trouverez toutes les règles supprimées dans`infra/cdk.out/assembly-<appId>-<stageName>/AwsSolutions-<appId>-<stageName>-${stackId}-NagReport.csv` .	

Évaluer la configuration et le schéma de la base de données

Tâche	Description	Compétences requises
Acquérir des variables d'environnement.	Pour obtenir les variables d'environnement requises, procédez comme suit : 1. Pour les trouver`DB_BASTION_ID` , connectez-vous à la console, puis naviguez jusqu'à la EC2 console. Choisissez Instances (en cours d'exécution), puis recherchez la ligne contenant - ssm-db-bastion	Développeur d’applications

Tâche	Description	Compétences requises
	Nom<stageName>. L'ID d'instance commence par i-. 2. Pour les trouverDB_ENDPOINT , sur la console Amazon Relational Database Service (Amazon RDS), choisissez DB Instances , puis sélectionnez le cluster régional dont l'identifiant de base de données commence par - -data <appId><stageName> -. Localisez le point de terminaison de l'instance Writer, qui se termine par rds.amazonaws.com.	

Tâche	Description	Compétences requises
Établissez la redirection de port.	Pour établir la redirection de port, procédez comme suit : 1. Installez le plugin AWS Systems Manager Session Manager. 2. Démarrez la redirection de port en `pnpm db:connect` exécutant `core/` l'utilitaire pour établir une connexion sécurisée via l'hôte Bastion. 3. Après avoir vu le texte `Waiting for connections...,` dans votre terminal, un tunnel SSH a été établi avec succès entre votre machine locale et le serveur Aurora via l'hôte EC2 bastion.	Développeur d’applications
Ajustez le délai d'expiration du gestionnaire de sessions de Systems Manager.	(Facultatif) Si le délai d'expiration de session par défaut de 20 minutes est trop court, vous pouvez l'augmenter jusqu'à 60 minutes dans la console Systems Manager en choisissant Session Manager, Preferences, Edit, Idle session timeout.	Développeur d’applications

Tâche	Description	Compétences requises
Visualisez la base de données.	pgAdmin est un outil open source convivial pour gérer les bases de données PostgreSQL. Il simplifie les tâches de base de données, vous permettant de créer, de gérer et d'optimiser efficacement les bases de données. Cette section explique comment installer pgAdmin et comment utiliser ses fonctionnalités pour la gestion des bases de données PostgreSQL. 1. Dans l'explorateur d'objets, ouvrez le menu contextuel (clic droit) pour Servers, puis choisissez Register, Server. 2. Dans l'onglet Général, entrez - <appId>dans <stageName>le champ Nom. 3. Pour récupérer le mot de passe de la base de données, ouvrez la console AWS Secrets Manager, sélectionnez le secret dont la description est Generated by the CDK for the stack : --data <appId><stageName>, puis choisissez la carte Secret Value. Choisissez Retrieve Secret Value, puis	Développeur d’applications

Tâche	Description	Compétences requises
	copiez la valeur secrète avec une clé ou un mot de passe. 4. Dans l'onglet Connexion, entrez 0.0.0 pour le champ nom/adresse de l'hôte, et entrez _admin pour le champ Nom d'utilisateur. <appId> Pour le champ Mot de passe, utilisez le code secret que vous avez récupéré précédemment. Choisissez « Oui » pour le champ Enregistrer le mot de passe ? champ. 5. Choisissez Enregistrer. 6. Pour afficher les tables, accédez à -, Databases , _db, Schemas, Tables. <appId><stageName> <appId><appId> 7. Ouvrez le menu contextue l (clic droit) du tableau des éléments, puis sélection nez Afficher/Modifier les données, toutes les lignes. 8. Explorez le tableau.	

Déboguer avec Node.js

Tâche	Description	Compétences requises

Déboguez le cas d'utilisation de la fonction Create Item.	Pour déboguer le cas d'utilisation lié à la création d'un élément, procédez comme suit :
	
	1. Ouvrez le `core/src/modules/item/create-item.use-case.ts` fichier et insérez le code suivant.
	
	``
	import { fileURLToPath } from "node:url";
	
	// existing create-item.use-case.ts code here
	
	if (process.argv[1] === fileURLToPath(import.meta.url)) {
	  createItemUseCase({
	    description: "Item 1's Description",
	    name: "Item 1",
	  });
	}
	``
	
	2. Le code ajouté à l'étape précédente garantit que la `createItemUseCase` fonction sera appelée lorsque ce module sera
		Développeur d’applications

Tâche	Description	Compétences requises
	exécuté directement. Définissez des points d'arrêt sur les lignes de ce bloc de code où vous souhaitez lancer le line-by-line débogage. 1. Ouvrez le terminal de JavaScript débogage VS Code, puis exécutez `pnpm tsx core/src/modules/item/create-item.use-case.ts` pour exécuter le code avec le line-by-line débogage. Vous pouvez également utiliser `console.log` des instructions, mais les instructions imprimées peuvent s'avérer inadéquates lorsque vous travaillez avec une logique métier complexe. Line-by-linele débogage vous donne plus de contexte.	

Développez le frontend

Tâche	Description	Compétences requises
Configurez le serveur de développement.	1. Accédez au `ui/` serveur de développement Next.js et	Développeur d’applications

Tâche	Description	Compétences requises
	exécutez-le `pnpm dev` pour le démarrer. 2. Accédez à votre application Web localement à l'adresse `http://localhost:3000` . Le serveur de développement Next.js est configuré avec un retour instantané Fast Refresh sur les modifications apportées à vos composants React. 3. Essayez de personnaliser la couleur de la barre de l'application. Ouvrez le `ui/src/components/theme/theme.tsx` fichier et recherchez la section qui définit le thème de la barre d'applications. Dans la `colorSchemes.light.palette.primary` section, mettez à jour la valeur principale de `colors.lagoon` à `colors.carrot` . Après avoir effectué cette modification, enregistrez le fichier et observez la mise à jour dans votre navigateur. 4. Faites des essais en modifiant le texte, les composants et en ajoutant de nouvelles pages.	

Outillage avec Green Boost

Tâche	Description	Compétences requises
Configurez monorepo et le gestionnaire de paquets pnpm.	1. Consultez `pnpm-workspace.yaml` la racine de votre référentiel de Go et remarquez comment les espaces de travail sont définis. Pour plus d'informations sur les espaces de travail, consultez la documentation pnpm. 2. Vérifiez `ui/package.json` et remarquez comment il fait référence à l'espace de travail `core/` avec le nom du package `"<appId>/core": "workspace:^",` . 3. Observez comment TypeScript la ESLint configuration est centralisée dans les packages utilitaires définis dans ce document`packages/` . Cette configuration est ensuite utilisée par les packages d'applications tels que `core/infra/`, et`ui/`. Cela est utile lorsque votre application évolue et que vous définissez d'autres packages d'applications, qui peuvent faire référence aux packages utilitaires	Développeur d’applications

Tâche	Description	Compétences requises
	sans dupliquer le code de configuration.	
Exécutez des scripts pnpm.	Exécutez les commandes suivantes à la racine de votre dépôt : 1. Exécutez `pnpm lint`. Cette commande exécute une analyse de code statique avec ESLint. 2. Exécutez `pnpm typecheck .` Cette commande exécute le TypeScript compilateur pour vérifier les types de votre code. 3. Exécutez `pnpm test`. Cette commande exécute Vitest pour exécuter des tests unitaires. Remarquez comment ces commandes sont exécutées dans tous les espaces de travail. Les commandes sont définies dans le `package.json#scripts` champ de chaque espace de travail.	Développeur d'applications

Tâche	Description	Compétences requises

À utiliser ESLint pour l'analyse de code statique.	Pour tester la capacité d'analyse de code statique de ESLint, procédez comme suit :
	
	1. Tout d'abord, assurez-vous que l' ESLint extension VS Code (ID :`dbaeumer.vscode-eslint`) est installée. Nous vous recommandons également d'installer VS Code Error Lens (ID :`usernamehw.errorlens`) pour voir les erreurs en ligne.
	2. Dans votre code, incluez délibérément une ligne de code qui utilise la `eval()` fonction, comme illustré dans l'exemple suivant.
	
	``
	const userInput = "import("fs").then((fs) => console.log(fs.readFileSync("/etc/passwd", { encoding: "utf8" })))";
	eval(userInput);
	``
	
	Important
	Ceci est uniquement à des fins de test. L'utilisation `eval()` est considérée comme potentiel
		Développeur d'applications

Tâche	Description	Compétences requises
	lement dangereus e et doit être évitée en raison des risques de sécurité. 3. Après avoir inclus la `eval()` ligne, ouvrez votre éditeur de code pour confirmer que l'odeur du code est ESLint indiquée en utilisant des gribouillis rouges. 4. Consultez ESLint les plugins et leur configura tion à l'adresse`packages/eslint-config-{node,next}/.eslintrc.cjs` .	

Tâche	Description	Compétences requises
Gérez les dépendances et les vulnérabilités.	1. Pour identifier les vulnérabilités et les risques courants (CVEs), exécutez la commande `pnpm audit` à la racine de votre référentiel. Vous devriez voir « Aucune vulnérabilité connue détectée ». 2. Installez un package intentionnellement vulnérable `core/` en l'exécutantpnpm `add minimist@0.2.3` , puis en exécutant `pnpm audit`. Notez la vulnérabilité signalée. 3. Désinstallez le package vulnérable qu'il `core/` contient en exécutantpnpm `remove minimist`.	Développeur d’applications

Tâche	Description	Compétences requises
Pré-validez les hameçons avec Husky.	1. Apportez quelques modifications mineures aux TypeScript fichiers du référentiel. Les modifications peuvent être aussi simples que l'ajout de commentaires. 2. Organisez et validez ces modifications en utilisant `git add -A` puis `git commit -m "test husky"`. Le déclencheur Husky pre-commit hook, défini dans `.husky/pre-commit`, exécute la commande. `pnpm lint-staged` 3. Observez comment lint-staged exécute les commandes spécifiées dans `*/.lintstagedrc.js` les fichiers du référentiel sur des fichiers qui ont été préparés par Git. Ces outils sont des mécanismes qui aident à empêcher le mauvais code de pénétrer dans votre application.	Développeur d'applications

Détruire l'infrastructure

Tâche	Description	Compétences requises
Supprimez le déploiement de votre compte.	1. Pour détruire l'infrastructure que vous avez mise en place lors de la première épopée, utilisez Run `pnpm destroy:local lninfra/`. 2. Attendez 15 minutes une fois l'opération `pnpm destroy:local` terminée, puis supprimez la fonction Lambda @Edge conservée en recherchant l'ID de votre application dans la console Lambda. Les fonctions Lambda @Edge sont répliquées., ce qui les rend difficiles à supprimer. Pour plus d'informations sur la suppression des fonctions Lambda @Edge, consultez la CloudFront documentation.	Développeur d’applications

Résolution des problèmes

Problème	Solution
Impossible d'établir la redirection de port	Assurez-vous que vos informations d'identification AWS sont correctement configurées et que vous disposez des autorisations nécessaires.

Problème	Solution
	Vérifiez que les variables d'environnement Bastion Host ID (`DB_BASTION_ID`) et Database Endpoint (`DB_ENDPOINT`) sont correctement définies. Si vous rencontrez toujours des problèmes, consultez la documentation AWS pour résoudre les problèmes liés aux connexions SSH et au gestionnaire de session.
Le site Web ne se charge pas `localhost :3000`	Vérifiez que la sortie du terminal indique une redirection de port réussie, y compris l'adresse de transfert. Assurez-vous qu'il n'y a aucun processus conflictuel utilisant le port 3000 sur votre machine locale. Vérifiez que l'application Green Boost est correctement configurée et s'exécute sur le port attendu (3000). Vérifiez dans votre navigateur Web la présence d'extensions ou de paramètres de sécurité susceptibles de bloquer les connexions locales.
Messages d'erreur lors du déploiement local (`pnpm deploy:local`)	Lisez attentivement les messages d'erreur pour identifier la cause du problème. Vérifiez que les variables d'environnement et les fichiers de configuration nécessaires sont correctement définis.

Ressources connexes

- Documentation du kit AWS CDK

- Documentation Green Boost
- Documentation Next.js
- Documentation Node.js
- Documentation React
- TypeScript documentation

Exécutez des tests unitaires pour une application Node.js à GitHub l'aide d'AWS CodeBuild

Créée par Thomas Scott (AWS) et Jean-Baptiste Guillois (AWS)

Récapitulatif

Ce modèle fournit un exemple de code source et des composants de test unitaires clés pour une API de jeu Node.js. Il inclut également des instructions pour exécuter ces tests unitaires à partir d'un GitHub référentiel à l'aide d'AWS CodeBuild, dans le cadre de votre flux de travail d'intégration continue et de livraison continue (CI/CD).

Le test unitaire est un processus de développement logiciel dans lequel différentes parties d'une application, appelées unités, sont testées individuellement et indépendamment pour en vérifier le bon fonctionnement. Les tests valident la qualité du code et confirment qu'il fonctionne comme prévu. D'autres développeurs peuvent également se familiariser facilement avec votre base de code en consultant les tests. Les tests unitaires réduisent le temps de refactorisation futur, aident les ingénieurs à se familiariser plus rapidement avec votre base de code et garantissent le comportement attendu.

Les tests unitaires consistent à tester des fonctions individuelles, notamment les fonctions AWS Lambda. Pour créer des tests unitaires, vous avez besoin d'un cadre de test et d'un moyen de valider les tests (assertions). Les exemples de code de ce modèle utilisent le framework de test Mocha et la bibliothèque d'assertions Chai.

Pour plus d'informations sur les tests unitaires et des exemples de composants de test, consultez la section Informations supplémentaires.

Conditions préalables et limitations

- Un compte AWS actif avec les CodeBuild autorisations correctes
- Un GitHub compte (voir les instructions d'inscription)
- Git (voir les instructions d'installation)
- Un éditeur de code pour apporter des modifications et envoyer votre code vers GitHub

Architecture

Ce modèle implémente l'architecture illustrée dans le schéma suivant.

Outils

Outils

- Git est un système de contrôle de version que vous pouvez utiliser pour le développement de code.
- AWS CodeBuild est un service d'intégration continue entièrement géré qui compile le code source, exécute des tests et produit des packages logiciels prêts à être déployés. Grâce à CodeBuild cela, vous n'avez pas besoin de provisionner, de gérer et de dimensionner vos propres serveurs de construction. CodeBuild évolue en continu et traite plusieurs versions simultanément, afin que vos versions ne soient pas laissées en attente dans une file d'attente. Vous pouvez démarrer rapidement en utilisant des environnements de génération prépackagés, ou bien, vous pouvez créer vos propres environnements de génération personnalisés, que vous utiliserez avec vos outils de génération. Avec CodeBuild, les ressources informatiques que vous utilisez vous sont facturées à la minute.

Code

Le code source de ce modèle est disponible sur GitHub, dans le référentiel d'applications de test unitaire de jeu Sample. Vous pouvez créer votre propre GitHub référentiel à partir de cet exemple (option 1) ou utiliser le référentiel d'échantillons directement (option 2) pour ce modèle. Suivez les instructions pour chaque option dans la section suivante. L'option que vous allez suivre dépend de votre cas d'utilisation.

Épopées

Option 1 - Exécutez des tests unitaires sur votre GitHub dépôt personnel avec CodeBuild

Tâche	Description	Compétences requises
Créez votre propre GitHub référentiel sur la base de l'exemple de projet.	1. Connectez-vous à GitHub. 2. Créez un nouveau référenti el. Pour obtenir des instructi ons, consultez la GitHub documentation. 3. Clonez et transférez le référentiel d'échantillons	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	dans le nouveau référentiel de votre compte.	

Tâche	Description	Compétences requises
Créez un nouveau CodeBuild projet.	1. Connectez-vous à l'AWS Management Console et ouvrez-la sur CodeBuild https://console.aws.amazon.com/codesuite/codebuild/home. 2. Choisissez Créer un projet de génération. 3. Dans la section Configuration du projet, pour Nom du projet, tapez aws-tests-sample-node-js. 4. Dans la section Source, pour Source provider, sélectionnez GitHub. 5. Pour Repository, choisissez Repository dans mon GitHub compte, puis collez l'URL dans le GitHub référentiel que vous venez de créer. 6. Dans la section Événements du webhook de la source principale, sélectionnez Reconstruire chaque fois qu'une modification de code est envoyée à ce référentiel. 7. Pour le type d'événement, choisissez PUSH. 8. Dans la section Environnement, choisissez Image	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	gérée, Amazon Linux et l'image la plus récente. 9. Conservez les paramètre s par défaut pour toutes les autres options, puis choisissez Créer un projet de construction.	
Démarrez la construction.	Sur la page Révision, choisissez Démarrer la génération pour exécuter la génération.	Développeur d'applications, administrateur AWS, AWS DevOps

Option 2 - Exécuter des tests unitaires sur un dépôt public avec CodeBuild

Tâche	Description	Compétences requises
Créez un nouveau projet CodeBuild de construction.	1. Connectez-vous à l'AWS Management Console et ouvrez-la sur CodeBuild https://console.aws.amazon.com/codesuite/codebuild/home. 2. Choisissez Créer un projet de génération. 3. Dans la section Configura tion du projet, pour Nom du projet, tapez aws-tests-sample-node-js. 4. Dans la section Source, pour Source provider, sélectionnez GitHub. 5. Pour Repository, choisisse z Public repository, puis	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	collez l'URL : https://github.com/aws-samples/node-js-tests-sample. 6. Dans la section Environnement, choisissez Image gérée, Amazon Linux et l'image la plus récente. 7. Conservez les paramètres par défaut pour toutes les autres options, puis choisissez Créer un projet de construction.	
Démarrez la construction.	Sur la page Révision, choisissez Démarrer la génération pour exécuter la génération.	Développeur d'applications, administrateur AWS, AWS DevOps

Analyser les tests unitaires

Tâche	Description	Compétences requises
Afficher les résultats des tests.	Dans la CodeBuild console, passez en revue les résultats du test unitaire de la CodeBuild tâche. Ils doivent correspondre aux résultats présentés dans la section Informations supplémentaires. Ces résultats valident l'intégration GitHub du référentiel avec CodeBuild.	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
Appliquez un webhook.	Vous pouvez désormais appliquer un webhook, ce qui vous permet de démarrer automatiquement une compilation chaque fois que vous envoyez des modificat ions de code à la branche principale de votre dépôt. Pour obtenir des instructi ons, consultez la CodeBuild documentation.	Développeur d'applications, administrateur AWS, AWS DevOps

Ressources connexes

- Exemple d'application de test unitaire de jeu (GitHub référentiel avec exemple de code)
- CodeBuild Documentation AWS
- GitHub événements webhook (CodeBuild documentation)
- Création d'un nouveau dépôt (GitHub documentation)

Informations supplémentaires

Résultats des tests unitaires

Dans la CodeBuild console, vous devriez voir les résultats des tests suivants une fois le projet construit avec succès.

Exemples de composants de test unitaire

Cette section décrit les quatre types de composants de test utilisés dans les tests unitaires : assertions, espions, stubs et simulacres. Il inclut une brève explication et un exemple de code pour chaque composant.

Assertions

Une assertion est utilisée pour vérifier un résultat attendu. Il s'agit d'un composant de test important car il valide la réponse attendue d'une fonction donnée. L'exemple d'assertion suivant confirme que l'ID renvoyé est compris entre 0 et 1 000 lors de l'initialisation d'un nouveau jeu.

```
const { expect }  = require('chai');
const { Game } = require('../src/index');

describe('Game Function Group', () => {
 it('Check that the Game ID is between 0 and 1000', function() {
      const game = new Game();
      expect(game.id).is.above(0).but.below(1000)
 });
});
```

espions

Un espion est utilisé pour observer ce qui se passe lorsqu'une fonction est en cours d'exécution. Par exemple, vous souhaiterez peut-être vérifier que la fonction a été appelée correctement. L'exemple suivant montre que les méthodes start et stop sont appelées sur un objet de classe Game.

```
const { expect }  = require('chai');
const { spy } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () => {
   it('should verify that the correct function is called', () => {
      const spyStart = spy(Game.prototype, "start");
      const spyStop = spy(Game.prototype, "stop");

      const game = new Game();
      game.start();
      game.stop();

      expect(spyStart.called).to.be.true
      expect(spyStop.called).to.be.true
    });
});
```

Talons

Un stub est utilisé pour remplacer la réponse par défaut d'une fonction. Cela est particulièrement utile lorsque la fonction envoie une requête externe, car vous souhaitez éviter de faire des demandes externes à partir de tests unitaires. (Les requêtes externes sont mieux adaptées aux tests d'intégration, qui permettent de tester physiquement les demandes entre différents composants.) Dans l'exemple suivant, un stub force la fonction GetID à renvoyer un ID.

```
const { expect }  = require('chai');
const {.stub } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
   it('Check that the Game ID is between 0 and 1000', function() {
      let generateIdStub = stub(Game.prototype, 'getId').returns(999999);

      const game = new Game();

      expect(game.getId).is.equal(999999);

      generateIdStub.restore();
    });
});
```

Des moqueries

Une simulation est une fausse méthode dont le comportement est préprogrammé pour tester différents scénarios. Une maquette peut être considérée comme une forme étendue de talon et peut effectuer plusieurs tâches simultanément. Dans l'exemple suivant, une simulation est utilisée pour valider trois scénarios :

- La fonction est appelée
- La fonction est appelée avec des arguments
- La fonction renvoie le nombre entier 9

```
const { expect }  = require('chai');
const {.mock } = require('sinon');

const { Game } = require('../src/index');

describe('Game Function Group', () =>  {
```

```
   it('Check that the Game ID is between 0 and 1000', function() {
      let mock = mock(Game.prototype).expects('getId').withArgs().returns(9);

      const game = new Game();
      const id = get.getId();

      mock.verify();
      expect(id).is.equal(9);
    });
});
```

Structurer un projet Python dans une architecture hexagonale à l'aide d'AWS Lambda

Créée par Furkan Oruc (AWS), Dominik Goby (AWS), Darius Kunce (AWS) et Michal Ploski (AWS)

Récapitulatif

Ce modèle montre comment structurer un projet Python dans une architecture hexagonale à l'aide d'AWS Lambda. Le modèle utilise l'AWS Cloud Development Kit (AWS CDK) comme outil d'infrastructure en tant que code (iAc), Amazon API Gateway comme API REST et Amazon DynamoDB comme couche de persistance. L'architecture hexagonale suit les principes de conception axés sur le domaine. Dans une architecture hexagonale, le logiciel comprend trois composants : le domaine, les ports et les adaptateurs. Pour obtenir des informations détaillées sur les architectures hexagonales et leurs avantages, consultez le guide Création d'architectures hexagonales sur AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Expérience en Python
- Connaissance d'AWS Lambda, d'AWS CDK, d'Amazon API Gateway et de DynamoDB
- Un GitHub compte (voir les instructions d'inscription)
- Git (voir les instructions d'installation)
- Un éditeur de code pour apporter des modifications et transférer votre code vers GitHub (par exemple, Visual Studio Code ou JetBrains PyCharm)
- Docker est installé et le daemon Docker est opérationnel

Versions du produit

- Git version 2.24.3 ou ultérieure
- Python version 3.7 ou ultérieure
- Kit de développement logiciel AWS version 2
- Poetry version 1.1.13 ou ultérieure

- AWS Lambda Powertools pour Python version 1.25.6 ou ultérieure
- pytest version 7.1.1 ou ultérieure
- Moto version 3.1.9 ou ultérieure
- version 1.9.0 ou ultérieure de pydantic
- Boto3 version 1.22.4 ou ultérieure
- mypy-boto3-dynamodb version 1.24.0 ou ultérieure

Architecture

Pile technologique cible

La pile technologique cible consiste en un service Python qui utilise API Gateway, Lambda et DynamoDB. Le service utilise un adaptateur DynamoDB pour conserver les données. Il fournit une fonction qui utilise Lambda comme point d'entrée. Le service utilise Amazon API Gateway pour exposer une API REST. L'API utilise AWS Identity and Access Management (IAM) pour l'authentification des clients.

Architecture cible

Pour illustrer l'implémentation, ce modèle déploie une architecture cible sans serveur. Les clients peuvent envoyer des demandes à un point de terminaison API Gateway. API Gateway transmet la demande à la fonction Lambda cible qui implémente le modèle d'architecture hexagonal. La fonction Lambda effectue des opérations de création, de lecture, de mise à jour et de suppression (CRUD) sur une table DynamoDB.

> **Important**
>
> Ce modèle a été testé dans un environnement PoC. Vous devez effectuer un examen de sécurité pour identifier le modèle de menace et créer une base de code sécurisée avant de déployer une architecture dans un environnement de production.

L'API prend en charge cinq opérations sur une entité de produit :

- `GET /products`renvoie tous les produits.
- `POST /products`crée un nouveau produit.
- `GET /products/{id}`renvoie un produit spécifique.
- `PUT /products/{id}`met à jour un produit spécifique.
- `DELETE /products/{id}`supprime un produit spécifique.

Vous pouvez utiliser la structure de dossiers suivante pour organiser votre projet selon le modèle d'architecture hexagonal :

```
app/  # application code
|--- adapters/  # implementation of the ports defined in the domain
     |--- tests/  # adapter unit tests
|--- entrypoints/  # primary adapters, entry points
     |--- api/  # api entry point
          |--- model/  # api model
          |--- tests/  # end to end api tests
|--- domain/  # domain to implement business logic using hexagonal architecture
     |--- command_handlers/  # handlers used to execute commands on the domain
     |--- commands/  # commands on the domain
     |--- events/  # events triggered via the domain
     |--- exceptions/  # exceptions defined on the domain
     |--- model/  # domain model
     |--- ports/  # abstractions used for external communication
     |--- tests/  # domain tests
|--- libraries/  # List of 3rd party libraries used by the Lambda function
infra/  # infrastructure code
simple-crud-app.py  # AWS CDK v2 app
```

Outils

Services AWS

- Amazon API Gateway est un service entièrement géré qui permet aux développeurs de créer, publier, gérer, surveiller et sécuriser facilement APIs à n'importe quelle échelle.
- Amazon DynamoDB est une base de données NoSQL à valeur clé entièrement gérée, sans serveur, conçue pour exécuter des applications hautes performances à n'importe quelle échelle.
- AWS Lambda est un service de calcul sans serveur piloté par les événements qui vous permet d'exécuter du code pour pratiquement n'importe quel type d'application ou de service principal sans

provisionner ni gérer de serveurs. Vous pouvez lancer des fonctions Lambda à partir de plus de 200 services AWS et applications logicielles en tant que service (SaaS), et ne payer que pour ce que vous utilisez.

Outils

- Git est utilisé comme système de contrôle de version pour le développement de code dans ce modèle.
- Python est utilisé comme langage de programmation pour ce modèle. Python fournit des structures de données de haut niveau et une approche de la programmation orientée objet. AWS Lambda fournit un environnement d'exécution Python intégré qui simplifie le fonctionnement des services Python.
- Visual Studio Code est utilisé comme IDE pour le développement et les tests de ce modèle. Vous pouvez utiliser n'importe quel IDE prenant en charge le développement en Python (par exemple, PyCharm).
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel open source qui vous permet de définir les ressources de vos applications cloud à l'aide de langages de programmation courants. Ce modèle utilise le CDK pour écrire et déployer l'infrastructure cloud sous forme de code.
- La poésie est utilisée pour gérer les dépendances dans le modèle.
- Docker est utilisé par le AWS CDK pour créer le package et la couche Lambda.

Code

Le code de ce modèle est disponible dans le référentiel d'exemples d'architecture hexagonale GitHub Lambda.

Bonnes pratiques

Pour utiliser ce modèle dans un environnement de production, suivez les meilleures pratiques suivantes :

- Utilisez les clés gérées par le client dans AWS Key Management Service (AWS KMS) pour chiffrer les groupes de CloudWatch journaux Amazon et les tables Amazon DynamoDB.
- Configurez AWS WAF pour Amazon API Gateway afin d'autoriser l'accès uniquement depuis le réseau de votre organisation.

- Envisagez d'autres options d'autorisation API Gateway si IAM ne répond pas à vos besoins. Par exemple, vous pouvez utiliser les groupes d'utilisateurs Amazon Cognito ou les autorisateurs Lambda d'API Gateway.
- Utilisez les sauvegardes DynamoDB.
- Configurez les fonctions Lambda avec un déploiement de cloud privé virtuel (VPC) afin de maintenir le trafic réseau dans le cloud.
- Mettez à jour la configuration d'origine autorisée pour le partage de ressources entre origines (CORS) avant le vol afin de restreindre l'accès au domaine d'origine demandeur uniquement.
- Utilisez cdk-nag pour vérifier le code AWS CDK afin de connaître les meilleures pratiques en matière de sécurité.
- Envisagez d'utiliser des outils d'analyse de code pour détecter les problèmes de sécurité courants dans le code. Par exemple, Bandit est un outil conçu pour détecter les problèmes de sécurité courants dans le code Python. PIP-Audit analyse les environnements Python à la recherche de packages présentant des vulnérabilités connues.

Ce modèle utilise AWS X-Ray pour suivre les demandes via le point d'entrée, le domaine et les adaptateurs de l'application. AWS X-Ray aide les développeurs à identifier les goulets d'étranglement et à déterminer les latences élevées afin d'améliorer les performances des applications.

Épopées

Initialiser le projet

Tâche	Description	Compétences requises
Créez votre propre référentiel.	1. Connectez-vous à GitHub. 2. Créez un nouveau référentiel. Pour obtenir des instructions, consultez la GitHub documentation. 3. Clonez et transférez le référentiel d'échantillons correspondant à ce modèle dans le nouveau référentiel de votre compte.	Développeur d’applications

Tâche	Description	Compétences requises

Installez les dépendances.	1. Installez Poetry.
	`pip install poetry`
	2. Installez les packages depuis le répertoire racine. La commande suivante installe l'application et les packages AWS CDK. Il installe également les packages de développement nécessaires à l'exécution des tests unitaires. Tous les packages installés sont placés dans un nouvel environnement virtuel.
	`poetry install`
	3. Pour afficher une représentation graphique des packages installés, exécutez la commande suivante.
	`poetry show --tree`
	4. Mettez à jour toutes les dépendances.
	`poetry update`
	5. Ouvrez un nouveau shell dans l'environnement virtuel nouvellement
		Développeur d’applications

Tâche	Description	Compétences requises
	créé. Il contient toutes les dépendances installées. `poetry shell`	

Tâche	Description	Compétences requises
Configurez votre IDE.	Nous recommandons Visual Studio Code, mais vous pouvez utiliser n'importe quel IDE de votre choix qui supporte Python. Les étapes suivantes concernent Visual Studio Code. 1. Mettez à jour le `.vscode/settings` fichier. `{ "python.testing.pytestArgs": [ "app/adapters/tests", "app/entrypoints/api/tests", "app/domain/tests" ], "python.testing.unittestEnabled": false, "python.testing.pytestEnabled": true, "python.envFile": "${workspaceFolder}/.env", }` 2. Créez un `.env` fichier dans le répertoire racine du projet. Cela garantit que le répertoire racine du projet est inclus dans le `PYTHONPATH` afin de	Développeur d'applications

Tâche	Description	Compétences requises
	`pytest` pouvoir le trouver et découvrir correctement tous les packages. `PYTHONPATH=.`	
Exécuter des tests unitaires, option 1 : utiliser Visual Studio Code.	1. Choisissez l'interpréteur Python de l'environnement virtuel géré par Poetry. 2. Exécutez des tests à partir de l'explorateur de tests.	Développeur d’applications

Exécuter des tests unitaires , option 2 : utiliser des commandes shell.	1. Démarrez un nouveau shell dans l'environnement virtuel.
	`poetry shell`
	2. Exécutez la `pytest` commande depuis le répertoire racine.
	`python -m pytest`
	Vous pouvez également exécuter la commande directement depuis Poetry.
	`poetry run python -m pytest`
		Développeur d’applications

Déployez et testez l'application

Tâche	Description	Compétences requises
Demandez des informations d'identification temporaires.	Pour avoir des informations d'identification AWS sur le shell lorsque vous exécutez`cdk deploy`, créez des informations d'identification temporaires à l'aide d'AWS IAM Identity Center (successeur d'AWS Single Sign-On). Pour obtenir des instructions, consultez le billet de blog Comment récupérer des informations d'identification à court terme pour une utilisation en CLI avec AWS IAM Identity Center.	Développeur d'applications, AWS DevOps

Déployez l'application.	1. Installez le kit AWS CDK v2.
	`npm install -g aws-cdk`
	Pour plus d'informations, consultez la documentation AWS CDK.
	2. Intégrez le CDK AWS à votre compte et à votre région.
	`cdk bootstrap aws://12345678900/us-east-1 --profile aws-profile-name`
		Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	3. Déployez l'application en tant que CloudFormation stack AWS à l'aide d'un profil AWS. `cdk deploy --profile aws-profile-name`	
Testez l'API, option 1 : utilisez la console.	Utilisez la console API Gateway pour tester l'API. Pour plus d'informations sur les opérations d'API et les messages de demande/réponse, consultez la section sur l'utilisation de l'API du fichier readme du référentiel. GitHub	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
Testez l'API, option 2 : utilisez Postman.	Si vous souhaitez utiliser un outil tel que Postman : 1. Installez Postman en tant qu'application autonome ou extension de navigateur. 2. Copiez l'URL du point de terminaison pour l'API Gateway. Il sera présenté dans le format suivant. `https://{api-id}.execute-api.{region}.amazonaws.com/{stage}/{path}` 3. Configurez la signature AWS dans l'onglet d'autorisation. Pour obtenir des instructions, consultez l'article AWS re:Post sur l'activation de l'authentification IAM pour API Gateway REST. APIs 4. Utilisez Postman pour envoyer des demandes à votre point de terminaison d'API.	Développeur d'applications, AWS DevOps

Développez le service

Tâche	Description	Compétences requises
Rédigez des tests unitaires pour le domaine commercial.	1. Créez un fichier Python dans le `app/domain/`	Développeur d’applications

Tâche	Description	Compétences requises

	`tests` dossier en utilisant le préfixe du nom de `test_` fichier.
	2. Créez une nouvelle méthode de test pour tester la nouvelle logique métier à l'aide de l'exemple suivant.
	`def test_create_product_should_store_in_repository():`
	`    # Arrange`
	`    command = create_product_command.CreateProductCommand(`
	`        name="Test Product",`
	`        description="Test Description",`
	`    )`
	`    # Act`
	`    create_product_command_handler.handle_create_product_command(`
	`        command=command, unit_of_work=mock_unit_of_work`
	`    )`
	`# Assert`
	3. Créez une classe de commande dans le `app/domain/commands` dossier.	

Tâche	Description	Compétences requises
	4. Si la fonctionnalité est nouvelle, créez un stub pour le gestionnaire de commandes dans le `app/domain/command_handlers` dossier. 5. Exécutez le test unitaire pour voir s'il échoue, car il n'existe toujours aucune logique métier. `python -m pytest`	

Tâche	Description	Compétences requises

Implémenter des commandes et des gestionnaires de commandes.	1. Implémentez la logique métier dans le fichier de gestionnaire de commandes nouvellement créé.
	2. Pour chaque dépendance interagissant avec des systèmes externes, déclarez une classe abstraite dans le `app/domain/ports` dossier.
	
	`class ProductsRepository(ABC):`
	`  @abstractmethod`
	`  def add(self, product: product.Product) -> None:`
	`  ...`
	
	`class UnitOfWork(ABC):`
	`  products: ProductsRepository`
	
	`  @abstractmethod`
	`  def commit(self) -> None:`
	`  ...`
	
	`  @abstractmethod`
	`  def __enter__(self) -> typing.Any:`
	`  ...`
	
	`  @abstractmethod`
	`  def __exit__(self, *args) -> None:`
		Développeur d’applications

Tâche	Description	Compétences requises

	...
	3. Mettez à jour la signature du gestionnaire de commandes pour accepter les dépendances nouvellement déclarées en utilisant la classe de port abstraite comme annotation de type.
	`def handle_create_product_command( command: create_product_command.CreateProductCommand, unit_of_work: unit_of_work.UnitOfWork,) -> str: ...`
	4. Mettez à jour le test unitaire pour simuler le comportement de toutes les dépendances déclarées pour le gestionnaire de commandes.
	`# Arrange mock_unit_of_work = unittest.mock.create_autospec( spec=unit_of_work.UnitOfWork, instance=True ) mock_unit_of_work.products =`	

Tâche	Description	Compétences requises
	unittest.mock.create_autospec(spec=unit_of_work.ProductsRepository, instance=True)	

	5. Mettez à jour la logique d'assertion dans le test pour vérifier les invocations de dépendance attendues.
	`# Assert`
	`mock_unit_of_work.commit.assert_called_once()`
	`product = mock_unit_of_work.products.add.call_args.args[0]`
	`assertpy.assert_that(product.name).is_equal_to("Test Product")`
	`assertpy.assert_that(product.description).is_equal_to("Test Description")`
	6. Exécutez le test unitaire pour voir s'il réussit.
	`python -m pytest`	

Tâche	Description	Compétences requises
Rédigez des tests d'intégration pour les adaptateurs secondaires.	1. Créez un fichier de test dans le `app/adapters/tests` dossier en l'utilisant `test_` comme préfixe de nom de fichier. 2. Utilisez la bibliothèque Moto pour simuler les services AWS. 3. Créez une nouvelle méthode de test pour un test d'intégration de l'adaptateur.	Développeur d’applications

```
@pytest.fixture
def mock_dynamodb():
   with moto.mock
_dynamodb():
    yield boto3.res
ource("dynamodb",
 region_name="eu-ce
ntral-1")
```

```
def test_add_
and_commit_should_
store_product(mock
_dynamodb):
    # Arrange
    unit_of_work =
 dynamodb_unit_of_w
ork.DynamoDBUnitOf
Work(
        table_nam
e=TEST_TABLE_NAME,
 dynamodb_client=mo
ck_dynamodb.meta.c
lient
    )
```

Tâche	Description	Compétences requises

	<pre> current_time = datetime.datetime.now(datetime.timezone.utc).isoformat()
	
	    new_product_id = str(uuid.uuid4())
	    new_product = product.Product(
	        id=new_product_id,
	        name="test-name",
	        description="test-description",
	        createDate=current_time,
	        lastUpdateDate=current_time,
	    )
	
	    # Act
	    with unit_of_work:
	        unit_of_work.products.add(new_product)
	        unit_of_work.commit()
	
	    # Assert</pre> 4. Créez une classe d'adaptateur dans le `app/adapters` dossier. Utilisez la classe abstraite du dossier ports comme classe de base.	

Tâche	Description	Compétences requises
	5. Exécutez le test unitaire pour le voir échouer, car il n'y a toujours aucune logique. `python -m pytest`	

Tâche	Description	Compétences requises

Implémentez des adaptateurs secondaires.	1. Implémentez la logique dans le fichier d'adaptateur nouvellement créé.
	2. Mettez à jour les assertions de test.
	
	`# Assert`
	`    with unit_of_work_readonly:`
	`        product_from_db = unit_of_work_readonly.products.get(new_product_id)`
	
	`    assertpy.assert_that(product_from_db).is_not_none()`
	`    assertpy.assert_that(product_from_db.dict()).is_equal_to(`
	`        {`
	`            "id": new_product_id,`
	`            "name": "test-name",`
	`            "description": "test-description",`
	`            "createDate": current_time,`
	`            "lastUpdateDate": current_time,`
	`        }`
	`    )`
		Développeur d’applications

Tâche	Description	Compétences requises
	3. Exécutez le test unitaire pour voir s'il réussit. `python -m pytest`	

Tâche	Description	Compétences requises
Rédigez end-to-end des tests.	1. Créez un fichier de test dans le `app/entry points/api/tests` dossier en l'utilisant `test_` comme préfixe de nom de fichier. 2. Créez un dispositif de contexte Lambda qui sera utilisé par le test pour appeler Lambda. 3. Créez une méthode de test pour l'invocation de l'API.	Développeur d’applications

```
@pytest.fixture
def lambda_co
ntext():
    @dataclass
    class LambdaCon
text:
        function_
name: str = "test"
        memory_li
mit_in_mb: int = 128
        invoked_f
unction_arn: str =
 "arn:aws:lambda:eu
-west-1:809313241:
function:test"
        aws_reque
st_id: str =
 "52fdfc07-2182-154
f-163f-5f0f9a621d7
2"

 return LambdaCon
text()
```

Tâche	Description	Compétences requises

	`def test_crea te_product(lambda_ context):`
	`  # Arrange`
	`  name = "TestName"`
	`  description = "Test description"`
	`  request = api_model.CreatePr oductRequest(name= name, descripti on=description)`
	
	`  minimal_event = api_gateway_proxy_ event.APIGatewayPr oxyEvent(`
	`  {`
	`  "path": "/ products",`
	`  "httpMeth od": "POST",`
	`  "requestC ontext": {  # correlation ID`
	
	`  "requestId": "c6af9ac6-7b61-11e 6-9a41-93e8deadbee f"`
	`  },`
	`  "body": json.dumps(request .dict()),`
	`  }`
	`  )`
	
	`  create_pr oduct_func_mock = unittest.mock.crea te_autospec(`	

Tâche	Description	Compétences requises

	<pre>spec=crea
	te_product_command
	_handler.handle_cr
	eate_product_comma
	nd
	)
	handler.c
	reate_product_comm
	and_handler.handle
	_create_product_co
	mmand = (
	create_pr
	oduct_func_mock
	)
	
	# Act
	handler.h
	andler(minimal_eve
	nt, lambda_context)</pre>
	4. Exécutez le test unitaire pour le voir échouer, car il n'y a toujours aucune logique.
	<pre>python -m pytest</pre>	

Tâche	Description	Compétences requises

Implémentez les adaptateurs principaux.	1. Créez une fonction pour la logique métier de l'API et déclarez-la en tant que ressource d'API.
	
	`@tracer.capture_method`
	`@app.post("/products")`
	`@utils.parse_event(model=api_model.CreateProductRequest, app_context=app)`
	`def create_product(`
	`request: api_model.CreateProductRequest,`
	`) -> api_model.CreateProductResponse:`
	`"""Creates a product."""`
	`...`
	
	Note
	Tous les décorateurs que vous voyez sont des fonctionnalités de la bibliothèque AWS Lambda Powertools for Python. Pour plus de détails, consultez le site Web AWS Lambda
		Développeur d'applications

Tâche	Description	Compétences requises

	Powertools for Python.
	2. Implémentez la logique de l'API.
	`id=create_product_command_handler.handle_create_product_command( command=create_product_command.CreateProductCommand( name=request.name, description=request.description, ), unit_of_work=unit_of_work, ) response = api_model.CreateProductResponse(id=id) return response.dict()`
	3. Exécutez le test unitaire pour voir s'il réussit.
	`python -m pytest`	

Ressources connexes

Guide APG

- Création d'architectures hexagonales sur AWS

Références AWS

- Documentation AWS Lambda
- Documentation du kit de développement AWS
  - Votre première application AWS CDK
- Documentation d'API Gateway
  - Contrôler l'accès à une API avec des autorisations IAM
  - Utiliser la console API Gateway pour tester une méthode d'API REST
- Documentation Amazon DynamoDB

Outils

- Site web git-scm.com
- Installation de Git
- Création d'un nouveau GitHub référentiel
- Site Web Python
- Outils puissants AWS Lambda pour Python
- Site de Postman
- bibliothèque d'objets fictifs en Python
- Site de poésie

IDEs

- Site Web de Visual Studio Code
- PyCharm website

Plus de modèles

- Accès Services AWS depuis une application ASP.NET Core à l'aide des pools d'identités Amazon Cognito
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS Fargate, d' PrivateLinkAWS et d'un Network Load Balancer
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Associer un AWS CodeCommit référentiel dans un compte Compte AWS à Amazon SageMaker AI Studio Classic dans un autre compte
- Automatisez la suppression des AWS CloudFormation piles et des ressources associées
- Limitez l'accès en fonction de l'adresse IP ou de la géolocalisation en utilisant AWS WAF
- Créez une architecture faiblement couplée avec des microservices en utilisant DevOps Practices et AWS Cloud9
- Créez une application mobile React Native sans serveur à l'aide d'AWS Amplify
- Créez et testez des applications iOS avec AWS CodeCommit CodePipeline, AWS et AWS Device Farm
- Configurez la journalisation pour les applications .NET dans Amazon CloudWatch Logs en utilisant NLog
- Création d'un pipeline et d'une AMI à l'aide de CodePipeline and HashiCorp Packer
- Créez un pipeline et déployez des mises à jour d'artefacts sur des instances locales à l'aide de EC2 CodePipeline
- Créez une définition de tâche Amazon ECS et montez un système de fichiers sur des EC2 instances à l'aide d'Amazon EFS
- Déployez une application basée sur GRPC sur un cluster Amazon EKS et accédez-y à l'aide d'un Application Load Balancer
- Déployez une ChatOps solution pour gérer les résultats du scan SAST en utilisant Amazon Q Developer dans les applications de chat, les actions personnalisées et AWS CloudFormation
- Déployez des CloudWatch canaris Synthetics à l'aide de Terraform
- Déployez des microservices Java sur Amazon ECS à l'aide d'AWS Fargate
- Déployez un cas d'utilisation de RAG AWS en utilisant Terraform et Amazon Bedrock
- Déployez des ressources dans une AWS Wavelength zone à l'aide de Terraform

- Implémentez la gestion des versions d'API basée sur les chemins en utilisant des domaines personnalisés dans Amazon API Gateway
- Migrer une file d'attente de messagerie de Microsoft Azure Service Bus vers Amazon SQS
- Migrer une application .NET de Microsoft Azure App Service vers AWS Elastic Beanstalk
- Migrer une application Web Go sur site vers AWS Elastic Beanstalk à l'aide de la méthode binaire
- Migrer un serveur SFTP sur site vers AWSAWS Transfer for SFTP
- Migrer d'un serveur WebSphere d'applications IBM vers Apache Tomcat sur Amazon EC2
- Migrez d'IBM WebSphere Application Server vers Apache Tomcat sur Amazon EC2 avec Auto Scaling
- Migrer d'Oracle GlassFish vers AWS Elastic Beanstalk
- Migrez des applications Java sur site vers AWS à l'aide d'AWS App2Container
- Migrer OpenText TeamSite les charges de travail vers le cloud AWS
- Migrer les certificats SSL Windows vers un Application Load Balancer à l'aide d'ACM
- Modernisez les applications ASP.NET Web Forms sur AWS
- Surveillez l'activité des applications à l'aide de CloudWatch Logs Insights
- Exécuter un conteneur Docker d'API Web ASP.NET Core sur une instance Amazon Linux EC2
- Diffusez du contenu statique dans un compartiment Amazon S3 via un VPC en utilisant Amazon CloudFront
- Configuration d'une PeopleSoft architecture à haute disponibilité sur AWS
- Simplifiez le développement et le déploiement des robots Amazon Lex à l'aide d'un flux de travail automatisé
- Résoudre les problèmes liés aux états en AWS Step Functions utilisant Amazon Bedrock
- Utilisez Network Firewall pour capturer les noms de domaine DNS à partir de l'indication du nom du serveur pour le trafic sortant
- Visualisez les résultats du modèle AI/ML à l'aide de Flask et AWS Elastic Beanstalk

IoT

Rubriques

- Configuration de la journalisation et de la surveillance des événements de sécurité dans votre AWS IoT environnement
- Extraire et interroger AWS IoT SiteWise les attributs de métadonnées dans un lac de données
- Configuration et résolution des problèmes liés à AWS IoT Greengrass avec des appareils clients
- Plus de modèles

Configuration de la journalisation et de la surveillance des événements de sécurité dans votre AWS IoT environnement

Créée par Prateek Prakash (AWS)

Récapitulatif

Garantir la sécurité de vos environnements Internet des objets (IoT) est une priorité importante, notamment parce que les entreprises connectent des milliards d'appareils à leurs environnements informatiques. Ce modèle fournit une architecture de référence que vous pouvez utiliser pour implémenter la journalisation et la surveillance des événements de sécurité dans votre environnement IoT sur le AWS Cloud. Généralement, un environnement IoT sur le AWS Cloud comporte les trois couches suivantes :

- Des appareils IoT qui génèrent des données de télémétrie pertinentes.
- AWS IoT des services (par exemple, AWS IoT CoreAWS IoT Device Management, ou AWS IoT Device Defender) qui connectent vos appareils IoT à d'autres appareils et Services AWS.
- Backend Services AWS qui aide à traiter les données de télémétrie et fournit des informations utiles pour vos différents cas d'utilisation commerciaux.

Les meilleures pratiques décrites dans le livre blanc AWS IoT Lens - AWS Well-Architected Framework peuvent vous aider à revoir et à améliorer votre architecture basée sur le cloud et à mieux comprendre l'impact commercial de vos décisions de conception. Il est important d'analyser les journaux et les indicateurs des applications sur vos appareils et dans le AWS Cloud. Vous pouvez y parvenir en utilisant différentes approches et techniques (par exemple, la modélisation des menaces) pour identifier les mesures et les événements qui doivent être surveillés pour détecter les problèmes de sécurité potentiels.

Ce modèle décrit comment utiliser les services de sécurité pour concevoir AWS IoT et mettre en œuvre une architecture de référence de journalisation et de surveillance de la sécurité pour un environnement IoT sur le AWS Cloud. Cette architecture s'appuie sur les meilleures pratiques de AWS sécurité existantes et les applique à votre environnement IoT.

Conditions préalables et limitations

Prérequis

- Un environnement de zone d'atterrissage existant. Pour plus d'informations à ce sujet, consultez le guide Configuration d'un AWS environnement multi-comptes sécurisé et évolutif sur le site Web de AWS Prescriptive Guidance.
- Les comptes suivants doivent être disponibles dans votre zone de landing zone :
  - Compte Log Archive : ce compte est destiné aux utilisateurs qui ont besoin d'accéder aux informations de journalisation des comptes des unités organisationnelles de votre zone d'atterrissage (OUs). Pour plus d'informations à ce sujet, consultez la section Security OU — Log Archive account du guide AWS Security Reference Architecture sur le site Web AWS Prescriptive Guidance.
  - Compte de sécurité : vos équipes de sécurité et de conformité utilisent ce compte à des fins d'audit ou pour effectuer des opérations de sécurité d'urgence. Ce compte est également désigné comme compte administrateur pour Amazon GuardDuty. Les utilisateurs du compte administrateur peuvent configurer GuardDuty, en plus de consulter et de gérer GuardDuty les résultats pour leur propre compte et pour tous les comptes des membres. Pour plus d'informations à ce sujet, consultez la section Gestion de plusieurs comptes GuardDuty dans la GuardDuty documentation.
  - Compte IoT — Ce compte est destiné à votre environnement IoT.

Architecture

Ce modèle étend la solution de journalisation centralisée de la bibliothèque de AWS solutions pour collecter et traiter les événements IoT liés à la sécurité. La solution de journalisation centralisée est déployée dans le compte Security et permet de collecter, d'analyser et d'afficher CloudWatch les journaux Amazon dans un tableau de bord unique. Cette solution consolide, gère et analyse les fichiers journaux provenant de sources multiples. Enfin, la solution de journalisation centralisée utilise également Amazon OpenSearch Service et les OpenSearch tableaux de bord pour afficher une vue unifiée de tous les événements du journal.

Le schéma d'architecture suivant montre les principaux composants d'une architecture de journalisation et de référence de sécurité IoT sur le AWS Cloud.

Le schéma suivant illustre le flux de travail suivant :

1. Les objets IoT sont les appareils qui doivent être surveillés pour détecter les événements de sécurité anormaux. Ces appareils exécutent un agent pour publier des événements ou des mesures de sécurité sur AWS IoT Core et AWS IoT Device Defender.
2. Lorsque la AWS IoT journalisation est activée, AWS IoT envoie des événements de progression concernant chaque message lorsqu'il est transmis de vos appareils à Amazon CloudWatch Logs via le courtier de messages et le moteur de règles. Vous pouvez utiliser CloudWatch les abonnements Logs pour transférer des événements vers une solution de journalisation centralisée. Pour plus d'informations à ce sujet, consultez AWS IoT les métriques et les dimensions dans la AWS IoT Core documentation.
3. AWS IoT Device Defender permet de surveiller les configurations non sécurisées et les indicateurs de sécurité de vos appareils IoT. Lorsqu'une anomalie est détectée, des alarmes avertissent Amazon Simple Notification Service (Amazon SNS), qui joue le rôle d' AWS Lambda abonné. La fonction Lambda envoie l'alarme sous forme de message à CloudWatch Logs. Vous pouvez utiliser CloudWatch les abonnements Logs pour transférer des événements vers votre solution de journalisation centralisée. Pour plus d'informations à ce sujet, consultez les sections Contrôles d'audit, Téléchargement de journaux côté appareil vers CloudWatch et Configuration de la AWS IoT journalisation dans la AWS IoT Core documentation.
4. AWS CloudTrail enregistre les actions du plan de AWS IoT Core contrôle qui apportent des modifications (par exemple, création, mise à jour ou attachement APIs). Lorsqu'il CloudTrail est configuré dans le cadre de la mise en œuvre d'une zone d'atterrissage, il envoie des événements à CloudWatch Logs. Vous pouvez utiliser des abonnements pour transférer des événements vers votre solution de journalisation centralisée.
5. AWS Config les règles gérées ou personnalisées évaluent les ressources qui font partie de votre environnement IoT. Surveillez vos notifications de modification de conformité en utilisant les CloudWatch événements avec CloudWatch journaux comme cible. Une fois les notifications de modification de conformité envoyées à CloudWatch Logs, vous pouvez utiliser des abonnements pour transférer des événements vers votre solution de journalisation centralisée.
6. Amazon analyse GuardDuty en permanence les événements CloudTrail de gestion et aide à identifier les appels d'API adressés aux AWS IoT Core points de terminaison à partir d'adresses IP malveillantes connues, de géolocalisations inhabituelles ou de proxys anonymisés. Surveillez GuardDuty les notifications en utilisant les CloudWatch événements avec les groupes de CloudWatch journaux dans les journaux comme cible. Lorsque GuardDuty des notifications sont envoyées à CloudWatch Logs, vous pouvez utiliser des abonnements pour transférer des événements vers votre solution de surveillance centralisée ou utiliser la GuardDuty console de votre compte Security pour consulter les notifications.

7. AWS Security Hub surveille votre compte IoT en utilisant les meilleures pratiques de sécurité. Surveillez les notifications du Security Hub en utilisant comme cible les CloudWatch événements avec des groupes de CloudWatch journaux dans les journaux. Lorsque les notifications Security Hub sont envoyées à CloudWatch Logs, utilisez des abonnements pour transférer les événements vers votre solution de surveillance centralisée ou utilisez la console Security Hub de votre compte Security pour consulter les notifications.
8. Amazon Detective évalue et analyse les informations afin d'en isoler la cause première et de prendre des mesures en fonction des résultats de sécurité relatifs à des appels inhabituels vers des AWS IoT terminaux ou d'autres services de votre architecture IoT.
9. Amazon Athena interroge les journaux stockés dans votre compte Log Archive afin de mieux comprendre les résultats de sécurité et d'identifier les tendances et les activités malveillantes.

Outils

- Amazon Athena est un service de requête interactif qui facilite l'analyse des données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du SQL standard.
- AWS CloudTrailvous aide à activer la gouvernance, la conformité et l'audit opérationnel et des risques de votre Compte AWS.
- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez les utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos ressources et vos applications.
- Amazon CloudWatch Logs centralise les journaux de tous vos systèmes, applications et applications Services AWS que vous utilisez. Vous pouvez consulter et surveiller les journaux, y rechercher des codes ou modèles d'erreur spécifiques, les filtrer en fonction de champs spécifiques ou les archiver en toute sécurité pour une analyse future.
- AWS Configfournit une vue détaillée de la configuration des AWS ressources de votre Compte AWS.
- Amazon Detective facilite l'analyse, l'investigation et l'identification rapide de la cause première des problèmes de sécurité ou des activités suspectes.
- AWS Glueest un service d'extraction, de transformation et de chargement (ETL) entièrement géré qui permet de classer vos données, de les nettoyer, de les enrichir et de les déplacer de manière fiable entre différents magasins de données et flux de données de manière simple et rentable.
- Amazon GuardDuty est un service de surveillance continue de la sécurité.

- AWS IoT Corefournit une communication bidirectionnelle sécurisée pour les appareils connectés à Internet (tels que les capteurs, les actionneurs, les appareils intégrés, les appareils sans fil et les appareils intelligents) pour qu'ils se connectent via MQTT, HTTPS et WAN. AWS Cloud LoRa
- AWS IoT Device Defender est un service de sécurité qui vous permet de vérifier la configuration de vos appareils et de surveiller les appareils connectés afin de détecter les comportements anormaux et d'atténuer les risques liés à la sécurité.
- Amazon OpenSearch Service est un service géré qui facilite le déploiement, l'exploitation et le dimensionnement de OpenSearch clusters dans le AWS Cloud.
- AWS Organizationsest un service de gestion de comptes qui vous permet de consolider plusieurs comptes au Comptes AWS sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Security Hubfournit une vue complète de l'état de votre sécurité AWS et vous aide à vérifier que votre environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.
- Amazon Virtual Private Cloud (Amazon VPC) fournit une section isolée de manière logique dans AWS Cloud laquelle vous pouvez lancer des AWS ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Épopées

Configurez un compte IoT dans votre environnement de zone d'atterrissage

Tâche	Description	Compétences requises
Validez les garde-fous de sécurité du compte IoT.	Vérifiez que les garde-fou s pour CloudTrail, AWS Config GuardDuty, et Security Hub sont activés dans votre compte IoT.	Administrateur AWS
Vérifiez que votre compte IoT est configuré en tant que compte membre de votre compte Security.	Vérifiez que votre compte IoT est configuré et associé en tant que compte membre	Administrateur AWS

Tâche	Description	Compétences requises
	GuardDuty et Security Hub dans votre compte Security. Pour plus d'informations à ce sujet, consultez les GuardDuty sections Gestion des comptes AWS Organizations dans la GuardDuty documentation et Gestion des comptes administrateurs et membres dans la documentation du Security Hub.	
Validez l'archivage des journaux.	Validez cela CloudTrail AWS Config, et les journaux de flux VPC sont stockés dans le compte Log Archive.	Administrateur AWS

Configuration de la solution de journalisation centralisée

Tâche	Description	Compétences requises
Configurez la solution de journalisation centralisée dans votre compte Security.	Connectez-vous au compte AWS Management Console de sécurité et configurez la solution de journalisation centralisée depuis la bibliothèque de AWS solutions pour collecter, analyser et afficher les CloudWatch journaux dans Amazon OpenSearch Service et les OpenSearch tableaux de bord.	Administrateur AWS

Tâche	Description	Compétences requises
	Pour plus d'informations à ce sujet, consultez Collecter, analyser et afficher Amazon CloudWatch Logs dans un tableau de bord unique avec la solution de journalisation centralisée, extrait du guide de mise en œuvre de la journalisation centralisée dans la bibliothèque de AWS solutions.	

Configurez et configurez AWS les ressources de votre compte IoT

Tâche	Description	Compétences requises
Configurez la AWS IoT journalisation.	Connectez-vous à AWS Management Console votre compte IoT. Configurez et configurez AWS IoT Core pour envoyer des CloudWatch journaux à Logs. Pour plus d'informations à ce sujet, voir Configurer la AWS IoT journalisation et surveiller AWS IoT à l'aide CloudWatch des journaux dans la AWS IoT Core documentation.	Administrateur AWS
Configurez AWS IoT Device Defender.	Configurez AWS IoT Device Defender pour auditer vos ressources IoT et détecter les anomalies.	Administrateur AWS

Tâche	Description	Compétences requises
	Pour plus d'informations à ce sujet, consultez Getting started with AWS IoT Device Defender dans la AWS IoT Core documentation.	
Configurez CloudTrail.	Configuré CloudTrail pour envoyer des événements à CloudWatch Logs. Pour plus d'informations à ce sujet, consultez la section Envoi d'événements aux CloudWatch journaux dans la CloudTrail documentation.	Administrateur AWS
Configuration AWS Config et AWS Config règles.	Configuration AWS Config et AWS Config règles requises. Pour plus d'informations à ce sujet, consultez les sections Configuration AWS Config avec la console et Ajout de AWS Config règles dans la AWS Config documentation.	Administrateur AWS

Tâche	Description	Compétences requises
Configurez GuardDuty.	Configurez et configurez GuardDuty pour envoyer les résultats à Amazon CloudWatch Events en ciblant les groupes de CloudWatch journaux dans Logs. Pour plus d'informations à ce sujet, consultez la section Création de réponses personnalisées aux GuardDuty résultats avec Amazon CloudWatch Events dans la GuardDuty documentation.	Administrateur AWS
Configurez Security Hub.	Configurez Security Hub et activez les normes CIS AWS Foundations Benchmark et AWS Foundational Security Best Practices. Pour plus d'informations à ce sujet, consultez la section Réponse et correction automatisées dans la documentation de Security Hub.	Administrateur AWS

Tâche	Description	Compétences requises
Configurez Amazon Detective.	Configurez Detective pour faciliter l'analyse des résultats de sécurité. Pour plus d'informations à ce sujet, consultez Getting started with Amazon Detective dans la documentation Amazon Detective.	Administrateur AWS
Configurez Amazon Athena et. AWS Glue	Configurez Athena et interroge z AWS Glue les Service AWS journaux chargés des enquêtes sur les incidents de sécurité. Pour plus d'informations à ce sujet, consultez la section Interrogation Service AWS des journaux dans la documenta tion Amazon Athena.	Administrateur AWS

Ressources connexes

- Qu'est-ce qu'une zone d'atterrissage ?

Extraire et interroger AWS IoT SiteWise les attributs de métadonnées dans un lac de données

Créée par Ambarish Dongaonkar (AWS)

Récapitulatif

AWS IoT SiteWise utilise des modèles d'actifs et des hiérarchies pour représenter vos équipements industriels, vos processus et vos installations. Chaque modèle ou actif peut avoir plusieurs attributs spécifiques à votre environnement. Les exemples d'attributs de métadonnées incluent le site ou l'emplacement physique de l'actif, les détails de l'usine et les identifiants de l'équipement. Ces valeurs d'attribut complètent les données de mesure des actifs afin de maximiser la valeur commerciale. L'apprentissage automatique (ML) peut fournir des informations supplémentaires sur ces métadonnées et rationaliser les tâches d'ingénierie.

Toutefois, les attributs de métadonnées ne peuvent pas être demandés directement depuis le AWS IoT SiteWise service. Pour rendre les attributs interrogeables, vous devez les extraire et les ingérer dans un lac de données. Ce modèle utilise un script Python pour extraire les attributs de tous les AWS IoT SiteWise actifs et les intégrer dans un lac de données situé dans un bucket Amazon Simple Storage Service (Amazon S3). Une fois ce processus terminé, vous pouvez utiliser des requêtes SQL dans Amazon Athena pour accéder aux attributs de AWS IoT SiteWise métadonnées et à d'autres ensembles de données, tels que les ensembles de données de mesures. Les informations relatives aux attributs de métadonnées sont également utiles lorsque vous travaillez avec des AWS IoT SiteWise moniteurs ou des tableaux de bord. Vous pouvez également créer un QuickSight tableau de bord Amazon en utilisant les attributs extraits dans le compartiment Amazon S3.

Le modèle comporte un code de référence, et vous pouvez implémenter le code en utilisant les meilleurs services de calcul pour votre cas d'utilisation, tels que AWS Lambda ou AWS Glue.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Autorisations pour configurer des AWS Lambda fonctions ou AWS Glue des tâches.
- Un compartiment Amazon S3.

- Les modèles d'actifs et les hiérarchies sont configurés dans AWS IoT SiteWise. Pour plus d'informations, consultez la section Création de modèles d'actifs dans la AWS IoT SiteWise documentation.

Architecture

Vous pouvez utiliser une fonction Lambda ou une AWS Glue tâche pour terminer ce processus. Nous vous recommandons d'utiliser Lambda si vous avez moins de 100 modèles et que chaque modèle possède en moyenne 15 attributs ou moins. Pour tous les autres cas d'utilisation, nous vous recommandons d'utiliser AWS Glue.

L'architecture de la solution et le flux de travail sont illustrés dans le schéma suivant.

1. La AWS Glue tâche planifiée ou la fonction Lambda s'exécute. Il extrait les attributs des métadonnées des actifs AWS IoT SiteWise et les intègre dans un compartiment Amazon S3.
2. Un AWS Glue robot d'exploration explore les données extraites dans le compartiment Amazon S3 et crée des tables dans un. AWS Glue Data Catalog
3. À l'aide du SQL standard, Amazon Athena interroge les tables du. AWS Glue Data Catalog

Automatisation et mise à l'échelle

Vous pouvez planifier l'exécution quotidienne ou hebdomadaire de la fonction ou de la AWS Glue tâche Lambda, en fonction de la fréquence de mise à jour de la configuration de vos AWS IoT SiteWise actifs.

Il n'y a pas de limite au nombre de AWS IoT SiteWise ressources que l'exemple de code peut traiter, mais un grand nombre d'actifs peut augmenter le temps nécessaire pour terminer le processus.

Outils

- Amazon Athena est un service de requête interactif qui vous permet d'analyser les données directement dans Amazon S3 à l'aide du SQL standard.
- AWS Glueest un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS IoT SiteWisevous aide à collecter, modéliser, analyser et visualiser les données des équipements industriels à grande échelle.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

Épopées

Configuration de la tâche ou de la fonction

Tâche	Description	Compétences requises
Configurez les autorisations dans IAM.	Dans la console IAM, accordez des autorisations au rôle IAM assumé par la fonction ou la AWS Glue tâche Lambda pour effectuer les opérations suivantes : • Lire depuis le AWS IoT SiteWise service • Écrire dans le compartiment Amazon S3 Pour plus d'informations, consultez la section Création d'un rôle pour un Service AWS dans la documentation IAM.	AWS général

Tâche	Description	Compétences requises
Créez la fonction ou AWS Glue la tâche Lambda.	Si vous utilisez Lambda, créez une nouvelle fonction Lambda. Pour Runtime, choisissez Python. Pour plus d'informations, consultez la section Création de fonctions Lambda avec Python dans la documentation Lambda. Si vous en utilisez AWS Glue, créez une nouvelle tâche shell Python dans la AWS Glue console. Pour plus d'informations, consultez la section Ajout de tâches shell Python dans la AWS Glue documentation.	AWS général
Mettez à jour la fonction ou AWS Glue la tâche Lambda.	Modifiez la nouvelle fonction ou AWS Glue tâche Lambda et entrez l'exemple de code dans la section Informations supplémentaires. Modifiez le code en fonction de votre cas d'utilisation. Pour plus d'informations, voir Modifier le code à l'aide de l'éditeur de console dans la documentation Lambda et voir Utilisation de scripts dans la AWS Glue documentation.	AWS général

Exécuter le job ou la fonction

Tâche	Description	Compétences requises
Exécutez la fonction ou AWS Glue le job Lambda.	Exécutez la fonction ou AWS Glue le job Lambda. Pour plus d'informations, consultez Invoke the Lambda function dans la documentation Lambda ou consultez Starting jobs using triggers dans la documentation. AWS Glue Cela extrait les attributs de métadonnées pour les actifs et les modèles de la AWS IoT SiteWise hiérarchie et les stocke dans le compartiment Amazon S3 spécifié.	AWS général
Configurez un AWS Glue robot d'exploration.	Configurez un AWS Glue robot avec le classificateur de format nécessaire pour un fichier au format CSV. Utilisez les détails du compartiment et du préfixe Amazon S3 utilisés dans la fonction AWS Glue ou la tâche Lambda. Pour plus d'informations, consultez la section Définition des robots d'exploration dans la AWS Glue documentation.	AWS général
Lancez le AWS Glue crawler.	Exécutez le robot d'exploration pour traiter le fichier de données créé par la fonction AWS Glue ou la tâche Lambda. Le robot crée une	AWS général

Tâche	Description	Compétences requises
	table dans le champ spécifié AWS Glue Data Catalog. Pour plus d'informations, consultez la section Démarrage de robots d'exploration à l'aide de déclencheurs dans la AWS Glue documentation.	
Interrogez les attributs des métadonnées.	À l'aide d'Amazon Athena, utilisez le code SQL standard pour effectuer les AWS Glue Data Catalog requêtes nécessaires à votre cas d'utilisation. Vous pouvez joindre la table attributaire des métadonnées à d'autres bases de données et tables. Pour plus d'informations, consultez Getting Started dans la documentation Amazon Athena.	AWS général

Ressources connexes

- Documentation Amazon Athena
- AWS Glue documentation
- AWS IoT SiteWise Référence d'API
- AWS IoT SiteWise guide de l'utilisateur
  - Premiers pas
  - Modélisation des actifs industriels
  - Définition des relations entre les modèles d'actifs (hiérarchies)
  - Associer et dissocier des actifs
  - Création de la AWS IoT SiteWise démo

- IOTSiteWise (SDK pour la documentation Python)
- Documentation Lambda

Informations supplémentaires

Code

L'exemple de code fourni est fourni à titre de référence, et vous pouvez personnaliser ce code selon vos besoins en fonction de votre cas d'utilisation.

```
# Following code can be used in an AWS Lambda function or in an AWS Glue Python shell
 job.
# IAM roles used for this job need read access to the AWS IoT SiteWise service and
 write access to the S3 bucket.
sw_client = boto3.client('iotsitewise')
s3_client = boto3.client('s3')
output = io.StringIO()

attribute_list=[]
bucket = '{3_bucket name}'
prefix = '{s3_bucket prefix}'
output.write("model_id,model_name,asset_id,asset_name,attribuet_id,attribute_name,attribute_val
\n")

m_resp = sw_client.list_asset_models()
for m_rec in m_resp['assetModelSummaries']:
     model_id = m_rec['id']
     model_name = m_rec['name']

     attribute_list.clear()
     dam_response = sw_client.describe_asset_model(assetModelId=model_id)
     for rec in dam_response['assetModelProperties']:
         if 'attribute' in rec['type']:
            attribute_list.append(rec['name'])

     response = sw_client.list_assets(assetModelId=model_id, filter='ALL')
     for asset in response['assetSummaries']:
         asset_id = asset['id']
         asset_name = asset['name']
         resp = sw_client.describe_asset(assetId=asset_id)
         for rec in resp['assetProperties']:
            if rec['name'] in attribute_list:
```

```
                p_resp = sw_client.get_asset_property_value(assetId=asset_id,
 propertyId=rec['id'])
                if 'propertyValue' in p_resp:
                    if p_resp['propertyValue']['value']:
                        if 'stringValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['stringValue']) + "\n")

                        if 'doubleValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['doubleValue']) + "\n")
                        if 'integerValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['integerValue']) + "\n")
                         if 'booleanValue' in p_resp['propertyValue']['value']:
                             output.write(model_id + "," + model_name + ","
 + asset_id + "," + asset_name + "," + rec['id'] + "," + rec['name'] + "," +
 str(p_resp['propertyValue']['value']['booleanValue']) + "\n")

output.seek(0)
s3_client.put_object(Bucket=bucket, Key= prefix + '/data.csv', Body=output.getvalue())
output.close()
```

Configuration et résolution des problèmes liés à AWS IoT Greengrass avec des appareils clients

Créée par Marouane Sefiani et Akalanka De Silva (AWS)

Récapitulatif

AWS IoT Greengrass est un environnement d'exécution périphérique et un service cloud open source permettant de créer, de déployer et de gérer des logiciels Internet des objets (IoT) sur des appareils périphériques. Les cas d'utilisation d'AWS IoT Greengrass incluent :

- Maisons intelligentes dans lesquelles une passerelle AWS IoT Greengrass est utilisée comme hub pour la domotique
- Des usines intelligentes dans lesquelles AWS IoT Greengrass peut faciliter l'ingestion et le traitement local des données depuis l'atelier

AWS IoT Greengrass peut agir en tant que point de terminaison de connexion MQTT sécurisé et authentifié pour d'autres appareils périphériques (également appelés appareils clients), qui autrement se connecteraient généralement directement à AWS IoT Core. Cette fonctionnalité est utile lorsque les appareils clients ne disposent pas d'un accès réseau direct au point de terminaison AWS IoT Core.

Vous pouvez configurer AWS IoT Greengrass pour une utilisation avec des appareils clients dans les cas d'utilisation suivants :

- Pour que les appareils clients puissent envoyer des données à AWS IoT Greengrass
- Pour qu'AWS IoT Greengrass transmette les données à AWS IoT Core
- Pour tirer parti des fonctionnalités avancées du moteur de règles AWS IoT Core

Ces fonctionnalités nécessitent l'installation et la configuration des composants suivants sur l'appareil AWS IoT Greengrass :

- courtier MQTT
- Pont MQTT
- Authentification de l'appareil client
- Détecteur IP

En outre, les messages publiés depuis les appareils clients doivent être au format JSON ou au format Protocol Buffers (protobuf).

Ce modèle décrit comment installer et configurer ces composants requis, et fournit des conseils de dépannage et les meilleures pratiques.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI) version 2
- Deux appareils clients exécutant Python 3.7 ou version ultérieure
- Un appareil principal exécutant Java Runtime Environment (JRE) version 8 ou ultérieure, et Amazon Corretto 11 ou OpenJDK 11

Limites

- Vous devez choisir une région AWS dans laquelle AWS IoT Core est disponible. Pour consulter la liste actuelle des régions pour AWS IoT Core, consultez la section Services AWS par région.
- Le périphérique principal doit disposer d'au moins 172 Mo de RAM et 512 Mo d'espace disque.

Architecture

Le schéma suivant montre l'architecture de la solution pour ce modèle.

L'architecture inclut :

- Deux appareils clients. Chaque appareil contient une clé privée, un certificat de périphérique et un certificat d'autorité de certification (CA) racine. Le SDK pour appareils AWS IoT, qui contient un client MQTT, est également installé sur chaque appareil client.
- Un appareil principal sur lequel AWS IoT Greengrass a été déployé avec les composants suivants :
  - courtier MQTT
  - Pont MQTT
  - Authentification de l'appareil client

- Détecteur IP

Cette architecture prend en charge les scénarios suivants :

- Les appareils clients peuvent utiliser leur client MQTT pour communiquer entre eux via le broker MQTT du périphérique principal.
- Les appareils clients peuvent également communiquer avec AWS IoT Core dans le cloud via le broker MQTT de l'appareil principal et le pont MQTT.
- AWS IoT Core dans le cloud peut envoyer des messages aux appareils clients via le client de test MQTT, le pont MQTT et le courtier MQTT de l'appareil principal.

Pour plus d'informations sur les communications entre les appareils clients et le périphérique principal, consultez la section Informations supplémentaires.

Outils

Services AWS

- AWS IoT Greengrass est un environnement d'exécution périphérique et un service cloud open source pour l'Internet des objets (IoT) qui vous aide à créer, déployer et gérer des applications IoT sur vos appareils.
- AWS IoT Core fournit une communication bidirectionnelle sécurisée permettant aux appareils connectés à Internet de se connecter au cloud AWS.
- Le SDK pour appareils AWS IoT est un kit de développement logiciel qui comprend des bibliothèques open source, des guides de développement avec des exemples et des guides de portage afin que vous puissiez créer des produits ou des solutions IoT innovants sur les plateformes matérielles de votre choix.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

Bonnes pratiques

- La charge utile des messages provenant des appareils clients doit être au format JSON ou Protobuf afin de tirer parti des fonctionnalités avancées du moteur de règles AWS IoT Core, telles que la transformation et les actions conditionnelles.

- Configurez le pont MQTT pour autoriser la communication bidirectionnelle.
- Configurez et déployez le composant de détection IP dans AWS IoT Greengrass pour vous assurer que les adresses IP de l'appareil principal sont incluses dans le champ du nom alternatif du sujet (SAN) du certificat de courtier MQTT.

Épopées

Configuration de l'appareil principal

Tâche	Description	Compétences requises
Configurez AWS IoT Greengrass sur votre appareil principal.	Installez le logiciel AWS IoT Greengrass Core en suivant les instructions du guide du développeur.	AWS IoT Greengrass

Vérifiez l'état de votre installation.	Utilisez la commande suivante pour vérifier l'état du service AWS IoT Greengrass sur votre appareil principal :
	`sudo systemctl status greengrass.service`
	Le résultat attendu de la commande est le suivant :
	`Launched Nucleus successfully`
		AWS général

Configurez une politique IAM et associez-la au rôle de service Greengrass.	1. Créez une politique IAM pour autoriser les communications vers et depuis le pont MQTT. Voici un exemple de politique : `{`	AWS général

Tâche	Description	Compétences requises
	<pre> "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iot:*"], "Resource": "*" }, { "Sid": "GreengrassActions", "Effect": "Allow", "Action": ["greengrass:*"], "Resource": "*" }] }</pre> 2. Associez la politique au rôle de service Greengrass. Pour obtenir le rôle de service, utilisez la commande suivante : <pre>aws greengrassv2 get-service-role-f</pre>	

Tâche	Description	Compétences requises
	`or-account --region <region>` où `<region>` fait référence à votre région AWS.	
Configurez et déployez les composants requis dans le dispositif principal AWS IoT Greengrass.	Configurez et déployez les composants suivants : • `greengrass.clientdevices.mqtt.Moquette` (voir les détails de configuration) • `greengrass.clientdevices.mqtt.Bridge` (voir les détails de configuration et la tâche suivante) • `greengrass.clientdevices.Auth` (voir les détails de configuration et la tâche après la suivante) • `aws.greengrass.clientdevices.IPDetector` (voir les détails de configuration)	AWS IoT Greengrass

Tâche	Description	Compétences requises
Vérifiez que le pont MQTT autorise la communication bidirectionnelle.	Pour relayer des messages MQTT entre les appareils clients et AWS IoT Core, configurez et déployez le composant du pont MQTT et spécifiez les sujets à relayer. Voici un exemple : `{ "mqttTopicMapping": { "ClientDevicesToCloud": { "topic": "dt/#", "source": "LocalMqtt", "target": "IotCore" }, "CloudToClientDevices": { "topic": "cmd/#", "source": "IotCore", "target": "LocalMqtt" } } }`	AWS IoT Greengrass

Tâche	Description	Compétences requises
Vérifiez que le composant d'authentification permet aux appareils clients de se connecter et de publier des sujets ou de s'y abonner.	La `aws.greengrass.clientdevices.Auth` configuration suivante permet à tous les appareils clients de se connecter, de publier des messages et de s'abonner à toutes les rubriques. `{ "deviceGroups": { "formatVersion": "2021-03-05", "definitions": { "MyPermissiveDeviceGroup": { "selectionRule": "thingName: *", "policyName": "MyPermissivePolicy" } }, "policies": { "MyPermissivePolicy": { "AllowAll": { "statementDescription": "Allow client devices to perform all actions.", "operations": ["*"], "resources": ["*"] } }`	AWS IoT Greengrass

Tâche	Description	Compétences requises

	<pre>}
	}
	}</pre>	

Configuration des appareils clients

Tâche	Description	Compétences requises
Installez le SDK pour appareils AWS IoT.	Installez le SDK pour appareils AWS IoT sur les appareils clients. Pour obtenir la liste complète des langues prises en charge et des langues associées SDKs, consultez la documentation AWS IoT Core. Par exemple, le SDK pour appareils AWS IoT pour Python se trouve sur. GitHub Pour installer ce SDK : 1. Vérifiez que Python 3.7 ou version ultérieure est installé, comme indiqué sur la page Prérequis du GitHub référentiel. 2. Utilisez la commande pip pour installer le SDK. Pour macOS et Linux : <pre>python3 -m pip install awsiotsdk</pre> Pour Windows :	AWS IoT général

Tâche	Description	Compétences requises

	`python -m pip install awsiotsdk`
	
	Vous pouvez également installer le SDK à partir du référentiel source :
	
	`# Create a workspace directory to hold all the SDK files`
	`mkdir sdk-workspace`
	`cd sdk-workspace`
	`# Clone the repository`
	`git clone https://github.com/aws/aws-iot-device-sdk-python-v2.git`
	`# Install using Pip (use 'python' instead of 'python3' on Windows)`
	`python3 -m pip install ./aws-iot-device-sdk-python-v2`	

Tâche	Description	Compétences requises
Créez quelque chose.	1. Dans la console AWS IoT, si un bouton Get started apparaît, choisissez-le. Sinon, dans le volet de navigation, choisissez Security, Policies. 2. Si la boîte de dialogue Vous n'avez pas encore de politique apparaît, choisissez Créer une politique. Sinon, cliquez sur Create. 3. Entrez un nom pour la politique AWS IoT (par exemple,`ClientDevicePolicy`). 4. Dans la section Ajouter des instructions, remplacez la politique existante par le code JSON suivant. Remplacez `<region>` et `<account>` par votre région AWS et votre numéro de compte AWS. `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "iot:Connect", "Resource": "arn:aws:iot:region:account:client/*" },`	AWS IoT Core

Tâche	Description	Compétences requises

	{
	"Effect": "Allow",
	"Action": "iot:Publish",
	"Resource": "*"
	},
	{
	"Effect": "Allow",
	"Action": "iot:Receive",
	"Resource": "*"
	},
	{
	"Effect": "Allow",
	"Action": "iot:Subscribe",
	"Resource": "*"
	},
	{
	"Effect": "Allow",
	"Action": [
	"iot:GetThingShadow",
	"iot:UpdateThingShadow",
	"iot:DeleteThingShadow"
	],
	"Resource": "arn:aws:iot:region:account:thing/*"
	
	}
	]	

Tâche	Description	Compétences requises
	<pre>}</pre> 5. Choisissez Créer. 6. Sur la console AWS IoT, dans le volet de navigation, choisissez Manage, Things. 7. Si la boîte de dialogue Vous n'avez encore rien s'affiche , choisissez Enregistrer un objet. Sinon, cliquez sur Create. 8. Sur la page Creating AWS IoT things (Création d'objets AWS IoT), choisissez Create a single thing (Créer un objet unique). 9. Sur la page Add your device to the device registry (Ajouter votre appareil au registre des appareils), entrez un nom pour votre objet IoT (par exemple, `ClientDevice1`), puis choisissez Next (Suivant). **Note** Vous ne pouvez pas modifier le nom d'un objet après l'avoir créé. Pour changer le nom, vous devez créer un nouvel objet, lui donner le	

Tâche	Description	Compétences requises
	nouveau nom, puis supprimer l'ancien. 10. Sur la page Add a certificate for your thing (Ajouter un certificat pour votre objet), choisissez Create certificate (Créer un certificat). 11. Choisissez les liens Télécharger pour télécharger le certificat, la clé privée et le certificat CA racine. **Important** Il s'agit de votre seule opportunité de télécharger votre certificat et votre clé privée. 12. Choisissez Activer pour activer votre certificat. Le certificat doit être actif pour qu'un appareil puisse se connecter à AWS IoT. 13. Choisissez Attacher une stratégie. 14. Pour Ajouter une politique pour votre objet ClientDevicePolicy, choisissez Enregistrer l'objet.	

Tâche	Description	Compétences requises
Téléchargez le certificat CA depuis l'appareil principal de Greengrass.	Si vous vous attendez à ce que le périphérique principal de Greengrass fonctionne dans des environnements hors ligne, vous devez mettre le certificat de base de CA de Greengrass à la disposition de l'appareil client afin qu'il puisse vérifier le certificat du courtier MQTT (qui est émis par l'autorité de certification principale de Greengrass). Il est donc important d'obtenir une copie de ce certificat. Utilisez l'une des méthodes suivantes pour télécharger le certificat CA : • Si vous avez accès au réseau à l'appareil AWS IoT Greengrass depuis votre PC, entrez `https://<device IP>:8883` dans votre navigateur Web et consultez le certificat du courtier MQTT et le certificat CA. Vous pouvez également enregistrer le certificat CA sur l'appareil client. • Vous pouvez également utiliser la ligne de commande OpenSSL :	AWS général

Tâche	Description	Compétences requises
	`openssl s_client -showcerts -connect <device IP>:8883`	
Copiez les informations d'identification sur les appareils clients.	Copiez le certificat CA principal de Greengrass, le certificat de l'appareil et la clé privée dans les appareils clients.	AWS général

Tâche	Description	Compétences requises
Associez les appareils clients au périphérique principal.	Associez les appareils clients à un périphérique principal afin qu'ils puissent découvrir le périphérique principal. Les appareils clients peuvent ensuite utiliser l'API de découverte Greengrass pour récupérer les informations de connectivité et les certificats pour leurs appareils principaux associés. Pour plus d'informations, consultez Associer des appareils clients dans la documentation AWS IoT Greengrass. 1. Sur la console AWS IoT Greengrass, sélectionnez les appareils Core. 2. Choisissez l'appareil principal à gérer. 3. Sur la page de détails de l'appareil principal, choisissez l'onglet Appareils clients. 4. Dans la section Appareils clients associés, choisissez Associer les appareils clients. 5. Dans le mode Associer les appareils clients au périphérique principal, procédez comme suit pour	AWS IoT Greengrass

Tâche	Description	Compétences requises
	chaque appareil client à associer : a. Entrez le nom de l'objet AWS IoT à associer en tant qu'appareil client. b. Choisissez Ajouter. 6. Choisissez Associer. Les appareils clients que vous avez associés peuvent désormais utiliser l'API de découverte Greengrass pour découvrir cet appareil principal .	

Envoyer et recevoir des données

Tâche	Description	Compétences requises
Envoyez des données d'un appareil client à un autre appareil client.	Utilisez le client MQTT de votre appareil pour publier un message sur le `dt/client 1/sensor` sujet.	AWS général
Envoyez des données depuis l'appareil client vers AWS IoT Core.	Utilisez le client MQTT de votre appareil pour publier un message sur le `dt/client 1/sensor` sujet. Dans le client de test MQTT, abonnez-vous au sujet sur lequel l'appareil envoie des messages ou abonnez-vous	AWS général

Tâche	Description	Compétences requises
	à # pour tous les sujets (voir détails).	
Envoyez des messages depuis AWS IoT Core aux appareils clients.	Sur la page du client de test MQTT, dans l'onglet Publier dans un sujet, dans le champ Nom du sujet, entrez le nom du sujet de votre message. Dans cet exemple, utilisez `cmd/client1` pour le sujet.	AWS général

Résolution des problèmes

Problème	Solution
Impossible de vérifier l'erreur du certificat du serveur	Cette erreur se produit lorsque le client MQTT ne peut pas vérifier le certificat présenté par le courtier MQTT lors de la prise de contact TLS. La raison la plus courante est que le client MQTT ne possède pas le certificat CA. Suivez ces étapes pour vous assurer que le certificat CA est fourni au client MQTT. 1. Si vous avez accès au réseau à l'appareil AWS IoT Greengrass depuis votre PC, entrez `https://<device IP>:8883` dans une fenêtre de navigateur pour voir le certificat du courtier MQTT et le certificat CA. Vous pouvez également enregistrer le certificat CA sur l'appareil client. Vous pouvez également utiliser la ligne de commande OpenSSL :

Problème	Solution
	``` openssl s_client -showcerts -connect <device IP>:8883 ``` 2. Enregistrez le contenu des certificats Moquette CA et Greengrass Core CA dans des fichiers, puis visualisez le contenu décodé à l'aide de la commande : ``` openssl x509 -in <Name of CA>.pem - text ``` Le certificat Moquette CA doit afficher le champ SAN comme dans cet exemple : ``` X509v3 Subject Alternative Name: IP Address:XXX.XXX.XXX.XXX, IP Address:127.0.0.1, DNS:localhost ```
Impossible de vérifier l'erreur du nom du serveur	Cette erreur se produit lorsque le client MQTT ne parvient pas à vérifier qu'il se connecte au bon serveur. La raison la plus courante est que l'adresse IP de l'appareil Greengrass n'est pas répertoriée dans le champ SAN du certificat. Suivez les instructions de la solution précédent e pour obtenir le certificat de courtier MQTT et vérifier que le champ SAN contient l'adresse IP de l'appareil AWS IoT Greengrass, comme expliqué dans la section Informati ons supplémentaires. Si ce n'est pas le cas, vérifiez que le composant du détecteur IP est correctement installé et redémarrez le périphéri que principal.

Problème	Solution
Impossible de vérifier le nom du serveur uniquement lors de la connexion à partir d'un appareil client intégré	Mbed TLS, qui est une bibliothèque TLS populaire utilisée dans les appareils embarqués , prend actuellement en charge la vérification du nom DNS uniquement dans le champ SAN du certificat, comme indiqué dans le code de la bibliothèque Mbed TLS. Comme le périphéri que principal ne possède pas son propre nom de domaine et dépend de l'adresse IP, les clients TLS qui utilisent Mbed TLS échoueron t à la vérification du nom du serveur lors de la prise de contact TLS, ce qui provoquera un échec de connexion. Nous vous recommand ons d'ajouter la vérification de l'adresse IP du SAN à votre bibliothèque TLS Mbed via la fonction x509_crt_check_san.

Ressources connexes

- Documentation AWS IoT Greengrass
- Documentation de base d'AWS IoT Core
- Composant du broker MQTT
- composant de pont MQTT
- Composant d'authentification de l'appareil client
- composant du détecteur IP
- Kits de développement logiciel pour appareils AWS IoT
- Implémentation d'appareils clients locaux avec AWS IoT Greengrass (article de blog AWS)
- RFC 5280 — Certificat d'infrastructure à clé publique Internet X.509 et profil de liste de révocation de certificats (CRL)

Informations supplémentaires

Cette section fournit des informations supplémentaires sur les communications entre les appareils clients et le périphérique principal.

Le broker MQTT écoute une tentative de connexion client TLS sur le port 8883 du périphérique principal. L'illustration suivante montre un exemple de certificat de serveur du courtier MQTT.

L'exemple de certificat affiche les détails suivants :

- Le certificat est délivré par l'autorité de certification AWS IoT Greengrass Core, qui est locale et spécifique à l'appareil principal, c'est-à-dire qu'elle agit en tant qu'autorité de certification locale.
- Ce certificat est automatiquement modifié chaque semaine par le composant d'authentification du client, comme indiqué dans l'illustration suivante. Vous pouvez définir cet intervalle dans la configuration du composant d'authentification du client.

- Le nom alternatif du sujet (SAN) joue un rôle essentiel dans la vérification du nom du serveur côté client TLS. Cela permet au client TLS de s'assurer qu'il se connecte au bon serveur et d'éviter les man-in-the-middle attaques lors de la configuration de la session TLS. Dans l'exemple de certificat, le champ SAN indique que ce serveur écoute sur localhost (le socket de domaine Unix local) et que l'interface réseau possède l'adresse IP 192.168.1.12.

Le client TLS utilise le champ SAN du certificat pour vérifier qu'il se connecte à un serveur légitime lors de la vérification du serveur. En revanche, lors d'une prise de contact TLS classique entre un serveur HTTP et un navigateur, le nom de domaine figurant dans le champ nom commun (CN) ou dans le champ SAN est utilisé pour vérifier le domaine auquel le navigateur se connecte réellement pendant le processus de vérification du serveur. Si le périphérique principal n'a pas de nom de domaine, l'adresse IP incluse dans le champ SAN a le même objectif. Pour plus d'informations, consultez la section Nom alternatif du sujet de la RFC 5280 — Profil du certificat d'infrastructure à clé publique Internet X.509 et de la liste de révocation des certificats (CRL).

Le composant détecteur d'adresses IP d'AWS IoT Greengrass garantit que les adresses IP correctes sont incluses dans le champ SAN du certificat.

Dans l'exemple, le certificat est signé par l'appareil AWS IoT Greengrass agissant en tant qu'autorité de certification locale. Le client TLS (client MQTT) n'est pas au courant de l'existence de cette autorité de certification. Nous devons donc fournir un certificat de certification semblable au suivant.

Plus de modèles

- Ingérez de manière rentable des données IoT directement dans Amazon S3 à l'aide d'AWS IoT Greengrass

Migration et modernisation

Rubriques

- Migration
- Modernisation
- ordinateurs centraux

Migration

Rubriques

- Création de CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel et Python
- Commencez par la découverte automatique de portefeuilles
- Migrez les charges de travail Cloudera sur site vers Cloudera Data Platform sur AWS
- Résoudre les erreurs de connexion après la migration de Microsoft SQL Server vers le cloud AWS
- Redémarrez automatiquement l'agent de réplication AWS sans le désactiver SELinux après le redémarrage d'un serveur source RHEL
- Ré-architecte
- Réhéberger
- Déménager
- Recréation de plateforme
- Schémas de migration par charge de travail
- Plus de modèles

Création de CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel et Python

Créée par Venkata Naveen Koppula (AWS)

Récapitulatif

Ce modèle décrit les étapes de création automatique de CloudFormation modèles AWS pour AWS Database Migration Service (AWS DMS) à l'aide de Microsoft Excel et Python.

La migration de bases de données à l'aide d'AWS DMS implique souvent la création de CloudFormation modèles AWS pour provisionner les tâches AWS DMS. Auparavant, la création de CloudFormation modèles AWS nécessitait la connaissance du langage de programmation JSON ou YAML. Avec cet outil, vous n'avez besoin que de connaissances de base sur Excel et sur la façon d'exécuter un script Python à l'aide d'un terminal ou d'une fenêtre de commande.

En entrée, l'outil utilise un classeur Excel qui inclut les noms des tables à migrer, les Amazon Resource Names (ARNs) des points de terminaison AWS DMS et les instances de réplication AWS DMS. L'outil génère ensuite des CloudFormation modèles AWS pour les tâches AWS DMS requises.

Pour obtenir des étapes détaillées et des informations générales, consultez le billet de blog Créer des CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel sur le blog de base de données AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Microsoft Excel version 2016 ou ultérieure
- Python version 2.7 ou ultérieure
- Le module Python xlrd (installé à l'invite de commande avec la commande : pip install xlrd)
- Points de terminaison source et cible AWS DMS et instance de réplication AWS DMS

Limites

- Les noms des schémas, des tables et des colonnes associées sont transformés en minuscules sur les points de terminaison de destination.

- Cet outil ne traite pas de la création de points de terminaison et d'instances de réplication AWS DMS.
- Actuellement, l'outil ne prend en charge qu'un seul schéma pour chaque tâche AWS DMS.

Architecture

Pile technologique source

- Une base de données sur site
- Microsoft Excel

Pile technologique cible

- CloudFormation Modèles AWS
- Une base de données dans le cloud AWS

Architecture

Outils

- Pycharm IDE, ou tout environnement de développement intégré (IDE) supportant la version 3.6 de Python
- Microsoft Office 2016 (pour Microsoft Excel)

Épopées

Configuration du réseau, de l'instance de réplication AWS DMS et des points de terminaison

Tâche	Description	Compétences requises
Si nécessaire, demandez une augmentation du quota de service.	Demandez une augmentation du quota de service pour les tâches AWS DMS si nécessaire.	AWS général

Tâche	Description	Compétences requises
Configurez la région AWS, les clouds privés virtuels (VPCs), les plages d'adresses CIDR, les zones de disponibilité et les sous-réseaux.		AWS général
Configurez l'instance de réplication AWS DMS.	L'instance de réplication AWS DMS peut se connecter à la fois aux bases de données sur site et aux bases de données AWS.	AWS général
Configurez les points de terminaison AWS DMS.	Configurez les points de terminaison pour les bases de données source et cible.	AWS général

Préparation des feuilles de travail pour les tâches et les balises AWS DMS

Tâche	Description	Compétences requises
Configurez la liste des tables.	Répertoriez toutes les tables impliquées dans la migration.	Base de données
Préparez la feuille de travail des tâches.	Préparez la feuille de calcul Excel à l'aide de la liste de tableaux que vous avez configurée.	AWS, Microsoft Excel en général
Préparez la feuille de travail sur les balises.	Détaillez les balises de ressources AWS à associer aux tâches AWS DMS.	AWS, Microsoft Excel en général

Téléchargez et exécutez l'outil

Tâche	Description	Compétences requises
Téléchargez et extrayez l'outil de génération de modèles depuis le GitHub référentiel.	GitHub référentiel : https://github.com/aws-samples/dms-cloudformation-templates-generator/	
Exécutez l'outil.	Suivez les instructions détaillées figurant dans le billet de blog répertorié sous « Références et aide ».	

Ressources connexes

- Création de CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel (article de blog)
- Générateur de CloudFormation modèles DMS (GitHub référentiel)
- Documentation Python
- Description et téléchargement du xlrd
- Documentation AWS DMS
- CloudFormation Documentation AWS

Commencez par la découverte automatique de portefeuilles

Créée par Pratik Chunawala (AWS) et Rodolfo Jr. Cerrada (AWS)

Récapitulatif

L'évaluation du portefeuille et la collecte de métadonnées constituent un défi crucial lors de la migration d'applications et de serveurs vers le cloud Amazon Web Services (AWS), en particulier pour les migrations de grande envergure impliquant plus de 300 serveurs. L'utilisation d'un outil de découverte automatique du portefeuille peut vous aider à collecter des informations sur vos applications, telles que le nombre d'utilisateurs, la fréquence d'utilisation, les dépendances et les informations sur l'infrastructure de l'application. Ces informations sont essentielles lors de la planification des vagues de migration afin de pouvoir hiérarchiser et regrouper correctement les applications présentant des caractéristiques similaires. L'utilisation d'un outil de découverte rationalise la communication entre l'équipe du portefeuille et les propriétaires de l'application, car l'équipe du portefeuille peut valider les résultats de l'outil de découverte plutôt que de collecter manuellement les métadonnées. Ce modèle décrit les principales considérations relatives à la sélection d'un outil de découverte automatique et fournit des informations sur la manière de le déployer et de le tester dans votre environnement.

Ce modèle inclut un modèle, qui constitue un point de départ pour créer votre propre liste d'activités de haut niveau. À côté de la liste de contrôle se trouve un modèle pour une matrice responsable, responsable, consultée et informée (RACI). Vous pouvez utiliser cette matrice RACI pour déterminer qui est responsable de chaque tâche de votre liste de contrôle.

Épopées

Sélectionnez un outil de découverte

Tâche	Description	Compétences requises
Déterminez si un outil de découverte convient à votre cas d'utilisation.	Un outil de découverte n'est peut-être pas la meilleure solution pour votre cas d'utilisation. Tenez compte du temps nécessaire pour sélectionner, acquérir, préparer et déployer un outil de découverte. La	Responsable de la migration, ingénieur de migration

Tâche	Description	Compétences requises
	configuration de l'applian ce de numérisation pour un outil de découverte sans agent dans votre environne ment ou l'installation d'agents sur toutes les charges de travail concernées peuvent prendre de 4 à 8 semaines. Une fois déployé, vous devez prévoir 4 à 12 semaines pour que l'outil de découverte collecte les métadonnées en analysant les charges de travail des applications et en effectuant une analyse de la pile d'applications. Si vous migrez moins de 100 serveurs, vous pourrez peut-être collecter manuellem ent les métadonnées et analyser les dépendances plus rapidement que le temps nécessaire au déploiement et à la collecte des métadonnées à l'aide d'un outil de découvert e automatique.	

Tâche	Description	Compétences requises
Sélectionnez un outil de découverte.	Consultez les considérations relatives à la sélection d'un outil de découverte automatique dans la section Informations supplémentaires. Déterminez les critères appropriés pour sélectionner un outil de découverte adapté à votre cas d'utilisation, puis évaluez chaque outil en fonction de ces critères. Pour une liste complète des outils de découverte automatisés, consultez la section Outils de migration de découverte, de planification et de recommandation.	Responsable de la migration, ingénieur de migration

Préparer l'installation

Tâche	Description	Compétences requises
Préparez la liste de contrôle préalable au déploiement.	Créez une liste des tâches que vous devez effectuer avant de déployer l'outil. Par exemple, consultez la liste de contrôle préalable au déploiement sur le site Web de documentation de Flexera.	Responsable du développement, ingénieur de migration, responsable de la migration, administrateur réseau
Préparez les exigences du réseau.	Fournissez les ports, les protocoles, les adresses IP et le routage nécessaires à l'exécution de l'outil	Ingénieur en migration, Administrateur réseau, Architecte cloud

Tâche	Description	Compétences requises
	et à l'accès aux serveurs cibles. Pour plus d'informations, consultez le guide d'installation de votre outil de découverte. Par exemple, consultez les exigences de déploiement sur le site Web de documentation de Flexera.	
Préparez les exigences relatives au compte et aux informations d'identification.	Identifiez les informations d'identification dont vous avez besoin pour accéder aux serveurs cibles et pour installer tous les composants de l'outil.	Administrateur cloud, AWS général, ingénieur en migration, responsable de la migration, administrateur réseau, administrateur AWS
Préparez les appareils sur lesquels vous allez installer l'outil.	Assurez-vous que les appareils sur lesquels vous allez installer les composants de l'outil répondent aux spécifications et aux exigences de plate-forme de l'outil.	Ingénieur en migration, responsable de la migration, administrateur réseau
Préparez les ordres de changement.	Selon le processus de gestion des modifications de votre organisation, préparez les ordres de modification nécessaires et assurez-vous que ces ordres de modification sont approuvés.	Responsable de la création, responsable de la migration

Tâche	Description	Compétences requises
Envoyez les exigences aux parties prenantes.	Envoyez la liste de contrôle préalable au déploiement et les exigences du réseau aux parties prenantes. Les parties prenantes doivent examiner, évaluer et préparer les exigences nécessair es avant de procéder au déploiement.	Responsable de la création, responsable de la migration

Déployer l'outil

Tâche	Description	Compétences requises
Téléchargez le programme d'installation.	Téléchargez le programme d'installation ou l'image de la machine virtuelle. Les images de machines virtuelles sont généralement disponibles au format OVF (Open Virtualiz ation Format).	Responsable de la création, responsable de la migration
Extrayez les fichiers.	Si vous utilisez un programme d'installation, vous devez le télécharger et l'exécuter sur un serveur local.	Responsable de la création, responsable de la migration
Déployez l'outil sur les serveurs.	Déployez l'outil de découverte sur les serveurs locaux cibles comme suit : • Si votre fichier source est une image de machine virtuelle, déployez-la dans votre environnement de	Responsable du développe ment, responsable de la migration, administrateur réseau

Tâche	Description	Compétences requises
	machine virtuelle, par exemple VMware. • Si votre fichier source est un programme d'installation, exécutez-le pour installer et configurer l'outil.	
Connectez-vous à l'outil de découverte.	Suivez les instructions qui s'affichent à l'écran et connectez-vous pour commencer à utiliser l'outil.	Responsable de la migration, responsable de la construction
Activez le produit.	Entrez votre clé de licence.	Responsable de la création, responsable de la migration
Configurez l'outil.	Entrez les informations d'identification nécessaires pour accéder aux serveurs cibles, telles que les informations d'identification pour Windows VMware, le protocole SNMP (Simple Network Management Protocol) et le protocole Secure Shell (SSH), ou les bases de données.	Responsable de la création, responsable de la migration

Testez l'outil

Tâche	Description	Compétences requises
Sélectionnez les serveurs de test.	Identifiez un petit ensemble de sous-réseaux ou d'adresses IP non liés à la production que vous pouvez utiliser pour	Responsable du développement, responsable de la migration, administrateur réseau

Tâche	Description	Compétences requises
	tester l'outil de découverte. Cela vous permet de valider rapidement les scans, d'identifier et de corriger rapidement les erreurs, et d'isoler vos tests des environnements de production.	
Commencez à scanner les serveurs de test sélectionnés.	Pour un outil de découverte sans agent, entrez les sous-réseaux ou les adresses IP des serveurs de test sélectionnés dans la console de l'outil de découverte, puis lancez l'analyse. Pour un outil de découverte basé sur un agent, installez l'agent sur les serveurs de test sélectionnés.	Responsable du développement, responsable de la migration, administrateur réseau
Passez en revue les résultats de l'analyse.	Passez en revue les résultats de l'analyse pour les serveurs de test. Si des erreurs sont détectées, résolvez-les et corrigez-les. Documentez les erreurs et les solutions. Vous ferez référence à ces informations à l'avenir, et vous pourrez les ajouter à l'historique de votre portefeuille.	Responsable du développement, responsable de la migration, administrateur réseau
Scannez à nouveau les serveurs de test.	Une fois le nouveau scan terminé, répétez le scan jusqu'à ce qu'il n'y ait plus d'erreur.	Responsable du développement, responsable de la migration, administrateur réseau

Ressources connexes

AWS resources

- Guide d'évaluation du portefeuille d'applications pour la AWS Cloud migration
- Outils de migration de découverte, de planification et de recommandation

Guides de déploiement pour les outils de découverte les plus fréquemment sélectionnés

- Déployez l'appliance virtuelle RN15 0 (documentation Flexera)
- Installation de Gatherer (documentation ModelizeIt)
- Installation du serveur d'analyse sur site (documentation ModelizeIt)

Informations supplémentaires

Considérations relatives à la sélection d'un outil de découverte automatique

Chaque outil de découverte présente des avantages et des limites. Lorsque vous sélectionnez l'outil adapté à votre cas d'utilisation, tenez compte des points suivants :

- Sélectionnez un outil de découverte capable de collecter la plupart, sinon la totalité, des métadonnées dont vous avez besoin pour atteindre votre objectif d'évaluation de portefeuille.
- Identifiez les métadonnées que vous devez collecter manuellement car l'outil ne les prend pas en charge.
- Fournissez les exigences relatives à l'outil de découverte aux parties prenantes afin qu'elles puissent examiner et évaluer l'outil en fonction de leurs exigences internes en matière de sécurité et de conformité, telles que les exigences en matière de serveur, de réseau et d'informations d'identification.
  - L'outil nécessite-t-il que vous installiez un agent dans la charge de travail intégrée ?
  - L'outil nécessite-t-il que vous installiez une appliance virtuelle dans votre environnement ?
- Déterminez vos exigences en matière de résidence des données. Certaines entreprises ne souhaitent pas stocker leurs données en dehors de leur environnement. Pour résoudre ce problème, vous devrez peut-être installer certains composants de l'outil dans l'environnement local.
- Assurez-vous que l'outil prend en charge le système d'exploitation (OS) et la version du système d'exploitation de la charge de travail intégrée.

- Déterminez si votre portefeuille comprend des serveurs centraux, de milieu de gamme et anciens. La plupart des outils de découverte peuvent détecter ces charges de travail en tant que dépendances, mais certains outils peuvent ne pas être en mesure d'obtenir les détails des appareils, tels que l'utilisation et les dépendances des serveurs. Les outils de découverte Device42 et ModernizeIT prennent tous deux en charge les serveurs mainframe et de milieu de gamme.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrez les charges de travail Cloudera sur site vers Cloudera Data Platform sur AWS

Créée par Battulga Purevragchaa (AWS), Nijjwol Lamsal (partenaire) et Nidhi Gupta (AWS)

Récapitulatif

Ce modèle décrit les étapes de haut niveau de la migration de vos charges de travail Cloudera Distributed Hadoop (CDH), Hortonworks Data Platform (HDP) et Cloudera Data Platform (CDP) sur site vers le cloud public CDP sur AWS. Nous vous recommandons de vous associer à Cloudera Professional Services et à un intégrateur de systèmes (SI) pour mettre en œuvre ces étapes.

Les clients de Cloudera souhaitent déplacer leurs charges de travail CDH, HDP et CDP sur site vers le cloud pour de nombreuses raisons. Voici quelques raisons typiques :

- Simplifiez l'adoption de nouveaux paradigmes de plateforme de données tels que Data Lakehouse ou Data Mesh
- Améliorez l'agilité de l'entreprise, démocratisez l'accès et l'inférence sur les actifs de données existants
- Réduisez le coût total de possession (TCO)
- Améliorez l'élasticité de la charge
- Améliorez l'évolutivité ; réduisez considérablement le temps de fourniture des services de données par rapport à l'ancienne base d'installation sur site
- Supprimez le matériel existant ; réduisez considérablement les cycles d'actualisation du matériel
- Profitez de la pay-as-you-go tarification, étendue aux charges de travail Cloudera sur AWS grâce au modèle de licence Cloudera (CCU)
- Profitez d'un déploiement plus rapide et d'une intégration améliorée grâce aux plateformes d'intégration continue et de livraison continue (CI/CD)
- Utilisez une plate-forme unifiée (CDP) unique pour plusieurs charges de travail

Cloudera prend en charge toutes les principales charges de travail, notamment le Machine Learning, l'ingénierie des données, l'entrepôt de données, la base de données opérationnelle, le traitement des flux (CSP), ainsi que la sécurité et la gouvernance des données. Cloudera propose ces charges de travail sur site depuis de nombreuses années, et vous pouvez les migrer vers le cloud AWS en utilisant le cloud public CDP avec Workload Manager et Replication Manager.

Cloudera Shared Data Experience (SDX) fournit un catalogue de métadonnées partagé pour ces charges de travail afin de faciliter une gestion et des opérations cohérentes des données. SDX inclut également une sécurité complète et granulaire pour se protéger contre les menaces, ainsi qu'une gouvernance unifiée pour les capacités d'audit et de recherche afin de garantir la conformité aux normes telles que la norme de sécurité des données du secteur des cartes de paiement (PCI DSS) et le RGPD.

La migration vers le CDP en un coup d'œil

Charge de travail	Charge de travail source	Cloud privé CDH, HDP et CDP
	Environnement source	• Windows, Linux • Sur site, en colocation ou dans tout autre environnement autre qu'AWS
	Charge de travail de destination	Cloud public CDP sur AWS
	Environnement de destination	• Modèle de déploiement : compte client • Modèle de fonctionnement : Client/plan de contrôle Cloudera
Migration	Stratégie de migration (7Rs)	Réhébergement, replateforme ou refactorisation
	S'agit-il d'une mise à niveau de la version de charge de travail ?	Oui
	Durée de migration	• Déploiement : environ une semaine pour créer un compte client, un cloud privé virtuel (VPC) et un environnement CDP Public Cloud géré par le client.

- Durée de migration : 1 à 4 mois, en fonction de la complexité et de la taille de la charge de travail.

Coût	Coût d'exécution de la charge de travail sur AWS	• À un niveau élevé, le coût d'une migration de charge de travail CDH vers AWS suppose que vous établirez un nouvel environnement sur AWS. Cela inclut la comptabilisation du temps et des efforts du personnel, ainsi que le provisionnement des ressources informati ques et les licences de logiciels pour le nouvel environnement. • Le modèle de tarification basé sur la consommat ion du cloud de Cloudera vous donne la flexibilité nécessaire pour tirer parti des fonctionnalités de mise à l'échelle automatique et en rafale. Pour plus d'informa tions, consultez les tarifs du service CDP Public Cloud sur le site Web de Cloudera. • Cloudera Enterprise Data Hub est basé sur Amazon Elastic Compute Cloud (Amazon EC2) et modélise étroitement les clusters traditionnels. Le hub de données peut être personnal isé, mais cela aura une incidence sur les coûts. • CDP Public Cloud Data Warehouse, Cloudera Machine Learning et

		Cloudera Data Engineering (CDE) sont basés sur des conteneurs et peuvent être configurés pour évoluer automatiquement.
	Configuration système requise	Consultez la section Conditions préalables.
Contrats et cadres relatifs aux infrastructures	SLA	Consultez l'accord de niveau de service Cloudera pour le cloud public CDP.
	DR	Consultez Disaster Recovery dans la documentation de Cloudera.
	Modèle de licence et d'exploitation (pour le compte AWS cible)	Modèle « Bring Your Own License » (BYOL)
Conformité	Exigences de sécurité	Consultez la présentation de la sécurité de Cloudera dans la documentation de Cloudera.
	Autres certifications de conformité	Consultez les informations sur le site Web de Cloudera concernant la conformité au règlement général sur la protection des données (RGPD) et le CDP Trust Center.

Conditions préalables et limitations

Prérequis

- Exigences relatives aux comptes AWS, y compris les comptes, les ressources, les services et les autorisations, telles que la configuration des rôles et des politiques AWS Identity and Access Management (IAM)
- Conditions préalables au déploiement du CDP depuis le site Web de Cloudera

La migration nécessite les rôles et l'expertise suivants :

Rôle	Compétences et responsabilités
Responsable de la migration	Assure le soutien exécutif, la collaboration des équipes, la planification, la mise en œuvre et l'évaluation
PME de Cloudera	Compétences spécialisées en administration CDH, HDP et CDP, en administration système et en architecture
Architecte AWS	Compétences en matière de services, de mise en réseau, de sécurité et d'architectures AWS

Architecture

La mise en place de l'architecture appropriée est une étape essentielle pour garantir que la migration et les performances répondent à vos attentes. Pour que votre effort de migration réponde aux hypothèses de ce manuel, votre environnement de données cible dans le cloud AWS, que ce soit sur des instances hébergées dans un cloud privé virtuel (VPC) ou sur CDP, doit correspondre de manière équivalente à votre environnement source en termes de systèmes d'exploitation et de versions logicielles, ainsi que des principales spécifications des machines.

Le schéma suivant (reproduit avec l'autorisation de la fiche technique de Cloudera Shared Data Experience) montre les composants de l'infrastructure de l'environnement CDP et la manière dont les niveaux ou les composants de l'infrastructure interagissent.

L'architecture inclut les composants CDP suivants :

- Data Hub est un service de lancement et de gestion de clusters de charges de travail basé sur Cloudera Runtime. Vous pouvez utiliser les définitions de clusters dans Data Hub pour provisionner

et accéder à des clusters de charge de travail pour des cas d'utilisation personnalisés et définir des configurations de clusters personnalisées. Pour plus d'informations, consultez le site Web de Cloudera.

- Le flux de données et le streaming répondent aux principaux défis auxquels les entreprises sont confrontées en matière de données en mouvement. Il gère les éléments suivants :
  - Traitement du streaming de données en temps réel à haut volume et à grande échelle
  - Suivi de la provenance des données et de la traçabilité des données de streaming
  - Gestion et surveillance des applications de pointe et des sources de streaming

  Pour plus d'informations, consultez Cloudera DataFlow et CSP sur le site Web de Cloudera.
- L'ingénierie des données inclut l'intégration des données, la qualité des données et la gouvernance des données, qui aident les organisations à créer et à maintenir des pipelines de données et des flux de travail. Pour plus d'informations, consultez le site Web de Cloudera. Découvrez la prise en charge des instances ponctuelles afin de réduire les coûts sur AWS pour les charges de travail d'ingénierie des données de Cloudera.
- Data Warehouse vous permet de créer des entrepôts de données et des data marts indépendants qui s'adaptent automatiquement aux demandes de charge de travail. Ce service fournit des instances de calcul isolées et une optimisation automatisée pour chaque entrepôt de données et chaque data mart, et vous aide à réduire les coûts lors des réunions SLAs. Pour plus d'informations, consultez le site Web de Cloudera. Découvrez la gestion des coûts et l'auto-scaling pour Cloudera Data Warehouse sur AWS.
- La base de données opérationnelle du CDP fournit une base fiable et flexible pour des applications évolutives et performantes. Il fournit une base de données évolutive en temps réel, toujours disponible, qui sert les données structurées traditionnelles ainsi que les nouvelles données non structurées au sein d'une plateforme opérationnelle et d'entreposage unifiée. Pour plus d'informations, consultez le site Web de Cloudera.
- Machine Learning est une plateforme d'apprentissage automatique native du cloud qui fusionne les fonctionnalités de science et d'ingénierie des données en libre-service dans un service unique et portable au sein d'un cloud de données d'entreprise. Il permet un déploiement évolutif de l'apprentissage automatique et de l'intelligence artificielle (IA) sur les données, où qu'elles soient. Pour plus d'informations, consultez le site Web de Cloudera.

CDP sur AWS

Le schéma suivant (adapté avec l'autorisation du site Web de Cloudera) montre l'architecture de haut niveau du CDP sur AWS. Le CDP met en œuvre son propre modèle de sécurité pour gérer à la fois les comptes et le flux de données. Ils sont intégrés à IAM grâce à l'utilisation de rôles entre comptes.

Le plan de contrôle CDP réside dans un compte principal Cloudera dans son propre VPC. Chaque compte client possède son propre sous-compte et son propre VPC. Les rôles IAM entre comptes et les technologies SSL acheminent le trafic de gestion vers et depuis le plan de contrôle vers les services clients qui résident sur des sous-réseaux publics routables par Internet au sein de chaque VPC client. Sur le VPC du client, le Cloudera Shared Data Experience (SDX) fournit une sécurité à la pointe de l'entreprise avec une gouvernance et une conformité unifiées afin que vous puissiez obtenir des informations plus rapidement à partir de vos données. SDX est une philosophie de conception intégrée à tous les produits Cloudera. Pour plus d'informations sur SDX et l'architecture réseau CDP Public Cloud pour AWS, consultez la documentation Cloudera.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Elastic Kubernetes Service (Amazon EKS) vous aide à exécuter Kubernetes sur AWS sans avoir à installer ou à gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Automatisation et outillage

- Pour obtenir des outils supplémentaires, vous pouvez utiliser Cloudera Backup Data Recovery (BDR), AWS Snowball et AWS Snowmobile pour faciliter la migration des données d'un CDH, HDP et CDP sur site vers un CDP hébergé par AWS.

- Pour les nouveaux déploiements, nous vous recommandons d'utiliser la solution AWS Partner pour le CDP.

Épopées

Préparation à la migration

Tâche	Description	Compétences requises
Engagez l'équipe Cloudera.	Cloudera applique un modèle d'engagement standardisé avec ses clients et peut travailler avec votre intégrateur de systèmes (SI) pour promouvoir la même approche. Contactez l'équipe client de Cloudera afin qu'elle puisse vous fournir des conseils et les ressources techniques nécessaires pour démarrer le projet. Contacter l'équipe Cloudera permet de s'assurer que toutes les équipes nécessaires peuvent préparer la migration à l'approche de sa date. Vous pouvez contacter les services professionnels de Cloudera pour faire passer votre déploiement Cloudera du stade pilote à celui de la production rapidement, à moindre coût et avec des performances optimales. Pour une liste complète des	Responsable de la migration

Tâche	Description	Compétences requises
	offres, consultez le site Web de Cloudera.	
Créez un environnement de cloud public CDP sur AWS pour votre VPC.	Travaillez avec Cloudera Professional Services ou votre SI pour planifier et déployer le cloud public CDP dans un VPC sur AWS.	Architecte cloud, Cloudera PME

Tâche	Description	Compétences requises
Hiérarchisez et évaluez les charges de travail pour la migration.	Évaluez toutes vos charges de travail sur site afin de déterminer les charges de travail les plus faciles à migrer. Il est préférable de passer en premier aux applications qui ne sont pas critiques, car elles n'auront qu'un impact minimal sur vos clients. Conservez les charges de travail critiques pour la fin, une fois que vous aurez réussi à migrer d'autres charges de travail. **Note** Les charges de travail transitoires (CDP Data Engineering) sont plus faciles à migrer que les charges de travail persistantes (CDP Data Warehouse). Il est également important de prendre en compte le volume et les emplaceme nts des données lors de la migration. Les défis peuvent inclure la réplication continue des données d'un environnement sur site vers le cloud et la modification des	Responsable de la migration

Tâche	Description	Compétences requises
	pipelines d'ingesti on de données pour importer les données directement dans le cloud.	
Discutez des activités de migration des applications CDH, HDP, CDP et des anciennes applications.	Envisagez et commencez à planifier les activités suivantes avec Cloudera Workload Manager : • Données et charges de travail à copier dans votre environnement AWS • Des données prêtes pour le cloud • Voisins bruyants, qui consomment des ressource s et créent des problèmes pour les autres locataires • Charges de travail élastique s • Petits clusters avec une charge opérationnelle élevée	Responsable de la migration

Tâche	Description	Compétences requises
Répondez aux exigences et aux recommandations de Cloudera Replication Manager.	Travaillez avec Cloudera Professional Services et votre SI pour préparer la migration des charges de travail vers votre environnement de cloud public CDP sur AWS. La compréhension des exigences et recommandations suivantes peut vous aider à éviter les problèmes courants pendant et après l'installation du service Replication Manager. • Consultez les documents de support de Replicati on Manager pour vérifier que vous répondez aux exigences en matière d'environnement et de système. Pour plus d'informations, consultez la matrice de support pour CDP Public Cloud Replicati on Manager sur le site Web de Cloudera. • Vous n'avez pas besoin d'un accès root aux nœuds sur lesquels l'application Replication Manager et le moteur Data Lifecycle Manager (DLM) seront installés. • Installez Apache Hive lors de l'installation initiale de	Responsable de la migration

Tâche	Description	Compétences requises
	Replication Manager, sauf si vous êtes certain de ne pas utiliser la réplication Hive à l'avenir. Si vous décidez d'installer Hive après avoir créé des politiques de réplication HDFS dans Replication Manager, vous devez supprimer puis recréer toutes les politique s de réplication HDFS après avoir ajouté Hive. • Les clusters utilisés dans Replication Manager doivent avoir des configurations symétriques. Chaque cluster associé à une relation de réplication doit être configuré exactement de la même manière pour la sécurité (Kerberos), la gestion des utilisateurs (LDAP/AD) et le proxy Knox. Les services de cluster tels que Hadoop Distributed File System (HDFS), Apache Hive, Apache Knox, Apache Ranger et Apache Atlas peuvent avoir différentes configurations pour une haute disponibilité (HA). Par exemple, les clusters source et cible peuvent avoir des	

Tâche	Description	Compétences requises
	configurations HA et non HA distinctes.	

Migrer le CDP vers AWS

Tâche	Description	Compétences requises
Migrez la première charge de travail pour les environnements de développement/test à l'aide de Cloudera Workload Manager.	Votre SI peut vous aider à migrer votre première charge de travail vers le cloud AWS. Il doit s'agir d'une application qui n'est ni orientée vers le client ni essentielle à la mission. Les applications dont les données peuvent être facilement ingérées par le cloud, telles que les charges de travail d'ingénierie des données CDP, sont les candidates idéales pour la migration de développement/test. Il s'agit d'une charge de travail transitoire à laquelle moins d'utilisateurs accèdent, par rapport à une charge de travail persistante telle qu'une charge de travail d'entrepôt de données CDP à laquelle de nombreux utilisateurs peuvent avoir besoin d'un accès ininterrompu. Les charges de travail liées à l'ingénierie des données ne sont pas persistantes, ce qui minimise	Responsable de la migration

Tâche	Description	Compétences requises
	l'impact commercial en cas de problème. Cependant , ces tâches peuvent être essentielles pour les rapports de production. Priorisez donc d'abord les charges de travail d'ingénierie des données à faible impact.	

Tâche	Description	Compétences requises
Répétez les étapes de migration si nécessaire.	Cloudera Workload Manager permet d'identifier les charges de travail les mieux adaptées au cloud. Il fournit des indicateurs tels que les évaluations des performan ces du cloud, les plans de dimensionnement/capacité pour l'environnement cible et les plans de réplication. Les meilleurs candidats à la migration sont les charges de travail saisonnières, les rapports ad hoc et les emplois intermittents qui ne consomment pas beaucoup de ressources. Cloudera Replication Manager déplace les données de l'environnement sur site vers le cloud, et du cloud vers l'environnement sur site. Optimisez de manière proactive les charges de travail, les applications, les performances et la capacité de l'infrastructure pour l'entrepo sage de données, l'ingénie rie des données et l'apprent issage automatique à l'aide de Workload Manager. Pour un guide complet sur la modernisation d'un entrepôt	PME de Cloudera

Tâche	Description	Compétences requises
	de données, consultez le site Web de Cloudera.	

Ressources connexes

Documentation Cloudera :

- Enregistrement de clusters classiques avec CDP, Cloudera Manager et Replication Manager :
  - Console de gestion
  - Réplication en ruche de Replication Manager
- Réplication de Sentry
- Autorisations de sentinelle
- Liste de contrôle pour la planification du cluster Data Hub
- Architecture du gestionnaire de charge de travail
- Exigences relatives à Replication Manager
- Observabilité de la plateforme de données Cloudera
- Exigences relatives à AWS

Documentation AWS :

- Migration des données dans le cloud

Résoudre les erreurs de connexion après la migration de Microsoft SQL Server vers le cloud AWS

Créée par Premkumar Chelladurai (AWS)

Récapitulatif

Après avoir migré Microsoft SQL Server exécuté sous Windows Server 2008 R2, 2012 ou 2012 R2 vers des instances Amazon Elastic Compute Cloud (Amazon EC2) sur le cloud Amazon Web Services (AWS), la connexion à SQL Server échoue et les erreurs suivantes apparaissent :

- `[Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error`
- `ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure. System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)`
- `TCP Provider: The semaphore timeout period has expired`

Ce modèle décrit comment résoudre ces erreurs en désactivant les fonctionnalités du Windows Scalable Networking Pack (SNP) au niveau du système d'exploitation (OS) et de l'interface réseau pour SQL Server exécuté sous Windows Server 2008 R2, 2012 ou 2012 R2.

Conditions préalables et limitations

Prérequis

- Privilèges d'administrateur pour Windows Server.
- Si vous avez utilisé AWS Application Migration Service comme outil de migration, vous avez besoin de l'une des versions de Windows Server suivantes :
  - Windows Server 2008 R2 Service Pack 1, 2012 ou 2012 R2
- Si vous avez utilisé CloudEndure Migration comme outil de migration, vous avez besoin de l'une des versions de Windows Server suivantes :
  - Windows Server 2003 R2 Service Pack 3, 2008, 2008 R2 Service Pack 1, 2012 ou 2012 R2

Outils

- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que vous le souhaitez, et vous pouvez les étendre ou les intégrer.
- Windows Server — Windows Server est une plate-forme permettant de créer une infrastructure d'applications, de réseaux et de services Web connectés.

Épopées

Désactiver les fonctionnalités SNP au niveau du système d'exploitation et de l'interface elastic network

Tâche	Description	Compétences requises
Désactivez les fonctionnalités du SNP au niveau du système d'exploitation.	1. Connectez-vous à Windows Server et ouvrez une invite de commande en tant qu'administrateur. 2. Exécutez la commande `netsh int tcp show global`. 3. Dans la sortie, vérifiez si l'un `Receive-Side Scaling` ou l'autre `Chimney Offload` est en `enabled` mode. Si c'est le cas`enabled`, exécutez les commandes suivantes : • `netsh int tcp set global chimney=disabled` • `netsh int tcp set global rss=disabled`	Administrateur AWS, administrateur système AWS, ingénieur en migration, administrateur du cloud

Tâche	Description	Compétences requises
Désactivez les fonctionnalités du protocole SNP au niveau de l'interface elastic network.	1. Choisissez Démarrer`ncpa.cpl`, puis appuyez sur Entrée. 2. Cliquez avec le bouton droit sur Elastic Network Adapter 3. Dans le menu contextuel, choisissez Propriétés. 4. Dans la fenêtre Propriété s de l'adaptateur Ethernet, choisissez Configurer. 5. Dans la fenêtre contextue lle Amazon Elastic Network Adapter Properties, sélectionnez l'onglet Avancé. 6. Dans la section Propriétés, désactivez tous les transfert s et les flux RSS.	Administrateur AWS, administr ateur du cloud, administrateur des systèmes AWS

Ressources connexes

- Comment résoudre les problèmes liés aux fonctionnalités avancées de performance réseau telles que RSS et NetDMA

Redémarrez automatiquement l'agent de réplication AWS sans le désactiver SELinux après le redémarrage d'un serveur source RHEL

Créée par Anil Kunapareddy (AWS), Shanmugam Shanker (AWS) et Venkatramana Chintha (AWS)

Récapitulatif

AWS Application Migration Service permet de simplifier, d'accélérer et d'automatiser la migration de votre charge de travail Red Hat Enterprise Linux (RHEL) vers le cloud Amazon Web Services (AWS). Pour ajouter des serveurs sources à Application Migration Service, vous devez installer l'agent de réplication AWS sur les serveurs.

Le service de migration d'applications fournit une réplication asynchrone en temps réel au niveau des blocs. Cela signifie que vous pouvez poursuivre les opérations informatiques normales pendant tout le processus de réplication. Ces opérations informatiques peuvent nécessiter le redémarrage ou le redémarrage de votre serveur source RHEL pendant la migration. Dans ce cas, l'agent de réplication AWS ne redémarrera pas automatiquement et la réplication de vos données s'arrêtera. En général, vous pouvez configurer Security-Enhanced Linux (SELinux) sur le mode désactivé ou sur le mode permissif pour redémarrer automatiquement AWS Replication Agent. Toutefois, les politiques de sécurité de votre entreprise peuvent interdire la désactivation SELinux et vous devrez peut-être également renommer vos fichiers.

Ce modèle décrit comment redémarrer automatiquement l'agent de réplication AWS sans le désactiver SELinux lorsque votre serveur source RHEL redémarre ou redémarre pendant une migration.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Charge de travail RHEL sur site que vous souhaitez migrer vers le cloud AWS.
- Service de migration d'applications initialisé à partir de la console du service de migration d'applications. L'initialisation n'est requise que la première fois que vous utilisez ce service. Pour obtenir des instructions, consultez la documentation du service de migration d'applications.
- Une politique AWS Identity and Access Management (IAM) existante pour le service de migration d'applications. Pour plus d'informations, consultez la documentation du service de migration des applications.

Versions

- RHEL version 7 ou ultérieure

Outils

Services AWS

- AWS Application Migration Service est une solution hautement automatisée lift-and-shift (réhébergement) qui simplifie, accélère et réduit le coût de la migration des applications vers AWS.

Commandes Linux

Le tableau suivant fournit une liste des commandes Linux que vous exécuterez sur votre serveur source RHEL. Ils sont également décrits dans les épopées et les récits de ce modèle.

Commande	Description
`#systemctl –version`	Identifie la version du système.
`#systemctl list-units --type=service`	Répertorie tous les services actifs disponibles sur le serveur RHEL.
`#systemctl list-units --type=service | grep running`	Répertorie tous les services actuellement en cours d'exécution sur le serveur RHEL.
`#systemctl list-units --type=service | grep failed`	Répertorie tous les services qui n'ont pas pu être chargés après le redémarrage ou le redémarrage du serveur RHEL.
`restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Modifie le contexte en`aws-replication-service` .
`yum install policycoreutils*`	Installe les utilitaires Policy Core nécessaires au fonctionnement du SELinux système.
`ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Effectue une recherche dans le journal d'audit et crée un module pour les politiques.

`semodule -i my-modprobe.pp`	Active la politique.
`cat my-modprobe.te`	Affiche le contenu du `my-modprobe.te` fichier.
`semodule -l | grep my-modprobe`	Vérifie si la politique a été chargée dans le SELinux module.

Épopées

Installez l'agent de réplication AWS et redémarrez le serveur source RHEL

Tâche	Description	Compétences requises
Créez un utilisateur du service de migration d'applications avec une clé d'accès et une clé d'accès secrète.	Pour installer l'agent de réplication AWS, vous devez créer un utilisateur du service de migration d'applications avec les informations d'identification AWS requises. Pour obtenir des instructions, consultez la documentation du service de migration d'applications.	Ingénieur en migration
Installez l'agent de réplication AWS.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Migration Service à la https://console.aws.amazon.com/mgn/maison. 2. Configurez les paramètres de réplication en suivant les instructions de la documentation du service de migration d'applications.	Ingénieur en migration

Tâche	Description	Compétences requises
	3. Installez l'agent de réplication AWS en suivant les instructions de la documentation du service de migration d'applications. 4. Sur la page Serveurs source, choisissez le serveur source RHEL, puis choisissez Replication pour démarrer la réplication initiale. Pour plus d'informations, consultez la documentation du service de migration des applications.	
Redémarrez ou redémarrez le serveur source RHEL.	Redémarrez ou redémarrez votre serveur source RHEL lorsque son état de réplication des données indique Bloqué sur le tableau de bord de migration.	Ingénieur en migration
Vérifiez l'état de réplication des données.	Attendez une heure, puis vérifiez à nouveau l'état de réplication des données sur le tableau de bord de migration. Il doit être en bon état de santé.	Ingénieur en migration

Vérifiez l'état de l'agent de réplication AWS sur le serveur source RHEL

Tâche	Description	Compétences requises
Identifiez la version du système.	Ouvrez l'interface de ligne de commande de votre serveur source RHEL et exécutez la commande suivante pour identifier la version du système : `#systemctl –version`	Ingénieur en migration
Répertoriez tous les services actifs.	Pour répertorier tous les services actifs disponibles sur le serveur RHEL, exécutez la commande suivante : `#systemctl list-units --type=service`	Ingénieur en migration
Répertorie tous les services en cours d'exécution.	Pour répertorier tous les services actuellement en cours d'exécution sur le serveur RHEL, utilisez la commande : `#systemctl list-units --type=service | grep running`	Ingénieur en migration
Répertoriez tous les services qui n'ont pas pu être chargés.	Pour répertorier tous les services qui n'ont pas pu être chargés après le redémarrage ou le redémarrage du serveur RHEL, exécutez la commande suivante :	Ingénieur en migration

Tâche	Description	Compétences requises
	`#systemctl list-units --type=service | grep failed`	

Création et exécution du SELinux module

Tâche	Description	Compétences requises
Modifiez le contexte de sécurité.	Dans l'interface de ligne de commande de votre serveur source RHEL, exécutez la commande suivante pour remplacer le contexte de sécurité par le service de réplication AWS : `restorecon -Rv /etc/rc.d/init.d/aws-replication-service`	Ingénieur en migration
Installez les principaux utilitaires.	Pour installer les principaux utilitaires nécessaires au fonctionnement du SELinux système et à ses politiques, exécutez la commande suivante : `yum install policycoreutils*`	Ingénieur en migration
Effectuez une recherche dans le journal d'audit et créez un module pour les politiques.	Exécutez la commande : `ausearch -c "insmod" --raw | audit2allow -M my-modprobe`	Ingénieur en migration

Tâche	Description	Compétences requises
Affichez le contenu du my-modprobe-te fichier.	Le `my-modprobe.te` fichier est généré par la commande audit2allow. Il inclut les SELinux domaines, le répertoire des sources de politiques et les sous-répertoires, et spécifie les règles du vecteur d'accès et les transitions associées aux domaines. Pour afficher le contenu du fichier, exécutez la commande suivante : `cat my modprobe.te`	Ingénieur en migration
Activez la politique.	Pour insérer le module et activer le package de politiques, exécutez la commande suivante : `semodule -i my-modprobe.pp`	Ingénieur en migration
Vérifiez si le module a été chargé.	Exécutez la commande : `semodule -l | grep my-modprobe` Une fois le SELinux module chargé, vous n'aurez plus à passer en mode désactivé ou SELinux en mode permissif lors de votre migration.	Ingénieur en migration

Tâche	Description	Compétences requises
Redémarrez ou redémarrez le serveur source RHEL et vérifiez l'état de réplication des données.	Ouvrez la console AWS Migration Service, accédez à la progression de la réplication des données, puis redémarrez ou redémarrez votre serveur source RHEL. La réplication des données devrait désormais reprendre automatiquement après le redémarrage du serveur source RHEL.	Ingénieur en migration

Ressources connexes

- Documentation du service de migration d'applications
- Supports de formation technique
- Résolution des problèmes liés à l'agent de réplication AWS
- Politiques du service de migration des applications

Ré-architecte

Rubriques

- Convertir VARCHAR2 (1) le type de données pour Oracle en type de données booléen pour Amazon Aurora PostgreSQL
- Création d'utilisateurs et de rôles d'application dans Aurora PostgreSQL compatible
- Émulez Oracle DR à l'aide d'une base de données globale Aurora compatible avec PostgreSQL
- SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL
- Migrez progressivement d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle SQL Developer et d'AWS SCT
- Chargez des fichiers BLOB dans TEXT en utilisant le codage de fichiers compatible avec Aurora PostgreSQL
- Migrer Amazon RDS for Oracle vers Amazon RDS for PostgreSQL avec et en utilisant et AWS SCTAWS DMSAWS CLIAWS CloudFormation
- Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS
- Migrer les packages pragma Oracle SERIALLY_REUSERABLE vers PostgreSQL
- Migrer des tables externes Oracle vers des tables compatibles avec Amazon Aurora PostgreSQL
- Migrer les index basés sur les fonctions d'Oracle vers PostgreSQL
- Migrer les fonctions natives d'Oracle vers PostgreSQL à l'aide d'extensions
- Migrer une base de données DB2 d'Amazon EC2 vers Aurora compatible avec MySQL à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server d'Amazon EC2 vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer une base de données ThoughtSpot Falçon sur site vers Amazon Redshift
- Migrer une base de données Oracle vers Amazon DynamoDB à l'aide d'AWS DMS
- Migrer une table partitionnée Oracle vers PostgreSQL à l'aide d'AWS DMS
- Migrer d'Amazon RDS for Oracle vers Amazon RDS for MySQL
- Migrez d'IBM Db2 sur Amazon vers une version compatible avec Aurora PostgreSQL EC2 à l'aide d'AWS DMS et d'AWS SCT
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide d'AWS DMS SharePlex

- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide de vues matérialisées et d'AWS DMS
- Migrez d'Oracle sur Amazon EC2 vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer d'Oracle vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for MariaDB à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle sur site vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle sur site vers Amazon RDS for PostgreSQL à l'aide d'un assistant Oracle et d'AWS DMS
- Migrer d'une base de données Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle GoldenGate
- Migrer une base de données Oracle vers Amazon Redshift à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle vers Aurora PostgreSQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer les données d'une base de données Oracle sur site vers Aurora PostgreSQL
- Migrez de SAP ASE vers Amazon RDS for SQL Server à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer une base de données Vertica sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer les applications existantes d'Oracle Pro*C vers ECPG
- Migrer les colonnes générées virtuellement d'Oracle vers PostgreSQL
- Configuration de la fonctionnalité Oracle UTL_FILE sur Aurora compatible avec PostgreSQL
- Valider les objets de base de données après la migration d'Oracle vers Amazon Aurora PostgreSQL

Convertir VARCHAR2 (1) le type de données pour Oracle en type de données booléen pour Amazon Aurora PostgreSQL

Créée par Naresh Damera (AWS)

Récapitulatif

Lors d'une migration d'Amazon Relational Database Service (Amazon RDS) pour Oracle vers l'édition compatible avec Amazon Aurora PostgreSQL, il est possible que vous rencontriez une incompatibilité des données lors de la validation de la migration dans (). AWS Database Migration Service AWS DMS Pour éviter cette incompatibilité, vous pouvez convertir VARCHAR2 (1) type de données en type booléen.

VARCHAR2 le type de données stocke des chaînes de texte de longueur variable et VARCHAR2 (1) indique que la chaîne comporte 1 caractère ou 1 octet. Pour plus d'informations VARCHAR2, voir les types de données intégrés d'Oracle (documentation Oracle).

Dans ce modèle, dans la colonne de la table de données source d'échantillons, les données VARCHAR2 (1) sont soit un Y, pour Oui, soit un N, pour Non. Ce modèle inclut des instructions pour utiliser AWS DMS and AWS Schema Conversion Tool (AWS SCT) pour convertir ce type de données des valeurs Y et N dans VARCHAR2 (1) en valeurs vraies ou fausses dans le booléen.

Public visé

Ce modèle est recommandé pour ceux qui ont déjà migré des bases de données Oracle vers des bases de données compatibles avec Aurora PostgreSQL en utilisant. AWS DMS Lorsque vous terminez la migration, respectez les recommandations de la section Conversion d'Oracle vers Amazon RDS for PostgreSQL ou Amazon AWS SCT Aurora PostgreSQL (documentation).

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Vérifiez que votre environnement est préparé pour Aurora, notamment en configurant les informations d'identification, les autorisations et un groupe de sécurité. Pour plus d'informations, consultez Configuration de votre environnement pour Amazon Aurora (documentation Aurora).
- Base de données source Amazon RDS for Oracle qui contient une colonne de table VARCHAR2 contenant (1) données.

- Une instance de base de données cible compatible avec Amazon Aurora PostgreSQL. Pour plus d'informations, consultez Création d'un cluster de bases de données et connexion à une base de données sur un cluster de bases de données Aurora PostgreSQL (documentation Aurora).

Versions du produit

- Amazon RDS pour Oracle version 12.1.0.2 ou ultérieure.
- AWS DMS version 3.1.4 ou ultérieure. Pour plus d'informations, consultez les sections Utilisation d'une base de données Oracle comme source AWS DMS et Utilisation d'une base de données PostgreSQL comme cible AWS DMS pour AWS DMS (documentation). Nous vous recommandons d'utiliser la dernière version de AWS DMS pour bénéficier de la prise en charge la plus complète possible des versions et des fonctionnalités.
- AWS Schema Conversion Tool (AWS SCT) version 1.0.632 ou ultérieure. Nous vous recommandons d'utiliser la dernière version de AWS SCT pour bénéficier de la prise en charge la plus complète possible des versions et des fonctionnalités.
- Aurora prend en charge les versions de PostgreSQL répertoriées dans la section Versions du moteur de base de données pour Aurora compatible avec PostgreSQL (documentation Aurora).

Architecture

Pile technologique source

Instance de base de données Amazon RDS for Oracle

Pile technologique cible

Instance de base de données compatible avec Amazon Aurora PostgreSQL

Architecture source et cible

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.

- AWS Database Migration Service (AWS DMS) vous aide à migrer les banques de données vers AWS Cloud ou entre des combinaisons de configurations cloud et sur site.
- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le. AWS Cloud
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Autres services

- Oracle SQL Developer est un environnement de développement intégré qui simplifie le développement et la gestion des bases de données Oracle dans les déploiements traditionnels et basés sur le cloud. Dans ce modèle, vous utilisez cet outil pour vous connecter à l'instance de base de données Amazon RDS for Oracle et interroger les données.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données. Dans ce modèle, vous utilisez cet outil pour vous connecter à l'instance de base de données Aurora et interroger les données.

Épopées

Préparez-vous à la migration

Tâche	Description	Compétences requises
Créez un rapport de migration de base de données.	1. Dans AWS SCT, créez un rapport d'évaluation de la migration de base de données. Pour plus d'informations, consultez la section Création de rapports d'évaluation de la migration. 2. Passez en revue et exécutez les actions figurant dans le rapport	DBA, Développeur

Tâche	Description	Compétences requises
	d'évaluation de la migration . Pour plus d'informations, consultez la section Éléments d'action du rapport d'évaluation.	

Tâche	Description	Compétences requises
Désactivez les contraintes liées aux clés étrangères sur la base de données cible.	Dans PostgreSQL, les clés étrangères sont implément ées à l'aide de déclenche urs. Pendant la phase de chargement complet, AWS DMS charge chaque table une par une. Nous vous recommandons vivement de désactiver les contraintes liées aux clés étrangères lors d'un chargement complet en utilisant l'une des méthodes suivantes : • Désactivez temporair ement tous les déclenche urs depuis l'instance, et terminez le chargement complet. • Utilisez le paramètre `session_replicatio n_role` dans PostgreSQL. S'il n'est pas possible de désactiver les contraintes liées aux clés étrangères, créez une tâche de AWS DMS migration pour les données primaires spécifique à la table parent et à la table enfant.	DBA, Développeur

Tâche	Description	Compétences requises

Désactivez les clés primaires et les clés uniques de la base de données cible.	À l'aide des commandes suivantes, désactivez les clés primaires et les contraintes sur la base de données cible. Cela permet d'améliorer les performances de la tâche de chargement initiale.
	`ALTER TABLE <table> DISABLE PRIMARY KEY;`
	`ALTER TABLE <table> DISABLE CONSTRAINT <constraint_name>;`
		DBA, Développeur

Créez la tâche de chargement initiale.	Dans AWS DMS, créez la tâche de migration pour le chargement initial. Pour obtenir des instructions, reportez-vous à la section Création d'une tâche. Pour la méthode de migration, choisissez Migrer les données existantes. Cette méthode de migration est appelée `Full Load` dans l'API. Ne commencez pas encore cette tâche.	DBA, Développeur

Tâche	Description	Compétences requises
Modifiez les paramètres de tâche pour la tâche de chargement initiale.	Modifiez les paramètres des tâches pour ajouter la validation des données. Ces paramètres de validation doivent être créés dans un fichier JSON. Pour obtenir des instructions et des exemples, consultez la section Spécification des paramètres des tâches. Ajoutez les validations suivantes : • Pour vérifier que les VARCHAR2 (1) données sont correctement converties en booléens dans la base de données cible, ajoutez le code dans le script de validation des données dans la section Informations supplémentaires de ce modèle. Le script de validation convertit les valeurs booléennes de 1 en Y et de 0 en N dans la table cible, puis il compare les valeurs de la table cible à celles de la table source. Pour valider le reste de la migration des données, activez la validation des données dans la tâche. Pour plus d'informations, consultez	Administrateur AWS, DBA

Tâche	Description	Compétences requises
	la section Paramètres des tâches de validation des données.	
Créez la tâche de réplication en cours.	Dans AWS DMS, créez la tâche de migration qui synchronise la base de données cible avec la base de données source. Pour obtenir des instructions, reportez-vous à la section Création d'une tâche. Pour la méthode de migration, sélectionnez Répliquer uniquement les modifications de données. Ne commencez pas encore cette tâche.	DBA

Testez les tâches de migration

Tâche	Description	Compétences requises
Créez des exemples de données pour les tests.	Dans la base de données source, créez un exemple de table contenant des données à des fins de test.	Developer
Vérifiez qu'il n'y a pas d'activités conflictuelles.	Utilisez le `pg_stat_activity` pour vérifier toute activité sur le serveur susceptible d'affecter la migration. Pour plus d'informations, consultez The Statistic	Administrateur AWS

Tâche	Description	Compétences requises
	s Collector (documentation PostgreSQL).	
Démarrez les tâches de AWS DMS migration.	Dans la AWS DMS console, sur la page Tableau de bord, lancez le chargement initial et les tâches de réplication en cours que vous avez créées dans l'épopée précédente.	Administrateur AWS
Surveillez les tâches et les états de chargement des tables.	Pendant la migration, surveillez l'état des tâches et les états des tables. Lorsque la tâche de chargement initiale est terminée, dans l'onglet Statistiques du tableau : • L'état de chargement doit être Table terminée. • L'état de validation doit être validé.	Administrateur AWS
Vérifiez les résultats de la migration.	À l'aide de pgAdmin, interrogez la table sur la base de données cible. Une requête réussie indique que les données ont été migrées avec succès.	Developer
Ajoutez des clés primaires et des clés étrangères dans la base de données cible.	Créez la clé primaire et la clé étrangère dans la base de données cible. Pour plus d'informations, consultez ALTER TABLE (site Web de PostgreSQL).	DBA

Tâche	Description	Compétences requises
Nettoyez les données de test.	Dans les bases de données source et cible, nettoyez les données créées pour les tests unitaires.	Developer

Découper

Tâche	Description	Compétences requises
Terminez la migration.	Répétez l'épopée précédente, testez les tâches de migration en utilisant les données source réelles. Cela permet de migrer les données de la base de données source vers la base de données cible.	Developer
Vérifiez que les bases de données source et cible sont synchronisées.	Vérifiez que les bases de données source et cible sont synchronisées. Pour plus d'informations et d'instructions, consultez la section Validation AWS DMS des données.	Developer
Arrêtez la base de données source.	Arrêtez la base de données Amazon RDS for Oracle. Pour obtenir des instructions, consultez Arrêter temporairement une instance de base de données Amazon RDS. Lorsque vous arrêtez la base de données source, le chargement initial et les tâches de réplication en cours AWS DMS sont automatiq	Developer

Tâche	Description	Compétences requises
	uement interrompus. Aucune action supplémentaire n'est requise pour arrêter ces tâches.	

Ressources connexes

AWS références

- Migrer une base de données Oracle vers Aurora PostgreSQL à l' AWS DMS aide de AWS SCT et AWS (directives prescriptives)
- Conversion d'Oracle en Amazon RDS pour PostgreSQL ou Amazon AWS SCT Aurora PostgreSQL (documentation)
- Comment AWS DMS fonctionne (AWS DMS documentation)

Autres références

- Type de données booléen (documentation PostgreSQL)
- Types de données intégrés à Oracle (documentation Oracle)
- pgAdmin (site Web de pgAdmin)
- Développeur SQL (site Web Oracle)

Tutoriels et vidéos

- Commencer avec AWS DMS
- Commencer à utiliser Amazon RDS
- Présentation de AWS DMS (vidéo)
- Comprendre Amazon RDS (vidéo)

Informations supplémentaires

Script de validation des données

Le script de validation des données suivant convertit 1 en Y et 0 en N. Cela permet de mener à bien la AWS DMS tâche et de réussir la validation de la table.

```
{
"rule-type": "validation",
"rule-id": "5",
"rule-name": "5",
"rule-target": "column",
"object-locator": {
"schema-name": "ADMIN",
"table-name": "TEMP_CHRA_BOOL",
"column-name": "GRADE"
},
"rule-action": "override-validation-function",
"target-function": "case grade when '1' then 'Y' else 'N' end"
        }
```

L'`case`instruction du script effectue la validation. Si la validation échoue, AWS DMS insère un enregistrement dans la table public.awsdms_validation_failures_v1 de l'instance de base de données cible. Cet enregistrement inclut le nom de la table, l'heure de l'erreur et des détails sur les valeurs non concordantes dans les tables source et cible.

Si vous n'ajoutez pas ce script de validation des données à la AWS DMS tâche et que les données sont insérées dans la table cible, la AWS DMS tâche affiche l'état de validation sous la forme d'enregistrements non concordants.

Lors AWS SCT de la conversion, la tâche de AWS DMS migration change le type de données de VARCHAR2 (1) en type booléen et ajoute une contrainte de clé primaire sur la `"N0"` colonne.

Création d'utilisateurs et de rôles d'application dans Aurora PostgreSQL compatible

Créée par Abhishek Verma (AWS)

Récapitulatif

Lorsque vous migrez vers l'édition compatible avec Amazon Aurora PostgreSQL, les utilisateurs et les rôles de base de données qui existent sur la base de données source doivent être créés dans la base de données compatible avec Aurora PostgreSQL. Vous pouvez créer les utilisateurs et les rôles dans Aurora PostgreSQL compatible en utilisant deux approches différentes :

- Utilisez des utilisateurs et des rôles similaires dans la base de données cible et dans la base de données source. Dans cette approche, les langages de définition des données (DDLs) sont extraits de la base de données source pour les utilisateurs et les rôles. Ils sont ensuite transformés et appliqués à la base de données cible compatible Aurora PostgreSQL. Par exemple, le billet de blog Utiliser SQL pour mapper les utilisateurs, les rôles et les autorisations d'Oracle à PostgreSQL traite de l'utilisation de l'extraction à partir d'un moteur de base de données source Oracle.
- Utilisez des utilisateurs et des rôles standardisés couramment utilisés lors du développement, de l'administration et pour effectuer d'autres opérations connexes dans la base de données. Cela inclut les opérations de lecture seule, de lecture/écriture, de développement, d'administration et de déploiement effectuées par les utilisateurs respectifs.

Ce modèle contient les autorisations requises pour la création d'utilisateurs et de rôles dans Aurora PostgreSQL compatible avec l'approche standardisée des utilisateurs et des rôles. Les étapes de création des utilisateurs et des rôles sont alignées sur la politique de sécurité qui consiste à accorder le moindre privilège aux utilisateurs de la base de données. Le tableau suivant répertorie les utilisateurs, leurs rôles correspondants et leurs informations sur la base de données.

Utilisateurs	Rôles	Objectif
`APP_read`	`APP_RO`	Utilisé pour l'accès en lecture seule au schéma `APP`
`APP_WRITE`	`APP_RW`	Utilisé pour les opérations d'écriture et de lecture sur le schéma `APP`

`APP_dev_user`	`APP_DEV`	Utilisé à des fins de développement sur le schéma`APP_DEV`, avec accès en lecture seule au schéma `APP`
`Admin_User`	`rds_superuser`	Utilisé pour effectuer des opérations d'administration sur la base de données
`APP`	`APP_DEP`	Utilisé pour créer les objets sous le `APP` schéma et pour le déploiement d'objets dans le `APP` schéma

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- Une base de données PostgreSQL, une base de données Amazon Aurora PostgreSQL Edition compatible ou une base de données Amazon Relational Database Service (Amazon RDS) pour PostgreSQL

Versions du produit

- Toutes les versions de PostgreSQL

Architecture

Pile technologique source

- Toute base de données

Pile technologique cible

- Compatible avec Amazon Aurora PostgreSQL

Architecture cible

Le schéma suivant montre les rôles des utilisateurs et l'architecture du schéma dans la base de données compatible Aurora PostgreSQL.

Automatisation et mise à l'échelle

Ce modèle contient les utilisateurs, les rôles et le script de création de schéma, que vous pouvez exécuter plusieurs fois sans aucun impact sur les utilisateurs existants de la base de données source ou cible.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.

Autres services

- psql est un outil frontal basé sur un terminal qui est installé avec chaque installation de base de données PostgreSQL. Il possède une interface de ligne de commande pour exécuter des commandes SQL, PL-PGSQL et du système d'exploitation.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Épopées

Création des utilisateurs et des rôles

Tâche	Description	Compétences requises
Créez l'utilisateur de déploiement.	L'utilisateur de déploiement APP sera utilisé pour créer et modifier les objets	DBA

Tâche	Description	Compétences requises

	de base de données lors des déploiements. Utilisez les scripts suivants pour créer le rôle d'utilisateur de déploiement APP_DEP dans le schémaAPP. Validez les droits d'accès pour vous assurer que cet utilisateur a uniquement le privilège de créer des objets dans le schéma requisAPP.
	1. Connectez-vous à l'utilisateur administrateur et créez le schéma.
	`CREATE SCHEMA APP;`
	2. Créez l'utilisateur.
	`CREATE USER APP WITH PASSWORD <password> ;`
	3. Créez le rôle.
	`CREATE ROLE APP_DEP ;`
	`GRANT all on schema APP to APP_DEP ;`
	`GRANT USAGE ON SCHEMA APP to APP_DEP ;`
	`GRANT connect on database <db_name> to APP_DEP ;`
	`GRANT APP_DEP to APP;`
	4. Pour tester les privilèges, connectez-vous aux tables APP et créez-les.	

Tâche	Description	Compétences requises

	`set search_path to APP;`
	`SET`
	`CREATE TABLE test(id integer ) ;`
	`CREATE TABLE`
	5. Vérifiez les privilèges.
	`select schemaname , tablename , tableowner from pg_tables where tablename like 'test' ;`
	`schemaname | tablename | tableowner`
	`APP | test | APP`	

Tâche	Description	Compétences requises

Créez l'utilisateur en lecture seule.	L'utilisateur en lecture seule `APP_read` sera utilisé pour effectuer l'opération en lecture seule dans le schéma. `APP` Utilisez les scripts suivants pour créer l'utilisateur en lecture seule. Validez les droits d'accès pour vous assurer que cet utilisateur a le privilège de lire uniquement les objets du schéma `APP` et d'accorder automatiquement un accès en lecture à tout nouvel objet créé dans le schéma`APP`.
	1. Créez l'utilisateur`APP_read`.
	`create user APP_read ;`
	`alter user APP_read with password 'your_password' ;`
	2. Créez le rôle.
	`CREATE ROLE APP_ro ;`
	`GRANT SELECT ON ALL TABLES IN SCHEMA APP TO APP_RO ;`
	`GRANT USAGE ON SCHEMA APP TO APP_RO`
	`GRANT CONNECT ON DATABASE testdb TO APP_RO ;`
	`GRANT APP_RO TO APP_read;`
		DBA

Tâche	Description	Compétences requises

	3. Pour tester les privilèges, connectez-vous en utilisant l'APP_readutilisateur.
	
	`set search_path to APP ;`
	`create table test1( id integer) ;`
	`ERROR: permission denied for schema APP`
	`LINE 1: create table test1( id integer) ;`
	`insert into test values (34) ;`
	`ERROR: permission denied for table test`
	`SQL state: 42501`
	`select from test`
	`no rows selected`	

Tâche	Description	Compétences requises

Créez l'utilisateur de lecture/écriture.	L'utilisateur de lecture/écriture `APP_WRITE` sera utilisé pour effectuer des opérations de lecture et d'écriture sur le schéma. APP Utilisez les scripts suivants pour créer l'utilisateur de lecture/écriture et lui attribuer le `APP_RW` rôle. Validez les droits d'accès pour vous assurer que cet utilisateur dispose de privilèges de lecture et d'écriture uniquement sur les objets du schéma APP et pour accorder automatiquement un accès en lecture et en écriture à tout nouvel objet créé dans le schémaAPP.
	
	1. Créez l'utilisateur.
	
	`CREATE USER APP_WRITE ; alter user APP_WRITE with password 'your_password' ;`
	
	2. Créez le rôle.
	
	`CREATE ROLE APP_RW; GRANT SELECT, INSERT, UPDATE, DELETE ON ALL TABLES IN SCHEMA APP TO APP_RW ; GRANT CONNECT ON DATABASE postgres to APP_RW ; GRANT USAGE ON SCHEMA APP to APP_RW ;`	

Tâche	Description	Compétences requises

	<pre>ALTER DEFAULT
	 PRIVILEGES IN SCHEMA
	 APP
	GRANT SELECT, INSERT,
	 UPDATE, DELETE ON
	 TABLES TO APP_RW ;
	GRANT APP_RW to
	 APP_WRITE</pre>
	3. Pour tester les privilèges, connectez-vous en utilisant l'`APP_WRITE` utilisateur.
	<pre>SET SEARCH_PATH to
	 APP;
	CREATE TABLE
	 test1(id integer) ;
	ERROR: permission
	 denied for schema APP
	LINE 1: create table
	 test1(id integer) ;
	SELECT * FROM test ;
	id
	---- 	
	12
	INSERT INTO test
	 values (31) ;
	INSERT 0 1</pre>	

Tâche	Description	Compétences requises

Créez l'utilisateur administrateur.	L'utilisateur admin `Admin_User` sera utilisé pour effectuer des opérations d'administration sur la base de données. Des exemples de ces opérations sont `CREATE ROLE` et`CREATE DATABASE`. `Admin_User` utilise le rôle intégré `rds_superuser` pour effectuer des opérations d'administration sur la base de données. Utilisez les scripts suivants pour créer et tester les privilèges de l'utilisateur administrateur `Admin_User` dans la base de données.
	1. Créez l'utilisateur et accordez le rôle.
	`create user Admin_User WITH PASSWORD ‘Your password’ ALTER user Admin_user CREATEDB; ALTER user Admin_user CREATEROLE;`
	2. Pour tester le privilège, connectez-vous depuis l'`Admin_User` utilisateur.
	`SELECT * FROM APP.test ; id ---- 31`
		DBA

Tâche	Description	Compétences requises

	`CREATE ROLE TEST ;`
	`CREATE DATABASE`
	`test123 ;`	

Tâche	Description	Compétences requises

Créez l'utilisateur de développement.	L'utilisateur de développement `APP_dev_user` aura le droit de créer les objets dans son schéma local `APP_DEV` et d'accéder en lecture dans le schémaAPP. Utilisez les scripts suivants pour créer et tester les privilèges de l'utilisateur `APP_dev_user` dans la base de données.
	1. Créez l'utilisateur.
	`CREATE USER APP1_dev_user with password ‘your password’;`
	2. Créez le APP_DEV schéma pour`App_dev_user` .
	`CREATE SCHEMA APP1_DEV ;`
	3. Créez le rôle APP_DEV
	`CREATE ROLE APP1_DEV ;`
	`GRANT APP1_RO to APP1_DEV ;`
	`GRANT SELECT ON ALL TABLES IN SCHEMA APP1_DEV to APP1_dev_user`
	`GRANT USAGE, CREATE ON SCHEMA APP1_DEV to APP1_DEV_USER`
	`GRANT APP1_DEV to APP1_DEV_USER ;`
		DBA

Tâche	Description	Compétences requises

	4. Pour tester les privilèges, connectez-vous depuisAPP_dev_user .
	
	`CREATE TABLE APP1_dev.test1( id integer ) ;`
	`CREATE TABLE`
	`INSERT into APP1_dev.test1 ( select * from APP1.test );`
	`INSERT 0 1`
	`CREATE TABLE APP1.test4 ( id int) ;`
	`ERROR: permission denied for schema APP1`
	`LINE 1: create table APP1.test4 ( id int) ;`	

Ressources connexes

Documentation de PostgreSQL

- CRÉER UN RÔLE
- CRÉER UN UTILISATEUR
- Rôles prédéfinis

Informations supplémentaires

Amélioration de PostgreSQL 14

PostgreSQL 14 fournit un ensemble de rôles prédéfinis qui donnent accès à certaines fonctionnalités et informations privilégiées couramment nécessaires. Les administrateurs (y compris les rôles dotés de `CREATE ROLE` privilèges) peuvent accorder ces rôles ou d'autres rôles dans leur environnement aux utilisateurs, en leur donnant accès aux fonctionnalités et informations spécifiées.

Les administrateurs peuvent autoriser les utilisateurs à accéder à ces rôles à l'aide de la `GRANT` commande. Par exemple, pour attribuer le `pg_signal_backend` rôle à`Admin_User`, vous pouvez exécuter la commande suivante.

```
GRANT pg_signal_backend TO Admin_User;
```

Le `pg_signal_backend` rôle est destiné à permettre aux administrateurs d'activer des rôles fiables, non superutilisateurs, pour envoyer des signaux à d'autres backends. Pour plus d'informations, consultez la section Amélioration de PostgreSQL 14.

Ajustement précis de l'accès

Dans certains cas, il peut être nécessaire de fournir un accès plus granulaire aux utilisateurs (par exemple, un accès basé sur des tables ou un accès basé sur des colonnes). Dans de tels cas, des rôles supplémentaires peuvent être créés pour accorder ces privilèges aux utilisateurs. Pour plus d'informations, consultez la section Subventions PostgreSQL.

Émulez Oracle DR à l'aide d'une base de données globale Aurora compatible avec PostgreSQL

Créée par HariKrishna Boorgadda (AWS)

Récapitulatif

Les meilleures pratiques en matière de reprise après sinistre (DR) d'entreprise consistent essentiellement à concevoir et à mettre en œuvre des systèmes matériels et logiciels tolérants aux pannes capables de survivre à un sinistre (continuité des activités) et de reprendre leurs activités normales (reprise des activités), avec un minimum d'intervention et, idéalement, sans perte de données. La création d'environnements tolérants aux pannes pour répondre aux objectifs de reprise après sinistre des entreprises peut s'avérer coûteuse et chronophage et nécessite un engagement fort de la part de l'entreprise.

Oracle Database propose trois approches différentes de la reprise après sinistre qui offrent le plus haut niveau de protection et de disponibilité des données par rapport à toute autre approche de protection des données Oracle.

- Appliance de restauration Oracle Zero Data Loss
- Oracle Active Data Guard
- Oracle GoldenGate

Ce modèle permet d'émuler le GoldenGate DR Oracle en utilisant une base de données globale Amazon Aurora. L'architecture de référence utilise Oracle GoldenGate pour la reprise après sinistre dans trois régions AWS. Le modèle décrit la replateforme de l'architecture source vers la base de données globale Aurora native pour le cloud basée sur l'édition compatible Amazon Aurora PostgreSQL.

Les bases de données mondiales Aurora sont conçues pour les applications ayant une présence mondiale. Une seule base de données Aurora couvre plusieurs régions AWS avec jusqu'à cinq régions secondaires. Les bases de données globales Aurora offrent les fonctionnalités suivantes :

- Réplication physique au niveau du stockage
- Lectures globales à faible latence
- Reprise après sinistre rapide en cas de panne à l'échelle de la région
- Migrations rapides entre régions

- Faible délai de réplication entre les régions
- Little-to-no impact sur les performances de votre base de données

Pour plus d'informations sur les fonctionnalités et les avantages de la base de données globale Aurora, consultez la section Utilisation des bases de données mondiales Amazon Aurora. Pour plus d'informations sur les basculements non planifiés et gérés, consultez la section Utilisation du basculement dans une base de données globale Amazon Aurora.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un pilote PostgreSQL Java Database Connectivity (JDBC) pour la connectivité des applications
- Une base de données mondiale Aurora basée sur l'édition compatible avec Amazon Aurora PostgreSQL
- Une base de données Oracle Real Application Clusters (RAC) migrée vers la base de données globale Aurora basée sur la compatibilité avec Aurora PostgreSQL

Limites des bases de données globales Aurora

- Les bases de données mondiales Aurora ne sont pas disponibles dans toutes les régions AWS. Pour obtenir la liste des régions prises en charge, consultez la section Bases de données globales Aurora avec Aurora PostgreSQL.
- Pour plus d'informations sur les fonctionnalités non prises en charge et les autres limitations des bases de données mondiales Aurora, consultez les limites des bases de données mondiales Amazon Aurora.

Versions du produit

- Amazon Aurora PostgreSQL : édition compatible 10.14 ou ultérieure

Architecture

Pile technologique source

- Base de données à quatre nœuds Oracle RAC

- Oracle GoldenGate

Architecture source

Le schéma suivant montre trois clusters dotés d'Oracle RAC à quatre nœuds dans différentes régions AWS répliqués à l'aide d'Oracle. GoldenGate

Pile technologique cible

- Une base de données globale Amazon Aurora à trois clusters basée sur la compatibilité avec Aurora PostgreSQL, avec un cluster dans la région principale, deux clusters dans différentes régions secondaires

Architecture cible

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Les bases de données mondiales Amazon Aurora s'étendent sur plusieurs régions AWS, ce qui permet des lectures globales à faible latence et une restauration rapide après les rares pannes susceptibles d'affecter une région AWS entière.

Épopées

Ajouter des régions avec des instances de base de données de lecteur

Tâche	Description	Compétences requises
Attachez un ou plusieurs clusters Aurora secondaires.	Sur la console de gestion AWS, sélectionnez Amazon Aurora. Sélectionnez le cluster principal, choisissez Actions,	DBA

Tâche	Description	Compétences requises
	puis choisissez Ajouter une région dans la liste déroulante.	
Sélectionnez la classe d'instance.	Vous pouvez modifier la classe d'instance du cluster secondaire. Toutefois, nous vous recommandons de la conserver identique à la classe d'instance de cluster principale.	DBA
Ajoutez la troisième région.	Répétez les étapes de cette épopée pour ajouter un cluster dans la troisième région.	DBA

Basculez sur la base de données globale Aurora

Tâche	Description	Compétences requises
Supprimez le cluster principal de la base de données globale Aurora.	1. Sur la page Bases de données, choisissez le cluster principal. 2. Choisissez Supprimer du cluster global pour basculer vers un cluster secondaire.	DBA
Reconfigurez l'application pour détourner le trafic d'écriture vers le cluster qui vient d'être promu.	Modifiez le point de terminaison de l'application avec celui du cluster nouvellement promu.	DBA
Arrêtez d'exécuter des opérations d'écriture sur le cluster non disponible.	Arrêtez l'application et toute activité du langage de manipulation de données	DBA

Tâche	Description	Compétences requises
	(DML) sur le cluster que vous avez supprimé.	
Créez une nouvelle base de données globale Aurora.	Vous pouvez désormais créer une base de données globale Aurora avec le cluster nouvellement promu comme cluster principal.	DBA

Démarrez le cluster principal

Tâche	Description	Compétences requises
Sélectionnez le cluster principal à démarrer dans la base de données globale.	Sur la console Amazon Aurora, dans la configura tion de la base de données globale, choisissez le cluster principal.	DBA
Démarrez le cluster.	Dans la liste déroulant e Actions, sélectionnez Démarrer. Ce processus peut prendre un certain temps. Actualisez l'écran pour voir le statut ou consultez la colonne État pour connaître l'état actuel du cluster une fois l'opération terminée.	DBA

Nettoyez les ressources

Tâche	Description	Compétences requises
Supprimez les clusters secondaires restants.	Une fois le pilote de basculement terminé, supprimez les clusters secondaires de la base de données globale.	DBA
Supprimez le cluster principal.	Supprimez le cluster.	DBA

Ressources connexes

- Utilisation de bases de données globales Amazon Aurora
- Solutions de reprise après sinistre Aurora PostgreSQL utilisant la base de données mondiale Amazon Aurora (article de blog)

SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL

Créée par Rajkumar Raghuwanshi (AWS) et Jagadish Kantubugata (AWS)

Récapitulatif

Ce modèle décrit comment implémenter le hachage Secure Hash Algorithm 1 (SHA1) pour les adresses e-mail lors de la migration de SQL Server vers Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL compatible. Une adresse e-mail est un exemple d'informations personnelles identifiables (PII). Les informations personnelles sont des informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne.

Ce modèle couvre les défis liés au maintien de valeurs de hachage cohérentes entre les différents classements de base de données et encodages de caractères, et fournit une solution utilisant les fonctions et les déclencheurs PostgreSQL. Bien que ce modèle se concentre sur le SHA1 hachage, il peut être adapté à d'autres algorithmes de hachage pris en charge par le module de PostgreSQL. `pgcrypto` Tenez toujours compte des implications de sécurité de votre stratégie de hachage et consultez des experts en sécurité si vous manipulez des données sensibles.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Base de données source SQL Server
- Base de données PostgreSQL cible (compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL)
- Expertise en codage PL/pgSQL

Limites

- Ce modèle nécessite des modifications du classement au niveau de la base de données en fonction des cas d'utilisation.
- L'impact sur les performances sur les grands ensembles de données n'a pas été évalué.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de

terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Versions du produit

- Microsoft SQL Server 2012 ou version ultérieure

Architecture

Pile technologique source

- SQL Server
- .NET Framework

Pile technologique cible

- PostgreSQL
- `pgcrypto`extension

Automatisation et mise à l'échelle

- Envisagez d'implémenter la fonction de hachage en tant que procédure stockée pour faciliter la maintenance.
- Pour les grands ensembles de données, évaluez les performances et envisagez des stratégies de traitement par lots ou d'indexation.

Outils

Services AWS

- Amazon Aurora PostgreSQL compatible est un moteur de base de données relationnelle entièrement géré et conforme à la norme ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- AWS Database Migration Service (AWS DMS) vous aide à migrer les banques de données vers AWS Cloud ou entre des combinaisons de configurations cloud et sur site.

- Amazon Relational Database Service Amazon RDS pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le. AWS Cloud
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Autres outils

- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.
- SQL Server Management Studio (SSMS) est un environnement intégré permettant de gérer n'importe quelle infrastructure SQL.

Bonnes pratiques

- Utilisez les paramètres de classement appropriés pour gérer les caractères spéciaux du côté de la base de données cible.
- Effectuez des tests approfondis avec diverses adresses e-mail, y compris les adresses contenant des caractères non ASCII.
- Maintenez la cohérence de la gestion des majuscules et des minuscules entre les couches d'application et de base de données.
- Comparez les performances des requêtes à l'aide des valeurs hachées.

Épopées

Analyser la mise en œuvre du hachage de source

Tâche	Description	Compétences requises
Passez en revue le code SQL Server.	Pour examiner le code SQL Server qui génère SHA1 des hachages, procédez comme suit :	Ingénieur de données, DBA, développeur d'applications

Tâche	Description	Compétences requises
	• Analysez l'implémentation existante du SHA1 hachage dans SQL Server. • Identifiez les méthodes exactes utilisées pour la génération de hachage. • Documentez les paramètre s d'entrée et le format de sortie. • Passez en revue toutes les conversions ou transform ations de type de données. • Examinez les paramètres de classement et leur impact.	
Documentez l'algorithme de hachage et les transformations de données.	Pour documenter l'algorit hme de hachage exact et les transformations de données, procédez comme suit : • Créez une documentation technique détaillée sur le processus de hachage. • Documentez la logique de step-by-step transformation. • Spécifiez les formats d'entrée et de sortie ainsi que les types de données. • Incluez des boîtiers et une gestion spéciale des caractères.	Développeur d'applications, ingénieur de données, DBA

Création d'une fonction de hachage PostgreSQL

Tâche	Description	Compétences requises
Créez une `pgcrypto` extension.	Pour créer l'`pgcrypto`extension, `pgAdmin/psql` exécutez la commande suivante : `CREATE EXTENSION pgcrypto;`	DBA, ingénieur de données
Implémentez une fonction PostgreSQL.	Implémentez la fonction PostgreSQL suivante pour répliquer la logique de hachage de SQL Server. À un niveau élevé, cette fonction utilise les étapes suivantes : 1. Convertit éventuellement l'entrée en majuscules. 2. Crée un SHA1 hachage de l'entrée. 3. Prend les 10 derniers octets (80 bits) de ce hachage. 4. Convertit ces octets en un entier de 64 bits. `CREATE OR REPLACE FUNCTION utility.hex_to_bigint ( par_val character varying, par_upper character varying DEFAULT 'lower'::character varying)`	Ingénieur de données, DBA, développeur d'applications

Tâche	Description	Compétences requises

	RETURNS bigint
	LANGUAGE 'plpgsql'
	AS $BODY$
	DECLARE
	    retnumber bigint;
	    digest_bytes bytea;
	BEGIN
	    if lower(par_upper)
	 = 'upper'
	    then
	        digest_bytes :=
	 digest(upper(par_v
	al), 'sha1');
	    else
	        digest_bytes :=
	 digest((par_val),
	 'sha1');
	    end if;
	    retnumber := ('x'
	 || encode(substring(d
	igest_bytes, length(di
	gest_bytes)-10+1),
	 'hex'))::bit(64)::
	bigint;
	    RETURN retnumber;
	END;
	$BODY$;	

Tâche	Description	Compétences requises

Test de la fonction.	Pour tester la fonction, utilisez des exemples de données provenant de SQL Server pour vérifier les valeurs de hachage correspondantes. Exécutez la commande suivante :
	`select 'alejandro_rosalez@example.com' as Email, utility.hex_to_bigint('alejandro_rosalez@example.com', 'upper') as HashValue;`
	`--OUTPUT`
	`/*`
	`email hashvalue`
	`"alejandro_rosalez@example.com" 451397011176045063`
	`*/`
		Développeur d'applications, DBA, ingénieur de données

Implémenter des déclencheurs pour le hachage automatique

Tâche	Description	Compétences requises
Créez des déclencheurs sur les tables pertinentes.	Pour créer des déclencheurs sur les tables pertinentes afin de générer automatiquement des valeurs de hachage lors de l'insertion ou de la mise à jour, exécutez la commande suivante :	Développeur d'applications, ingénieur de données, DBA

Tâche	Description	Compétences requises

	`CREATE OR REPLACE FUNCTION update_email_hash() RETURNS TRIGGER AS $$ BEGIN NEW.email_hash = utility.hex_to_bigint(NEW.email, 'upper'); RETURN NEW; END; $$ LANGUAGE plpgsql;`
	
	`CREATE TRIGGER email_hash_trigger BEFORE INSERT OR UPDATE ON users FOR EACH ROW EXECUTE FUNCTION update_email_hash();`	

Migrer les données existantes

Tâche	Description	Compétences requises
Développez un script de migration ou utilisez-le AWS DMS.	Développez un script de migration ou AWS DMS utilisez-le pour renseigner les valeurs de hachage des données existantes (y compris les valeurs de hachage stockées `BIGINT` dans le système source). Réalisez les tâches suivantes :	Ingénieur de données, développeur d'applications, DBA

Tâche	Description	Compétences requises
	• Créez des scripts de migration pour le transfert de données avec des valeurs de hachage. • Configurez AWS DMS les tâches avec des règles de transformation appropriées. • Configurez les points de terminaison source et cible dans. AWS DMS • Implémenter des mécanismes de gestion des erreurs et de journalisation. • Concevez une stratégie de traitement par lots pour les grands ensembles de données. • Créez des requêtes de validation pour la vérification des données.	

Tâche	Description	Compétences requises
Utilisez la nouvelle fonction de hachage de PostgreSQL.	Pour utiliser la nouvelle fonction de hachage de PostgreSQL afin de garantir la cohérence, procédez comme suit : • Mettez en œuvre des procédures de validation pour vérifier la cohérence du hachage. • Créez des scripts de comparaison entre les systèmes source et cible. • Configurez des tests automatisés pour la vérificat ion de la valeur de hachage. • Documentez toutes les incohérences et les étapes de résolution.	Développeur d'applications, DBA, ingénieur DevOps

Mettre à jour les requêtes d'application

Tâche	Description	Compétences requises
Identifiez les requêtes relatives aux applications.	Pour identifier les requêtes d'application qui utilisent des valeurs hachées, procédez comme suit : • Analysez la base de code de l'application pour les requêtes utilisant des valeurs de hachage.	Développeur d'applications, DBA, ingénieur de données

Tâche	Description	Compétences requises
	• Passez en revue les procédures stockées et les fonctions qui font référence aux opérations de hachage. • Documentez les indicateurs de performance des requêtes et les plans d'exécution. • Identifiez les dépendances des recherches basées sur le hachage. • Cartographiez les composants de l'application concernés.	
Modifiez les requêtes.	Si nécessaire, modifiez les requêtes pour utiliser la nouvelle fonction de hachage PostgreSQL. Procédez comme suit : • Refactorisez les requêtes existantes pour utiliser la fonction de hachage PostgreSQL. • Mettez à jour les procédures et les fonctions stockées. • Implémentez et testez de nouveaux modèles de requêtes. • Optimisez les requêtes modifiées pour améliorer les performances.	Développeur d'applications, DBA, ingénieur de données

Tester et valider

Tâche	Description	Compétences requises
Effectuez des tests.	Pour effectuer des tests approfondis avec un sous-ensemble de données de production, procédez comme suit : • Créez un plan de test pour la validation des sous-ensembles de données. • Extraire un échantillon représentatif des données de production. • Configurez un environnement de test avec des configurations appropriées. • Exécutez des tests de chargement et de transformation des données. • Effectuez des tests de volume et de stress.	Développeur d'applications, ingénieur de données, DBA
Vérifiez que les valeurs de hachage correspondent.	Pour vérifier que les valeurs de hachage correspondent entre SQL Server et PostgreSQL, procédez comme suit : • Développez des scripts de comparaison pour les valeurs de hachage. • Créez des rapports de validation pour le hachage.	Développeur d'applications, ingénieur de données, DBA

Tâche	Description	Compétences requises
	• Mettez en œuvre des procédures de vérification automatisées. • Documentez toute anomalie constatée. • Analysez et corrigez les incohérences de hachage.	
Vérifiez le fonctionnement de l'application.	Pour vérifier le fonctionnement de l'application à l'aide des données migrées et de la nouvelle implémentation de hachage, procédez comme suit : • Exécutez des tests d' end-to-endapplications. • Validez toutes les fonctionn alités de l'application à l'aide de données hachées. • Testez les performances des applications avec la nouvelle implémentation. • Vérifiez les intégrations et les dépendances des API.	Développeur d'applications, DBA, ingénieur de données

Résolution des problèmes

Problème	Solution
Les valeurs de hachage ne correspondent pas.	Vérifiez les codages de caractères et les classements entre la source et la cible. Pour plus d'informations, consultez Gérer les modifications de classement dans PostgreSQ

Problème	Solution
	L sur Amazon Aurora et AmazonAWS RDS (blog).

Ressources connexes

AWS Blogs

- Gérez les modifications de classement dans PostgreSQL sur Amazon Aurora et Amazon RDS
- Migrez SQL Server vers Amazon Aurora PostgreSQL en utilisant les meilleures pratiques et les leçons apprises sur le terrain

Autres ressources

- Module pgcrypto de PostgreSQL (documentation de PostgreSQL)
- Fonctions de déclenchement de PostgreSQL (documentation PostgreSQL)
- Fonction HASHBYTES de SQL Server (documentation Microsoft)

Migrez progressivement d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle SQL Developer et d'AWS SCT

Créée par Pinesh Singal (AWS)

Récapitulatif

De nombreuses stratégies et approches de migration se déroulent en plusieurs phases qui peuvent durer de quelques semaines à plusieurs mois. Pendant ce temps, vous pouvez rencontrer des retards en raison de l'application de correctifs ou de mises à niveau dans les instances de base de données Oracle source que vous souhaitez migrer vers des instances de base de données PostgreSQL. Pour éviter cette situation, nous vous recommandons de migrer progressivement le code de base de données Oracle restant vers le code de base de données PostgreSQL.

Ce modèle fournit une stratégie de migration incrémentielle sans interruption pour une instance de base de données Oracle de plusieurs téraoctets qui effectue un grand nombre de transactions après votre migration initiale et qui doit être migrée vers une base de données PostgreSQL. Vous pouvez utiliser l' step-by-stepapproche de ce modèle pour migrer progressivement une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle vers une instance de base de données Amazon RDS for PostgreSQL sans vous connecter à la console de gestion Amazon Web Services (AWS).

Le modèle utilise Oracle SQL Developer pour trouver les différences entre deux schémas dans la base de données Oracle source. Vous utilisez ensuite AWS Schema Conversion Tool (AWS SCT) pour convertir les objets de schéma de base de données Amazon RDS for Oracle en objets de schéma de base de données Amazon RDS for PostgreSQL. Vous pouvez ensuite exécuter un script Python dans l'invite de commande Windows pour créer des objets AWS SCT pour les modifications incrémentielles apportées aux objets de base de données source.

> **Note**
>
> Avant de migrer vos charges de travail de production, nous vous recommandons d'exécuter une validation de principe (PoC) pour l'approche de ce modèle dans un environnement de test ou hors production.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une instance de base de données Amazon RDS pour Oracle existante.
- Une instance de base de données Amazon RDS pour PostgreSQL existante.
- AWS SCT, installé et configuré avec des pilotes JDBC pour les moteurs de base de données Oracle et PostgreSQL. Pour plus d'informations à ce sujet, consultez les sections Installation d'AWS SCT et Installation des pilotes de base de données requis dans la documentation AWS SCT.
- Oracle SQL Developer, installé et configuré. Pour plus d'informations à ce sujet, consultez la documentation Oracle SQL Developer.
- Le `incremental-migration-sct-sql.zip` fichier (joint), téléchargé sur votre ordinateur local.

Limites

- Les exigences minimales pour votre instance de base de données Amazon RDS for Oracle source sont les suivantes :
  - Oracle versions 10.2 et ultérieures (pour les versions 10.x), 11g (versions 11.2.0.3.v1 et ultérieures) et jusqu'à 12.2, et 18c pour les éditions Enterprise, Standard, Standard One et Standard Two
- Les exigences minimales pour votre instance de base de données Amazon RDS pour PostgreSQL cible sont les suivantes :
  - PostgreSQL versions 9.4 et ultérieures (pour les versions 9.x), 10.x et 11.x
- Ce modèle utilise Oracle SQL Developer. Vos résultats peuvent varier si vous utilisez d'autres outils pour rechercher et exporter les différences de schéma.
- Les scripts SQL générés par Oracle SQL Developer peuvent générer des erreurs de transformation, ce qui signifie que vous devez effectuer une migration manuelle.
- Si les connexions de test source et cible AWS SCT échouent, assurez-vous de configurer les versions du pilote JDBC et les règles entrantes pour que le groupe de sécurité du cloud privé virtuel (VPC) accepte le trafic entrant.

Versions du produit

- instance de base de données Amazon RDS pour Oracle version 12.1.0.2 (version 10.2 et versions ultérieures)

- Instance de base de données Amazon RDS pour PostgreSQL version 11.5 (version 9.4 et versions ultérieures)
- Oracle SQL Developer version 19.1 et versions ultérieures
- AWS SCT version 1.0.632 et versions ultérieures

Architecture

Pile technologique source

- Instance de base de données Amazon RDS pour Oracle

Pile technologique cible

- Instance de base de données Amazon RDS pour PostgreSQL

Architecture source et cible

Le schéma suivant montre la migration d'une instance de base de données Amazon RDS pour Oracle vers une instance de base de données Amazon RDS pour PostgreSQL.

Le schéma montre le flux de travail de migration suivant :

1. Ouvrez Oracle SQL Developer et connectez-vous aux bases de données source et cible.
2. Générez un rapport de comparaison, puis générez le fichier de scripts SQL pour les objets de différence de schéma. Pour plus d'informations sur les rapports de différence, consultez la section Rapports de différence détaillés dans la documentation Oracle.
3. Configurez AWS SCT et exécutez le code Python.
4. Le fichier de scripts SQL est converti d'Oracle en PostgreSQL.
5. Exécutez le fichier de scripts SQL sur l'instance de base de données PostgreSQL cible.

Automatisation et évolutivité

Vous pouvez automatiser cette migration en ajoutant des paramètres supplémentaires et des modifications liées à la sécurité pour plusieurs fonctionnalités dans un seul programme à votre script Python.

Outils

- AWS SCT — AWS Schema Conversion Tool (AWS SCT) convertit votre schéma de base de données existant d'un moteur de base de données à un autre.
- Oracle SQL Developer — Oracle SQL Developer est un environnement de développement intégré (IDE) qui simplifie le développement et la gestion des bases de données Oracle dans les déploiements traditionnels et basés sur le cloud.

Code

Le `incremental-migration-sct-sql.zip` fichier (joint) contient le code source complet de ce modèle.

Épopées

Créez le fichier de scripts SQL pour les différences de schéma de base de données source

Tâche	Description	Compétences requises
Exécutez Database Diff dans Oracle SQL Developer.	1. Connectez-vous à votre instance de base de données Oracle source, choisissez Tools, puis Database Diff. 2. Choisissez votre base de données source dans Source Connection. 3. Choisissez la base de données source mise à jour ou corrigée dans Destinati on Connection. 4. Configurez les options restantes en fonction de vos besoins, choisissez Next, puis Finish pour générer le rapport de comparaison.	DBA

Tâche	Description	Compétences requises
Générez le fichier de scripts SQL.	Choisissez Generate Script pour générer les différences entre les fichiers SQL. Cela génère le fichier de scripts SQL qu'AWS SCT utilise pour convertir votre base de données d'Oracle en PostgreSQL.	DBA

Utilisez le script Python pour créer les objets de base de données cibles dans AWS SCT

Tâche	Description	Compétences requises
Configurez AWS SCT à l'aide de l'invite de commande Windows.	1. Copiez le `AWSSchemaConversionToolBatch.jar` fichier depuis votre dossier AWS SCT préinstallé et collez-le dans votre répertoire de travail. 2. Déployez le code Python à partir du `run_aws_sct_sql.py` fichier du `incremental-migration-sct-sql.zip` dossier (joint). Cela crée des fichiers .xml et .sct dans le `projects` répertoire contenant les détails de configuration de votre environnement de base de données source et cible. Il lit également le fichier de scripts SQL que vous avez	DBA

Tâche	Description	Compétences requises

	généré dans Oracle SQL Developer. Enfin, il crée des objets de fichier .sql dans le `output` répertoire.
	3. Configurez les détails de configuration de l'environnement source et cible dans le `database_migration.txt` fichier en utilisant le format suivant :
	`#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432`
	4. Modifiez les paramètres de configuration AWS SCT en fonction de vos besoins, puis copiez le fichier de scripts	

Tâche	Description	Compétences requises
	SQL dans votre répertoire de travail, dans le `input` sous-répertoire.	
Exécutez le script python.	1. Exécutez le script Python à l'aide de la commande suivante : `$ python run_aws_sct_sql.py database_migration.txt` 2. Cela crée le fichier SQL des objets de base de données. Les codes non convertis présentant des erreurs de transformation peuvent être convertis manuellement.	DBA
Création des objets dans Amazon RDS for PostgreSQL	Exécutez les fichiers SQL et créez des objets dans votre instance de base de données Amazon RDS for PostgreSQL.	DBA

Ressources connexes

- Oracle sur Amazon RDS
- PostgreSQL sur Amazon RDS
- Utilisation de l'interface utilisateur AWS SCT
- Utilisation d'Oracle comme source pour AWS SCT

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Chargez des fichiers BLOB dans TEXT en utilisant le codage de fichiers compatible avec Aurora PostgreSQL

Créée par Bhanu Ganesh Gudivada (AWS) et Jeevan Shetty (AWS)

Récapitulatif

Au cours de la migration, il arrive souvent que vous deviez traiter des données structurées et non structurées chargées à partir de fichiers sur un système de fichiers local. Les données peuvent également se trouver dans un jeu de caractères différent de celui de la base de données.

Ces fichiers contiennent les types de données suivants :

- Métadonnées : ces données décrivent la structure du fichier.
- Données semi-structurées : il s'agit de chaînes textuelles dans un format spécifique, tel que JSON ou XML. Vous pouvez peut-être faire des assertions à propos de ces données, par exemple « commencera toujours par « **<** » ou « ne contient aucun caractère de nouvelle ligne ».
- Texte intégral — Ces données contiennent généralement tous les types de caractères, y compris les caractères de nouvelle ligne et les guillemets. Il peut également être composé de caractères multi-octets en UTF-8.
- Données binaires : ces données peuvent contenir des octets ou des combinaisons d'octets, y compris des valeurs nulles et des end-of-file marqueurs.

Le chargement d'une combinaison de ces types de données peut s'avérer difficile.

Le modèle peut être utilisé avec les bases de données Oracle sur site, les bases de données Oracle qui se trouvent sur des instances Amazon Elastic Compute Cloud (Amazon EC2) sur le cloud Amazon Web Services (AWS) et Amazon Relational Database Service (Amazon RDS) pour les bases de données Oracle. Par exemple, ce modèle utilise Amazon Aurora PostgreSQL Compatible Edition.

Dans Oracle Database, à l'aide d'un pointeur `BFILE` (fichier binaire), du `DBMS_LOB` package et des fonctions du système Oracle, vous pouvez charger un fichier et le convertir en CLOB avec un codage de caractères. PostgreSQL ne prenant pas en charge le type de données BLOB lors de la migration vers une base de données Amazon Aurora PostgreSQL Edition compatible, ces fonctions doivent être converties en scripts compatibles avec PostgreSQL.

Ce modèle propose deux approches pour charger un fichier dans une seule colonne de base de données d'une base de données compatible avec Amazon Aurora PostgreSQL :

- Approche 1 — Vous importez des données depuis votre compartiment Amazon Simple Storage Service (Amazon S3) en utilisant `table_import_from_s3` la fonction de l'extension avec `aws_s3` l'option d'encodage.
- Approche 2 — Vous encodez en hexadécimal à l'extérieur de la base de données, puis vous le décodez pour afficher à `TEXT` l'intérieur de la base de données.

Nous vous recommandons d'utiliser Approach 1 car la compatibilité avec Aurora PostgreSQL est directement intégrée à l'extension. `aws_s3`

Ce modèle utilise l'exemple du chargement d'un fichier plat contenant un modèle d'e-mail, comportant des caractères multi-octets et un formatage distinct, dans une base de données compatible avec Amazon Aurora PostgreSQL.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance Amazon RDS ou une instance compatible avec Aurora PostgreSQL
- Compréhension de base du SQL et du système de gestion de base de données relationnelle (RDBMS)
- Un bucket Amazon Simple Storage Service (Amazon S3).
- Connaissance des fonctions système dans Oracle et PostgreSQL
- Package RPM HexDump -XXD-0.1.1 (inclus avec Amazon Linux 2)

> **Note**
>
> Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.

Limites

- Pour le type de `TEXT` données, la plus longue chaîne de caractères pouvant être stockée est d'environ 1 Go.

Versions du produit

- Aurora prend en charge les versions de PostgreSQL répertoriées dans les mises à jour d'Amazon Aurora PostgreSQL.

Architecture

Pile technologique cible

- Compatible avec Aurora avec PostgreSQL

Architecture cible

Approche 1 — Utilisation de aws_s3.table_import_from_s3

À partir d'un serveur sur site, un fichier contenant un modèle d'e-mail avec des caractères multioctets et un formatage personnalisé est transféré vers Amazon S3. La fonction de base de données personnalisée fournie par ce modèle utilise la `aws_s3.table_import_from_s3` fonction with `file_encoding` pour charger des fichiers dans la base de données et renvoyer les résultats de la requête sous forme de type de `TEXT` données.

1. Les fichiers sont transférés vers le compartiment S3 intermédiaire.
2. Les fichiers sont chargés dans la base de données compatible avec Amazon Aurora PostgreSQL.
3. À l'aide du client pgAdmin, la `load_file_into_clob` fonction personnalisée est déployée dans la base de données Aurora.
4. La fonction personnalisée est utilisée en interne `table_import_from_s3` avec file_encoding. La sortie de la fonction est obtenue en utilisant `array_to_string` et `array_agg` comme `TEXT` sortie.

Approche 2 — Encodage en hexadécimal à l'extérieur de la base de données et décodage pour afficher le TEXTE à l'intérieur de la base de données

Un fichier provenant d'un serveur local ou d'un système de fichiers local est converti en vidage hexadécimal. Le fichier est ensuite importé dans PostgreSQL sous forme de champ. `TEXT`

1. Convertissez le fichier en vidage hexadécimal dans la ligne de commande à l'aide de l'`xxd -p` option.

2. Téléchargez les fichiers de vidage hexadécimal dans un environnement compatible avec Aurora PostgreSQL à l'aide de `\copy` cette option, puis décodez les fichiers de vidage hexadécimal en binaire.
3. Codez les données binaires à renvoyer sous forme `TEXT` de.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

Autres outils

- pgAdmin4 est une plateforme d'administration et de développement open source pour PostgreSQL. pgAdmin4 peut être utilisé sous Linux, Unix, Mac OS et Windows pour gérer PostgreSQL.

Épopées

Approche 1 : Importer des données depuis Amazon S3 vers une version compatible avec Aurora PostgreSQL

Tâche	Description	Compétences requises
Lancez une EC2 instance.	Pour obtenir des instructions sur le lancement d'une instance, consultez Lancer votre instance.	DBA
Installez l'outil pgAdmin du client PostgreSQL.	Téléchargez et installez pgAdmin.	DBA

Tâche	Description	Compétences requises
Créez une politique IAM.	Créez une politique AWS Identity and Access Management (IAM) nommée `aurora-s3-access-pol` qui accorde l'accès au compartiment S3 dans lequel les fichiers seront stockés. Utilisez le code suivant, en le `<bucket-name>` remplaçant par le nom de votre compartiment S3. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:GetObject", "s3:AbortMultipartUpload", "s3:DeleteObject", "s3:ListMultipartUploadParts", "s3:PutObject", "s3:ListBucket" ], "Resource": [`	DBA

Tâche	Description	Compétences requises

	<pre>"arn:aws:s3:::<bucket-name>/*",
	
	"arn:aws:s3:::<bucket-name>"
	]
	}
	]
	}</pre>	

Créez un rôle IAM pour l'importation d'objets depuis Amazon S3 vers Aurora compatible avec PostgreSQL.	Utilisez le code suivant pour créer un rôle IAM nommé `aurora-s3-import-role` avec la relation de AssumeRoleconfiance. `AssumeRole` permet à Aurora d'accéder à d'autres services AWS en votre nom.
	<pre>{
	"Version": "2012-10-17",
	"Statement": [
	{
	"Effect": "Allow","Principal": {
	"Service": "rds.amazonaws.com"
	},"Action": "sts:AssumeRole"
	}
	]
	}</pre>
		DBA

Tâche	Description	Compétences requises
Associez le rôle IAM au cluster.	Pour associer le rôle IAM au cluster de base de données compatible Aurora PostgreSQL, exécutez la commande AWS CLI suivante. Modifiez `<Account-ID>` l'ID du compte AWS qui héberge la base de données compatible Aurora PostgreSQL. Cela permet à la base de données compatible Aurora PostgreSQL d'accéder au compartiment S3. `aws rds add-role-to-db-cluster --db-cluster-identifier aurora-postgres-cl --feature-name s3Import --role-arn arn:aws:iam::<Account-ID>:role/aurora-s3-import-role`	DBA
Téléchargez l'exemple sur Amazon S3.	1. Dans la section Informations supplémentaires de ce modèle, copiez le code du modèle d'e-mail dans un fichier nommé `salary.event.notification.email.vm` . 2. Téléchargez le fichier vers le compartiment S3.	DBA, propriétaire de l'application

Tâche	Description	Compétences requises
Déployez la fonction personnalisée.	1. Dans la section Informations supplémentaires, copiez le contenu du fichier `load_file_into_clob` SQL de fonction personnalisée dans une table temporaire. 2. Connectez-vous à la base de données compatible Aurora PostgreSQL et déployez-la dans le schéma de base de données à l'aide du client pgAdmin.	Propriétaire de l'application, DBA

Tâche	Description	Compétences requises

Exécutez la fonction personnalisée pour importer les données dans la base de données.	Exécutez la commande SQL suivante en remplaçant les éléments entre crochets par les valeurs appropriées.
	
	`select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	
	Remplacez les éléments entre crochets par les valeurs appropriées, comme indiqué dans l'exemple suivant, avant d'exécuter la commande.
	
	`Select load_file _into_clob('aws-s3 -import-test'::tex t,'us-west-1'::tex t,'employee.salary .event.notificatio n.email.vm'::text);`
	
	La commande charge le fichier depuis Amazon S3 et renvoie le résultat sous la forme`TEXT`.
		Propriétaire de l'application, DBA

Approche 2 : convertir le fichier modèle en un dump hexadécimal dans un système Linux local

Tâche	Description	Compétences requises
Convertissez le fichier modèle en un dump hexadécimal.	**Note** L'utilitaire Hexdump affiche le contenu des fichiers binaires en hexadécimal, décimal, octal ou ASCII. La `hexdump` commande fait partie du `util-linux` package et est préinstallée dans les distributions Linux. Le package Hexdump RPM fait également partie d'Amazon Linux 2. (: Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.) Pour convertir le contenu du fichier en un dump hexadécimal, exécutez la commande shell suivante. `xxd -p </path/file.vm> | tr -d '\n' > </path/file.hex>`	DBA

Tâche	Description	Compétences requises
	Remplacez le chemin et le fichier par les valeurs appropriées, comme indiqué dans l'exemple suivant. `xxd -p employee.salary.event.notification.email.vm | tr -d '\n' > employee.salary.event.notification.email.vm.hex`	

Tâche	Description	Compétences requises

Chargez le fichier hexdump dans le schéma de base de données.	Utilisez les commandes suivantes pour charger le fichier hexdump dans la base de données compatible Aurora PostgreSQL.
	
	1. Connectez-vous à la base de données Aurora PostgreSQL et créez une nouvelle table appelée. `email_template_hex`
	
	`CREATE TABLE email_template_hex(hex_data TEXT);`
	
	2. Chargez les fichiers du système de fichiers local dans le schéma de base de données à l'aide de la commande suivante.
	
	`\copy email_template_hex FROM '/path/file.hex';`
	
	Remplacez le chemin par son emplacement sur votre système de fichiers local.
	
	`\copy email_template_hex FROM '/tmp/employee.salary.event.notification.email.vm.hex';`
		DBA

Tâche	Description	Compétences requises

	3. Créez une autre table appeléeemail_template_bytea .
	
	`CREATE TABLE email_template_bytea(hex_data bytea);`
	
	4. Insérez les données de email_template_hex dansemail_template_bytea .
	
	`INSERT INTO email_template_bytea (hex_data)`
	
	`(SELECT decode(hex_data, 'hex') FROM email_template_hex limit 1);`
	
	5. Pour renvoyer du code hexadécimal sous forme de TEXT données, exécutez la commande suivante.
	
	`SELECT encode(hex_data::bytea, 'escape') FROM email_template_bytea;`	

Ressources connexes

Références

- Utilisation d'une base de données PostgreSQL comme cible pour AWS Database Migration Service

- Manuel de migration d'Oracle Database 19c vers Amazon Aurora avec compatibilité avec PostgreSQL (12.4)
- Création de politiques IAM
- Associer un rôle IAM à un cluster de base de données Amazon Aurora MySQL
- pgAdmin

Didacticiels

- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)
- Migrer d'Oracle vers Amazon Aurora

Informations supplémentaires

Fonction personnalisée load_file_into_clob

```
CREATE OR REPLACE FUNCTION load_file_into_clob(
    s3_bucket_name text,
    s3_bucket_region text,
    file_name text,
    file_delimiter character DEFAULT '&'::bpchar,
    file_encoding text DEFAULT 'UTF8'::text)
    RETURNS text
    LANGUAGE 'plpgsql'
    COST 100
    VOLATILE PARALLEL UNSAFE
AS $BODY$
DECLARE
    blob_data BYTEA;
    clob_data TEXT;
    l_table_name CHARACTER VARYING(50) := 'file_upload_hex';
    l_column_name CHARACTER VARYING(50) := 'template';
    l_return_text TEXT;
    l_option_text CHARACTER VARYING(150);
    l_sql_stmt CHARACTER VARYING(500);

BEGIN

    EXECUTE format ('CREATE TEMPORARY TABLE %I (%I text, id_serial serial)',
 l_table_name, l_column_name);
```

```
    l_sql_stmt := 'select ''(format text, delimiter ''''' || file_delimiter || ''''',
 encoding ''''' || file_encoding ||  ''''')'' ';

    EXECUTE FORMAT(l_sql_stmt)
    INTO l_option_text;

    EXECUTE FORMAT('SELECT aws_s3.table_import_from_s3($1,$2,$6,
 aws_commons.create_s3_uri($3,$4,$5))')
    INTO l_return_text
    USING l_table_name, l_column_name, s3_bucket_name,
 file_name,s3_bucket_region,l_option_text;

    EXECUTE format('select array_to_string(array_agg(%I order by id_serial),E''\n'')
 from %I', l_column_name, l_table_name)
    INTO clob_data;

    drop table file_upload_hex;

    RETURN clob_data;
END;
$BODY$;
```

Modèle d'e-mail

```
##############################################################################################
##
 ##
##    johndoe Template Type: email
 ##
##    File: johndoe.salary.event.notification.email.vm
 ##
##    Author: Aimée Étienne    Date 1/10/2021
      ##
##  Purpose: Email template used by EmplmanagerEJB to inform a johndoe they         ##
##        have been given access to a salary event
 ##
##    Template Attributes:
 ##
##        invitedUser - PersonDetails object for the invited user
  ##
##        salaryEvent - OfferDetails object for the event the user was given access
 ##
```

```
##        buyercollege - CompDetails object for the college owning the salary event
 ##
##        salaryCoordinator - PersonDetails of the salary coordinator for the event
 ##
##        idp - Identity Provider of the email recipient
 ##
##        httpWebRoot - HTTP address of the server
 ##
##
 ##
#################################################################################

$!invitedUser.firstname $!invitedUser.lastname,

Ce courriel confirme que vous avez ete invite par $!salaryCoordinator.firstname $!
salaryCoordinator.lastname de $buyercollege.collegeName a participer a l'evenement
 "$salaryEvent.offeringtitle" sur johndoeMaster Sourcing Intelligence.

Votre nom d'utilisateur est $!invitedUser.username

Veuillez suivre le lien ci-dessous pour acceder a l'evenement.

${httpWebRoot}/myDashboard.do?idp=$!{idp}

Si vous avez oublie votre mot de passe, utilisez le lien "Mot de passe oublie" situe
 sur l'ecran de connexion et entrez votre nom d'utilisateur ci-dessus.

Si vous avez des questions ou des preoccupations, nous vous invitons a
 communiquer avec le coordonnateur de l'evenement $!salaryCoordinator.firstname $!
salaryCoordinator.lastname au ${salaryCoordinator.workphone}.

*******

johndoeMaster Sourcing Intelligence est une plateforme de soumission en ligne pour les
 equipements, les materiaux et les services.

Si vous avez des difficultes ou des questions, envoyez un courriel a
 support@johndoeMaster.com pour obtenir de l'aide.
```

Migrer Amazon RDS for Oracle vers Amazon RDS for PostgreSQL avec et en utilisant et AWS SCTAWS DMSAWS CLIAWS CloudFormation

Créée par Pinesh Singal (AWS)

Récapitulatif

Ce modèle montre comment migrer une instance de base de données Amazon Relational Database Service (Amazon RDS) de plusieurs téraoctets pour Oracle vers une instance de base de données Amazon RDS for PostgreSQL à l'aide du (). AWS Command Line Interface AWS CLI Cette approche permet un temps d'arrêt minimal et ne nécessite pas de connexion au AWS Management Console.

Ce modèle permet d'éviter les configurations manuelles et les migrations individuelles en utilisant les consoles AWS Schema Conversion Tool (AWS SCT) et AWS Database Migration Service (AWS DMS). La solution met en place une configuration unique pour plusieurs bases de données et effectue les migrations en utilisant AWS SCT et AWS DMS dans le AWS CLI.

Le modèle est utilisé AWS SCT pour convertir des objets de schéma de base de données d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL, AWS DMS puis pour migrer les données. À l'aide de scripts Python AWS CLI, vous créez des AWS SCT objets et des AWS DMS tâches à l'aide d'un AWS CloudFormation modèle.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Une instance de base de données Amazon RDS pour Oracle existante.
- Une instance de base de données Amazon RDS pour PostgreSQL existante.
- Une instance Amazon Elastic Compute Cloud (Amazon EC2) ou une machine locale avec un système d'exploitation Windows ou Linux pour exécuter des scripts.
- Compréhension des types de tâches de AWS DMS migration suivants :`full-load`,`cdc`,`full-load-and-cdc`. Pour plus d'informations, consultez la section Création d'une tâche dans la AWS DMS documentation.
- AWS SCT, installé et configuré avec les pilotes Java Database Connectivity (JDBC) pour les moteurs de base de données Oracle et PostgreSQL. Pour plus d'informations, consultez la section Installation et configuration AWS SCT dans la AWS SCT documentation.
- Le `AWSSchemaConversionToolBatch.jar` fichier du AWS SCT dossier installé, copié dans votre répertoire de travail.

- Le `cli-sct-dms-cft.zip` fichier (joint), téléchargé et extrait dans votre répertoire de travail.
- Version la plus récente du moteur d'instance de AWS DMS réplication. Pour plus d'informations, consultez la section Comment créer une instance de AWS DMS réplication dans la AWS Support documentation et les notes AWS DMS de publication.
- AWS CLI version 2, installée et configurée avec votre identifiant de clé d'accès, votre clé d'accès secrète et le Région AWS nom par défaut de l' EC2 instance ou du système d'exploitation sur lequel les scripts sont exécutés. Pour plus d'informations, consultez les sections Installation ou mise à jour vers la dernière version AWS CLI et Configuration des paramètres correspondants AWS CLI dans la AWS CLI documentation.
- Connaissance des AWS CloudFormation modèles. Pour plus d'informations, consultez la section AWS CloudFormation Fonctionnement de la AWS CloudFormation documentation.
- Python version 3, installé et configuré sur l' EC2 instance ou le système d'exploitation sur lequel les scripts sont exécutés. Pour plus d'informations, consultez la documentation Python.

Limites

- Les exigences minimales pour votre instance de base de données Amazon RDS for Oracle source sont les suivantes :
  - Versions Oracle 12c (12.1.0.2, 12.2.0.1), 18c (18.0.0.0) et 19c (19.0.0.0) pour les éditions Enterprise, Standard, Standard One et Standard Two.
  - Bien qu'Amazon RDS prenne en charge Oracle 18c (18.0.0.0), cette version est sur le point de devenir obsolète car Oracle ne fournit plus de correctifs pour 18c après cette date. end-of-support Pour plus d'informations, consultez Amazon RDS pour Oracle dans la documentation Amazon RDS.
  - Amazon RDS pour Oracle 11g n'est plus pris en charge.
- Les exigences minimales pour votre instance de base de données Amazon RDS pour PostgreSQL cible sont les suivantes :
  - PostgreSQL versions 9 (9.5 et 9.6), 10.x, 11.x, 12.x et 13.x

Versions du produit

- Instance de base de données Amazon RDS pour Oracle, versions 12.1.0.2 et ultérieures
- Instance de base de données Amazon RDS pour PostgreSQL version 11.5 et ultérieure
- AWS CLI version 2

- La dernière version de AWS SCT
- La dernière version de Python 3

Architecture

Pile technologique source

- Amazon RDS for Oracle

Pile technologique cible

- Amazon RDS for PostgreSQL

Architecture source et cible

Le schéma suivant montre la migration d'une instance de base de données Amazon RDS pour Oracle vers une instance de base de données Amazon RDS for AWS DMS PostgreSQL à l'aide de scripts Python.

Le schéma montre le flux de travail de migration suivant :

1. Le script Python permet AWS SCT de se connecter aux instances de base de données source et cible.
2. L'utilisateur AWS SCT commence par le script Python, convertit le code Oracle en code PostgreSQL et l'exécute sur l'instance de base de données cible.
3. Le script Python crée des tâches de AWS DMS réplication pour les instances de base de données source et cible.
4. L'utilisateur déploie des scripts Python pour démarrer les AWS DMS tâches, puis les arrête une fois la migration des données terminée.

Automatisation et évolutivité

Vous pouvez automatiser cette migration en ajoutant des paramètres et des modifications liées à la sécurité à votre script Python, afin de fournir des fonctionnalités supplémentaires.

Outils

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS CloudFormationvous aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions. Ce modèle convertit le fichier `.csv` d'entrée en fichier d'`.json`entrée à l'aide d'un script Python. Le `.json` fichier est utilisé dans AWS CLI les commandes pour créer une AWS CloudFormation pile qui crée plusieurs tâches de AWS DMS réplication avec Amazon Resource Names (ARNs), des types de migration, des paramètres de tâches et des mappages de tables.
- AWS Database Migration Service (AWS DMS) vous aide à migrer les banques de données vers AWS Cloud ou entre des combinaisons de configurations cloud et sur site. Ce modèle est utilisé AWS DMS pour créer, démarrer et arrêter des tâches avec un script Python qui s'exécute sur la ligne de commande et pour créer le AWS CloudFormation modèle.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible. Ce modèle nécessite que le `AWSSchemaConversionToolBatch.jar` fichier se trouve dans le AWS SCT répertoire installé.

Code

Le `cli-sct-dms-cft.zip` fichier (joint) contient le code source complet de ce modèle.

Épopées

Configurer AWS SCT et créer des objets de base de données dans AWS CLI

Tâche	Description	Compétences requises
Configurez AWS SCT pour exécuter à partir du AWS CLI.	1. Configurez les détails de configuration de l'environ nement source et cible dans le `database_migration .txt` fichier en utilisant le format suivant :	DBA

Tâche	Description	Compétences requises

	`#source_vendor,source_hostname,source_dbname,source_user,source_pwd,source_schema,source_port,source_sid,target_vendor,target_hostname,target_user,target_pwd,target_dbname,target_port`
	`ORACLE,myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com,ORCL,orcl,orcl1234,orcl,1521,ORCL,POSTGRESQL,mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com,pguser,pgpassword,pgdb,5432`
	2. Modifiez les paramètres AWS SCT de configuration en fonction de vos besoins dans les fichiers suivants :`project_settings.xml` ,`Oracle_PG_Test_Batch.xml` , et`ORACLE-orcl-to-POSTGRESQL.xml` .	

Tâche	Description	Compétences requises
Exécutez le script `run_aws_sct.py` Python.	Exécutez le script `run_aws_sct.py` Python à l'aide de la commande suivante : `$ python run_aws_sct.py database_migration.txt` Le script Python convertit les objets de base de données d'Oracle en PostgreSQL et crée des fichiers SQL au format PostgreSQL. Le script crée également le fichier PDF`Database migration assessment report` , qui fournit des recommandations détaillées et des statistiques de conversion pour les objets de base de données.	DBA
Créez des objets dans Amazon RDS for PostgreSQL.	1. Modifiez manuellement les fichiers SQL générés par AWS SCT, si nécessaire. 2. Exécutez les fichiers SQL et créez des objets dans votre instance de base de données Amazon RDS for PostgreSQL.	DBA

Configurez et créez AWS DMS des tâches à l'aide AWS CLI des AWS CloudFormation

Tâche	Description	Compétences requises
Créez une instance AWS DMS de réplication.	Connectez-vous à la AWS DMS console AWS Management Console, ouvrez-la et créez une instance de réplication configurée en fonction de vos besoins. Pour plus d'informations, consultez les sections Création d'une instance de réplication dans la AWS DMS documentation et Comment créer une instance de AWS DMS réplication dans la AWS Support documentation.	DBA
Créez le point de terminaison source.	Sur la AWS DMS console, choisissez Endpoints, puis créez un point de terminaison source pour la base de données Oracle en fonction de vos besoins. **Note** L'attribut de connexion supplémentaire doit `numberDataTypeScale` comporter une `-2` valeur.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Création de points de terminaison source et cible dans la AWS DMS documentation.	
Créez le point de terminaison cible.	Sur la AWS DMS console, choisissez Endpoints, puis créez un point de terminaison cible pour la base de données PostgreSQL en fonction de vos besoins. Pour plus d'informations, consultez la section Création de points de terminaison source et cible dans la AWS DMS documentation.	DevOps ingénieur

Tâche	Description	Compétences requises

Configurez les détails de AWS DMS réplication à exécuter à partir du AWS CLI.	Configurez les points de terminaison AWS DMS source et cible ainsi que les détails de réplication dans le `dms-arn-list.txt` fichier avec l'ARN du point de terminaison source, l'ARN du point de terminaison cible et l'ARN de l'instance de réplication en utilisant le format suivant :
	`#sourceARN,targetARN,repARN`
	`arn:aws:dms:us-east-1:123456789012:endpoint:EH7AINRUDZ5GOYIY6HVMXECMCQ`
	`arn:aws:dms:us-east-1:123456789012:endpoint:HHJVUV57N7O3CQF4PJZKGIOYY5`
	`arn:aws:dms:us-east-1:123456789012:rep:LL57N77AQQAHHJF4PJFHNEDZ5G`
		DBA

Tâche	Description	Compétences requises
Exécutez le script `dms-create-task.py` Python pour créer les AWS DMS tâches.	1. Exécutez le script `dms-create-task.py` Python à l'aide de la commande suivante : `$ python dms-create-task.py database_migration.txt dms-arn-list.txt <cft-stack-name> <migration-type>` où : • `database_migration.txt` est le fichier texte de migration de base de données. • `dms-arn-list.txt` est la liste des ARN pour AWS DMS. • `<cft-stack-name>`est le nom de AWS CloudFormation pile défini par l'utilisateur. • `<migration-type>` a pour valeur `full-load` , `cdc` ou `full-load-and-cdc`. 2. En fonction de votre type de migration, vous pouvez utiliser les commandes suivantes pour créer trois types de AWS DMS tâches :	DBA

Tâche	Description	Compétences requises
	• `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack full-load` • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack cdc` • `$ python dms-create-task.py database_migration.txt dms-arn-list.txt dms-cli-cft-stack full-load-and-cdc`	
Vérifiez que AWS DMS les tâches sont prêtes.	Sur la AWS DMS console, vérifiez le `Ready` statut de vos AWS DMS tâches dans la section État.	DBA

Démarrez et arrêtez les AWS DMS tâches à l'aide du AWS CLI

Tâche	Description	Compétences requises
Commencez les AWS DMS tâches.	Exécutez le script `dms-start-task.py` Python à l'aide de la commande suivante :	DBA

Tâche	Description	Compétences requises
	`$ python dms-start-task.py start '<cdc-start-datetime>'` **Note** La date et l'heure de début doivent être au `'YYYY-MM-DDTHH:MI:SS'` format `'DD-MON-YYYY'` ou (par exemple, `'01-Dec-2019'` ou `'2018-03-08T12:12:12'`). Vous pouvez consulter l'état des AWS DMS tâches dans l'onglet Tableau des statistiques de la page Tâches de la AWS DMS console.	

Tâche	Description	Compétences requises
Validez les données.	1. Une fois la migration à chargement complet terminée, la tâche continue de s'exécuter pour CDC. 2. Lorsque le CDC est terminé ou qu'aucune autre modification ne doit être migrée, passez en revue et validez les résultats et les données de la tâche de migration dans vos bases de données Oracle et PostgreSQL. Vous pouvez valider vos données en vérifiant les colonnes de statut et de nombre (`Validation state`,`Validation pending`, `Validation failed` `Validation suspended` , et`Validation details`) dans l'onglet Statistiques des tables de votre tâche de migration de base de données sur la page Tâches de la AWS DMS console. Pour plus d'informations, consultez la section validation AWS DMS des données dans la AWS DMS documentation.	DBA

Tâche	Description	Compétences requises
Arrêtez les AWS DMS tâches.	Exécutez le script Python à l'aide de la commande suivante : `$ python dms-start-task.py stop` **Note** AWS DMS les tâches peuvent s'arrêter avec un `failed` statut, en fonction de l'état de validation. Pour plus d'informations, consultez la section suivante, .	DBA

Résolution des problèmes

Problème	Solution
AWS SCT les connexions de test source et cible échouent.	Configurez les versions du pilote JDBC et les règles entrantes du groupe de sécurité VPC pour accepter le trafic entrant.
L'exécution du test du point de terminaison source ou cible échoue.	Vérifiez si les paramètres du point de terminaison et l'instance de réplication sont en `Available` état. Vérifiez si l'état de la connexion du terminal est`Successful` . Pour plus d'informations, consultez la section Comment résoudre les problèmes de connectiv

Problème	Solution
	ité des terminaux AWS DMS dans la AWS Support documentation.
L'exécution à chargement complet échoue.	Vérifiez si les types et les tailles de données des bases de données source et cible correspondent. Pour plus d'informations, consultez la section Résolution des problèmes liés aux tâches de migration AWS DMS dans la AWS DMS documentation.
Vous rencontrez des erreurs lors de l'exécution de la validation.	Vérifiez si la table possède une clé primaire car les tables non primaires ne sont pas validées. Si la table contient une clé primaire et des erreurs, vérifiez que l'attribut de connexion supplémentaire du point de terminaison source en possède un`numberDataTypeScale=-2` . Pour plus d'informations, consultez les sections Paramètres du point de terminaison lors de l'utilisation d'Oracle comme source pour AWS DMSOracleSettings, et Résolution des problèmes dans la AWS DMS documentation.

Ressources connexes

- Installation et configuration AWS SCT
- Présentation AWS DMS (vidéo)
- Exemples de commandes d'opération de CloudFormation pile pour AWS CLI et PowerShell
- Naviguer dans l'interface utilisateur du AWS SCT
- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Connexion aux bases de données Oracle avec AWS SCT

- Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS
- Sources pour la migration des données
- Objectifs de migration des données
- formation sur le cloud (AWS CLI documentation)
- create-stack (documentation)AWS CLI
- dms (AWS CLI documentation)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS

Créée par Pinesh Singal (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle vers une base de données Amazon RDS for PostgreSQL sur le cloud Amazon Web Services (AWS). Pour chiffrer les connexions entre les bases de données, le modèle utilise l'autorité de certification (CA) et le mode SSL dans Amazon RDS et AWS Database Migration Service (AWS DMS).

Le modèle décrit une stratégie de migration en ligne avec peu ou pas de temps d'arrêt pour une base de données source Oracle de plusieurs téraoctets comportant un grand nombre de transactions. Pour la sécurité des données, le modèle utilise le protocole SSL lors du transfert des données.

Ce modèle utilise AWS Schema Conversion Tool (AWS SCT) pour convertir le schéma de base de données Amazon RDS for Oracle en schéma Amazon RDS for PostgreSQL. Le modèle utilise ensuite AWS DMS pour migrer les données de la base de données Amazon RDS for Oracle vers la base de données Amazon RDS for PostgreSQL.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorité de certification (CA) de base de données Amazon RDS configurée uniquement avec rds-ca-rsa2048-g1
  - Le certificat rds-ca-2019 a expiré en août 2024.
  - Le certificat rds-ca-2015 a expiré le 5 mars 2020.
- AWS SCT
- AWS DMS
- pgAdmin
- Outils SQL (par exemple, SQL Developer ou SQL*Plus)

Limites

- Base de données Amazon RDS for Oracle : la configuration minimale requise concerne les versions 19c d'Oracle pour les éditions Enterprise et Standard Two.
- Base de données Amazon RDS for PostgreSQL : la configuration minimale requise est celle de PostgreSQL version 12 et ultérieure (pour les versions 9.x et ultérieures).

Versions du produit

- Instance de base de données Amazon RDS for Oracle version 12.1.0.2
- Instance de base de données Amazon RDS for PostgreSQL version 11.5

Architecture

Pile technologique source

- Une instance de base de données Amazon RDS for Oracle avec la version 12.1.0.2.v18.

Pile technologique cible

- AWS DMS
- Une instance de base de données Amazon RDS for PostgreSQL avec la version 11.5.

Architecture cible

Le schéma suivant montre l'architecture de l'architecture de migration des données entre les bases de données Oracle (source) et PostgreSQL (cible). L'architecture inclut les éléments suivants :

- Un cloud privé virtuel (VPC)
- Une zone de disponibilité
- Un sous-réseau privé
- Une base de données Amazon RDS for Oracle
- Une instance de réplication AWS DMS
- Une base de données RDS pour PostgreSQL

Pour chiffrer les connexions pour les bases de données source et cible, les modes CA et SSL doivent être activés dans Amazon RDS et AWS DMS.

Outils

Services AWS

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.
- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Autres services

- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Bonnes pratiques

Dans le cadre des bonnes pratiques de sécurité AWS, Amazon RDS fournit de nouveaux certificats d'autorité de certification. Pour plus d'informations sur les nouveaux certificats et les régions AWS prises en charge, consultez Utilisation du protocole SSL/TLS pour chiffrer une connexion à une instance ou à un cluster de base de données.

Si votre instance RDS possède actuellement un certificat CA et que vous souhaitez passer à un certificat CA `rds-ca-2019rds-ca-rsa2048-g1`, suivez les instructions de la section Mise à jour de votre certificat CA en modifiant votre instance ou cluster de base de données ou de la section Mise à jour de votre certificat CA en appliquant la maintenance.

Épopées

Configuration de l'instance Amazon RDS pour Oracle

Tâche	Description	Compétences requises
Créez l'instance de base de données Oracle.	Connectez-vous à votre compte AWS, ouvrez l'AWS Management Console et accédez à la console Amazon RDS. Sur la console, choisissez Créer une base de données, puis Oracle.	AWS, DBA en général
Configurez les groupes de sécurité.	Configurez les groupes de sécurité entrants et sortants.	AWS général
Créez un groupe d'options.	Créez un groupe d'options dans le même VPC et le même groupe de sécurité que la base de données Amazon RDS for Oracle. Pour Option, choisissez SSL. Pour Port, choisissez 2484 (pour les connexions SSL).	AWS général
Configurez les paramètres des options.	Utilisez les paramètres suivants : • `SQLNET.CIPHER_SUITE : SSL_RSA_WITH_AES_256_CBC_SHA` • `SQLNET.SSL_VERSION : 1.2 or 1.0`	AWS général
Modifiez l'instance de base de données RDS pour Oracle.	Définissez le certificat CA comme rds-ca-rsa2048-g1.	DBA, AWS général

Tâche	Description	Compétences requises
	Sous Groupe d'options, attachez le groupe d'options créé précédemment.	

Tâche	Description	Compétences requises

Vérifiez que l'instance de base de données RDS pour Oracle est disponible.	Assurez-vous que l'instance de base de données Amazon RDS for Oracle est opérationnelle et que le schéma de base de données est accessible.
	
	Pour vous connecter au RDS pour Oracle DB, utilisez la `sqlplus` commande depuis la ligne de commande.
	
	`$ sqlplus orcl/**** @myoracledb.cokmvis0v46q.us-east-1.rds.amazonaws.com:1521/ORCL`
	`SQL*Plus: Release 12.1.0.2.0 Production on Tue Oct 15 18:11:07 2019`
	`Copyright (c) 1982, 2016, Oracle. All rights reserved.`
	`Last Successful login time: Mon Dec 16 2019 23:17:31 +05:30`
	`Connected to:`
	`Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production`
	`With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options`
	`SQL>`
		DBA

Tâche	Description	Compétences requises
Créez des objets et des données dans la base de données RDS pour Oracle.	Créez des objets et insérez des données dans le schéma.	DBA

Configuration de l'instance Amazon RDS pour PostgreSQL

Tâche	Description	Compétences requises
Créez la base de données RDS pour PostgreSQL.	Sur la page Créer une base de données de la console Amazon RDS, choisissez PostgreSQL pour créer une instance de base de données Amazon RDS for PostgreSQL.	DBA, AWS général
Configurez les groupes de sécurité.	Configurez les groupes de sécurité entrants et sortants.	AWS général
Créez un groupe de paramètres.	Si vous utilisez PostgreSQL version 11.x, créez un groupe de paramètres pour définir les paramètres SSL. Dans PostgreSQL version 12, le groupe de paramètres SSL est activé par défaut.	AWS général
Modifiez les paramètres.	Modifiez le `rds.force_ssl` paramètre sur 1 (activé). Par défaut, le `ssl` paramètre est 1 (activé). En définissant le `rds.force_ssl` paramètre sur1, vous forcez toutes les connexions à se connecter uniquement via le mode SSL.	AWS général

Tâche	Description	Compétences requises
Modifiez l'instance de base de données RDS pour PostgreSQL.	Définissez le certificat CA comme rds-ca-rsa2048-g1. Attachez le groupe de paramètres par défaut ou le groupe de paramètres créé précédemment, selon votre version de PostgreSQL.	DBA, AWS général

Tâche	Description	Compétences requises

Vérifiez que l'instance de base de données RDS pour PostgreSQL est disponible.	Assurez-vous que la base de données Amazon RDS for PostgreSQL est opération nelle.
	
	La `psql` commande établit une connexion SSL avec `sslmode` set depuis la ligne de commande.
	
	L'une des options consiste `sslmode=1` à définir le groupe de paramètres et à utiliser une `psql` connexion sans inclure le `sslmode` paramètre dans la commande.
	
	Le résultat suivant indique que la connexion SSL est établie.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
	`pgdb=>`
		DBA

Tâche	Description	Compétences requises

	Une deuxième option consiste à le définir `sslmode=1` dans le groupe de paramètres et à inclure le `sslmode` paramètre dans la `psql` commande.
	
	Le résultat suivant indique que la connexion SSL est établie.
	
	`$ psql -h mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com -p 5432 "dbname=pgdb user=pguser sslmode=require"`
	`Password for user pguser:`
	`psql (11.3, server 11.5)`
	`SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)`
	`Type "help" for help.`
	`pgdb=>`	

Configuration et exécution d'AWS SCT

Tâche	Description	Compétences requises
Installer AWS SCT.	Installez la dernière version de l'application AWS SCT.	AWS général
Configurez AWS SCT avec des pilotes JDBC.	Téléchargez les pilotes Java Database Connectivity (JDBC) pour Oracle (ojdbc8.jar)	AWS général

Tâche	Description	Compétences requises
	et PostgreSQL (postgresql-42.2.5.jar). Pour configurer les pilotes dans AWS SCT, choisissez Paramètres, Paramètres globaux, Pilotes.	

Tâche	Description	Compétences requises
Créez le projet AWS SCT.	Créez le projet et le rapport AWS SCT en utilisant Oracle comme moteur de base de données source et Amazon RDS for PostgreSQL comme moteur de base de données cible : 1. Testez les connexions à la base de données Oracle source et à la base de données Amazon RDS for PostgreSQL cible en fournissant les détails de connexion. Pour la base de données Oracle source, les autorisations ou privilèges suivants sont requis : • `CONNECT` • `SELECT_CATALOG_ROLE` • `SELECT ANY DICTIONARY` • `SELECT on SYS.USER$ TO <sct_user>` Pour plus d'informations, consultez la section Utilisation de la base de données Oracle comme source pour AWS SCT.	AWS général

Tâche	Description	Compétences requises
	Les connexions source et cible doivent réussir avant qu'AWS SCT puisse démarrer le rapport de migration. 2. Après le rapport, entrez le schéma à convertir, puis choisissez Terminer.	

Tâche	Description	Compétences requises
Validez les objets de base de données	1. Choisissez Charger le schéma. AWS SCT affiche la source et les objets cibles convertis , y compris les objets présentant des erreurs. Mettez à jour tous les objets incorrects dans la base de données cible. 2. Passez en revue les erreurs et éliminez-les à l'aide d'une intervention manuelle. 3. Une fois toutes les erreurs corrigées, choisissez à nouveau Charger le schéma. 4. Choisissez Appliquer à la base de données. 5. Connectez-vous à pgAdmin ou à n'importe quel outil prenant en charge une connexion à une base de données PostgreSQL, et vérifiez le schéma et les objets.	DBA, AWS général

Configuration et exécution d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication.	1. Connectez-vous à votre compte, ouvrez l'AWS	AWS général

Tâche	Description	Compétences requises
	Management Console et accédez à la console AWS DMS. 2. Créez une instance de réplication avec des paramètres valides pour le VPC, le groupe de sécurité, la zone de disponibilité et des attributs de connexion supplémentaires.	
Importez le certificat.	Téléchargez le bundle de certificats (PEM) pour votre région AWS. Le bundle contient à la fois le certificat `rds-ca-2019` intermédiaire et le certifica t racine. Le bundle contient également les certificats CA `rds-ca-rsa2048-g1` `rds-ca-rsa4096-g1` ,, et `rds-ca-ecc384-g1` racine. Le magasin de confiance de votre application doit uniquemen t enregistrer le certificat CA racine.	AWS général

Tâche	Description	Compétences requises
Créez le point de terminaison source.	1. Créez un point de terminaison source pour Amazon RDS pour Oracle en choisissant Select RDS DB instance, puis en sélectionnant l'instance DB RDS for Oracle que vous avez créée. Les détails de configuration du point de terminaison seront automatiquement renseignés. 2. Choisissez Fournir les informations d'accès manuellement. Pour Port, assurez-vous de saisir 2484. 3. En mode SSL (Secure Socket Layer), choisisse `zverify-ca` , puis choisissez le certificat CA que vous avez créé précédemment. 4. Sous Paramètres du point de terminaison, ajoutez l'attribut de connexion supplémentaire `NumberDataTypeScale=-2` pour prendre en charge le type de `NUMBER` données sans taille.	AWS général

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Utilisation d'une base de données Oracle comme source pour AWS Database Migration Service.	
Créez le point de terminaison cible.	1. Créez un point de terminaison cible pour Amazon RDS pour PostgreSQL en choisissant Select RDS DB instance, puis en sélectionnant votre instance DB RDS for PostgreSQL. Les détails de configuration du point de terminaison seront automatiquement renseignés. 2. Choisissez Fournir les informations d'accès manuellement. Pour Port, assurez-vous de saisir 2484. Pour plus d'informations, consultez la section Utilisation d'une base de données PostgreSQL comme cible pour AWS Database Migration Service.	AWS général

Tâche	Description	Compétences requises
Testez les points de terminaison.	1. Testez les points de terminaison source et cible pour confirmer que les deux sont efficaces et disponibles. 2. Si un test échoue, assurez-vous que les règles entrantes du groupe de sécurité sont valides.	AWS général

Tâche	Description	Compétences requises
Créez des tâches de migration .	Pour créer une tâche de migration pour le chargement complet et la capture des données modifiées (CDC) ou pour la validation des données, procédez comme suit : 1. Pour créer une tâche de migration de base de données, choisissez l'instance de réplication, le point de terminaison de la base de données source et le point de terminaison de la base de données cible. Spécifiez le type de migration comme suit : • Migrer les données existantes (chargement complet) • Répliquer les modifications de données uniquement (CDC) • Migrer les données existantes et répliquer les modifications en cours (chargement complet et CDC) 2. Sous Mappages de tables, vous pouvez configurer les règles de sélection et les règles de transformation au format GUI ou JSON :	AWS général

Tâche	Description	Compétences requises

	• Sous Règles de sélection , sélectionnez le schéma, entrez le nom de la table et sélectionnez l'action (Inclure ou Exclure) à configurer ; par exemple, Schéma ORCL, nom de table %, Action Include.
	• Sous Règles de transformation, effectuez l'une des opérations suivantes :
	  • Sélectionnez le schéma et choisisse z l'action (majuscul e, préfixe, suffixe) ; par exemple, Target Schema ORCL, Action Make en minuscules.
	  • Sélectionnez le schéma, entrez le nom de la table et choisissez l'action (majuscule, préfixe, suffixe) ; par exemple, Target Schema ORCL, Table %, Action Make en minuscules.
	3. Activez la surveillance d'Amazon CloudWatch Logs.
	4. Pour les règles de mappage, ajoutez le code JSON suivant.	

Tâche	Description	Compétences requises

	{
	"rules": [
	{
	"rule-type": "transformation",
	"rule-id": "1",
	"rule-name": "1",
	"rule-target": "table",
	"object-locator": {
	"schema-name": "%",
	"table-name": "%"
	},
	"rule-action": "convert-lowercase",
	"value": null,
	"old-value": null
	},
	{
	"rule-type": "transformation",
	"rule-id": "2",
	"rule-name": "2",
	"rule-target": "schema",
	"object-locator": {	

Tâche	Description	Compétences requises
	"schema-name": "ORCL", "table-name": "%" }, { "rule-action": "convert-lowercase", "value": null, "old-value": null }, { "rule-type": "selection", "rule-id": "3", "rule-name": "3", "object-locator": { "schema-name": "ORCL", "table-name": "DEPT" }, "rule-action": "include", "filters": [] }] }	

Tâche	Description	Compétences requises
Planifiez le cycle de productio n.	Confirmez les interruptions de service auprès des parties prenantes telles que les propriétaires d'applications pour exécuter AWS DMS dans les systèmes de production.	Responsable de la migration

Tâche	Description	Compétences requises
Exécutez la tâche de migration .	1. Démarrez la tâche AWS DMS dont le statut est Ready et surveillez les journaux des tâches de migration sur Amazon CloudWatch pour détecter toute erreur. Si vous avez choisi Migrer les données existantes et répliquer les modifications en cours comme type de migration, et que le statut est Chargement complet de la réplication en cours, le chargement complet avec la migration des données CDC est terminé et la validation est en cours. 2. Après avoir démarré la migration, vous pouvez obtenir des informations supplémentaires sur la connexion SSL dans. CloudWatch Pour Oracle, CloudWatch affiche la chaîne de connexion suivante. `2019-12-17T09:15:1 1 [SOURCE_U NLOAD ]I: Connectin g to Oracle: Beginning session`	AWS général

Tâche	Description	Compétences requises

	`(oracle_endpoint_conn.c:834)`
	
	La chaîne de connexion PostgreSQL sera similaire à l'exemple suivant.
	
	`2019-12-17T09:15:11 [TARGET_LOAD ]I: Going to connect to ODBC connection string: PROTOCOL=7.4-0;DRIVER={PostgreSQL};SERVER=mypgdbinstance.cokmvis0v46q.us-east-1.rds.amazonaws.com;DATABASE=pgdb;PORT=5432;sslmode=require;UID=pguser; (odbc_endpoint_imp.c:2218)`	

Tâche	Description	Compétences requises
Validez les données.	Passez en revue les résultats et les données des tâches de migration dans les bases de données Oracle source et PostgreSQL cible : 1. Connectez-vous à pgAdmin et vérifiez les données de votre base de données PostgreSQL à l'aide du schéma. `ORCL` 2. Pour le CDC, vérifiez les modifications en cours en insérant ou en mettant à jour des données dans la base de données Oracle source.	DBA
Arrêtez la tâche de migration.	Une fois la validation des données terminée avec succès, arrêtez la tâche de migration.	AWS général

Nettoyez les ressources

Tâche	Description	Compétences requises
Supprimez les tâches AWS DMS.	1. Sur la console AWS DMS, accédez à Tâches de migration de base de données et arrêtez toute tâche AWS DMS en cours ou en cours d'exécution.	AWS général

Tâche	Description	Compétences requises
	2. Sélectionnez la ou les tâches, choisissez Actions, puis cliquez sur Supprimer.	
Supprimez les points de terminaison AWS DMS.	Sélectionnez les points de terminaison source et cible que vous avez créés, choisissez Actions, puis choisissez Supprimer.	AWS général
Supprimez l'instance de réplication AWS DMS.	Choisissez l'instance de réplication, sélectionnez Actions, puis sélectionnez Supprimer.	AWS général
Supprimez la base de données PostgreSQL.	1. Sur la console Amazon RDS, sélectionnez Databases. 2. Sélectionnez l'instanc e de base de données PostgreSQL que vous avez créée, choisissez Actions, puis choisissez Supprimer.	AWS général
Supprimez la base de données Oracle.	Sur la console Amazon RDS, sélectionnez l'instance de base de données Oracle, choisissez Actions, puis choisissez Supprimer.	AWS général

Résolution des problèmes

Problème	Solution
Les connexions de test source et cible AWS SCT échouent.	Configurez les versions du pilote JDBC et les règles entrantes du groupe de sécurité VPC pour accepter le trafic entrant.
L'exécution du test du point de terminaison source Oracle échoue.	Vérifiez les paramètres du point de terminaison et vérifiez si l'instance de réplication est disponible.
L'exécution à chargement complet de la tâche AWS DMS échoue.	Vérifiez si les types et les tailles de données des bases de données source et cible correspondent.
La tâche de migration de validation AWS DMS renvoie des erreurs.	1. Vérifiez si la table possède une clé primaire. Les tables sans clé primaire ne sont pas validées. 2. Si la table contient une clé primaire mais renvoie des erreurs, vérifiez l'attribut de connexion supplémentaire dans le point de terminaison source. L'attribut de connexion supplémentaire doit `numberDataTypeScale=-2` prendre en charge le type de `NUMBER` données sans taille de manière dynamique en fonction des données disponibles dans le tableau.

Ressources connexes

Bases de données

- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL

Connexion à la base de données SSL

- Utilisation du protocole SSL/TLS pour chiffrer une connexion à une instance de base de données
  - Utilisation du protocole SSL avec une instance de base de données RDS pour Oracle
  - Sécurisation des connexions à RDS pour PostgreSQL avec SSL/TLS
  - Téléchargez des ensembles de certificats pour des régions AWS spécifiques
    - Télécharger le certificat racine CA-2019 (expiré en août 2024)
- Utilisation de groupes d'options
  - Ajouter des options aux instances de base de données Oracle
  - couche Oracle Secure Sockets
- Utilisation de groupes de paramètres
- Paramètre de connexion SSLmode de PostgreSQL
- Utilisation du protocole SSL à partir de JDBC
- Rotation de votre certificat SSL/TLS
  - Mettre à jour votre certificat CA en modifiant votre instance ou cluster de base de données
  - Mettre à jour votre certificat CA en appliquant la maintenance

AWS SCT

- Outil de conversion de schéma AWS
- Guide de l'utilisateur de l'outil AWS Schema Conversion Tool
- Utilisation de l'interface utilisateur AWS SCT
- Utilisation de la base de données Oracle comme source pour AWS SCT

AWS DMS

- AWS Database Migration Service
- Guide de l'utilisateur d'AWS Database Migration Service
  - Utilisation d'une base de données Oracle comme source pour AWS DMS
  - Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS
- Utilisation du protocole SSL avec AWS Database Migration Service
- Migration d'applications exécutant des bases de données relationnelles vers AWS

Informations supplémentaires

Les certificats de l'autorité de certification Amazon RDS ont `rds-ca-2019` expiré en août 2024. Si vous utilisez ou prévoyez d'utiliser le protocole SSL ou TLS avec vérification des certificats pour vous connecter à vos instances de base de données RDS ou à vos clusters de bases de données multi-AZ, pensez à utiliser l'un des nouveaux certificats CA :`rds-ca-rsa2048-g1`,, `rds-ca-rsa4096-g1` ou. `rds-ca-ecc384-g1`

Migrer les packages pragma Oracle SERIALLY_REUSERABLE vers PostgreSQL

Créée par Vinay Paladi (AWS)

Récapitulatif

Ce modèle fournit une step-by-step approche pour la migration des packages Oracle définis comme le pragma SERIALLY_REUSIBLE vers PostgreSQL sur Amazon Web Services (AWS). Cette approche conserve les fonctionnalités du pragma SERIALLY_REUSERABLE.

PostgreSQL ne supporte pas le concept de packages ni le pragma SERIALLY_REUSIBLE. Pour obtenir des fonctionnalités similaires dans PostgreSQL, vous pouvez créer des schémas pour les packages et déployer tous les objets associés (tels que les fonctions, les procédures et les types) dans les schémas. Pour bénéficier des fonctionnalités du pragma SERIALLY_REUSERABLE, l'exemple de script de fonction wrapper fourni dans ce modèle utilise un pack d'extension AWS Schema Conversion Tool (AWS SCT).

Pour plus d'informations, consultez SERIALLY_REUSERABLE Pragma dans la documentation Oracle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- La dernière version d'AWS SCT et les pilotes requis
- Une base de données Amazon Aurora PostgreSQL Edition compatible ou une base de données Amazon Relational Database Service (Amazon RDS) pour PostgreSQL

Versions du produit

- Oracle Database version 10g et versions ultérieures

Architecture

Pile technologique source

- Base de données Oracle sur site

Pile technologique cible

- Compatible avec Aurora PostgreSQL ou Amazon RDS pour PostgreSQL
- AWS SCT

Architecture de migration

Outils

Services AWS

- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.
- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.

Autres outils

- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

Épopées

Migrer le package Oracle à l'aide d'AWS SCT

Tâche	Description	Compétences requises
Configurez AWS SCT.	Configurez la connectivité AWS SCT à la base de données source. Pour plus d'informations, consultez la section Utilisation de la base de données Oracle comme source pour AWS SCT.	DBA, Développeur

Tâche	Description	Compétences requises
Convertissez le script.	Utilisez AWS SCT pour convertir le package Oracle en sélectionnant la base de données cible compatible avec Aurora PostgreSQL.	DBA, Développeur
Enregistrez les fichiers .sql.	Avant d'enregistrer le fichier .sql, modifiez l'option Paramètres du projet dans AWS SCT sur Fichier unique par étape. AWS SCT séparera le fichier .sql en plusieurs fichiers .sql en fonction du type d'objet.	DBA, Développeur
Changez le code.	Ouvrez la `init` fonction générée par AWS SCT et modifiez-la comme indiqué dans l'exemple de la section Informations supplémen taires. Il ajoutera une variable pour obtenir la fonctionn alité`pg_serialize = 0` .	DBA, Développeur
Testez la conversion.	Déployez la `init` fonction sur la base de données compatibl e Aurora PostgreSQL et testez les résultats.	DBA, Développeur

Ressources connexes

- Outil de conversion de schéma AWS
- Amazon RDS
- Fonctionnalités d'Amazon Aurora

- PRAGMA RÉUTILISABLE EN SÉRIE

Informations supplémentaires

```
Source Oracle Code:

CREATE OR REPLACE PACKAGE test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
PROCEDURE function_1
 (test_id number);
PROCEDURE function_2
 (test_id number
 );
END;

CREATE OR REPLACE PACKAGE BODY test_pkg_var
IS
PRAGMA SERIALLY_REUSABLE;
v_char VARCHAR2(20) := 'shared.airline';
v_num number := 123;

PROCEDURE function_1(test_id number)
IS
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
v_char:='test1';
function_2(0);
END;

PROCEDURE function_2(test_id number)
is
begin
dbms_output.put_line( 'v_char-'|| v_char);
dbms_output.put_line( 'v_num-'||v_num);
END;
END test_pkg_var;

Calling the above functions

set serveroutput on
```

```
EXEC test_pkg_var.function_1(1);


EXEC test_pkg_var.function_2(1);


Target Postgresql Code:


CREATE SCHEMA test_pkg_var;

CREATE OR REPLACE FUNCTION test_pkg_var.init(pg_serialize IN INTEGER DEFAULT 0)

RETURNS void
AS
$BODY$

DECLARE

BEGIN

if aws_oracle_ext.is_package_initialized( 'test_pkg_var' ) AND pg_serialize = 0

then

return;

end if;

PERFORM aws_oracle_ext.set_package_initialized( 'test_pkg_var' );

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'shared.airline.basecurrency'::CHARACTER

VARYING(100));

PERFORM aws_oracle_ext.set_package_variable('test_pkg_var', 'v_num', 123::integer);

END;

$BODY$

LANGUAGE plpgsql;
```

```
CREATE OR REPLACE FUNCTION test_pkg_var.function_1(pg_serialize int default 1)

RETURNS void
AS

$BODY$
DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');

raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

PERFORM aws_oracle_ext.set_package_variable( 'test_pkg_var', 'v_char',
 'test1'::varchar);

PERFORM test_pkg_var.function_2(0);
END;

$BODY$
LANGUAGE plpgsql;


CREATE OR REPLACE FUNCTION test_pkg_var.function_2(IN pg_serialize integer default 1)

RETURNS void

AS

$BODY$

DECLARE

BEGIN

PERFORM test_pkg_var.init(pg_serialize);

raise notice 'v_char%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_char');
```

```
raise notice 'v_num%',aws_oracle_ext.get_package_variable( 'test_pkg_var', 'v_num');

END;
$BODY$
LANGUAGE plpgsql;


Calling the above functions

select test_pkg_var.function_1()

 select test_pkg_var.function_2()
```

Migrer des tables externes Oracle vers des tables compatibles avec Amazon Aurora PostgreSQL

Créée par anuradha chintha (AWS) et Rakesh Raghav (AWS)

Récapitulatif

Les tables externes permettent à Oracle d'interroger des données stockées en dehors de la base de données dans des fichiers plats. Vous pouvez utiliser le pilote ORACLE_LOADER pour accéder à toutes les données stockées dans n'importe quel format pouvant être chargées par l'utilitaire SQL*Loader. Vous ne pouvez pas utiliser le langage de manipulation de données (DML) sur des tables externes, mais vous pouvez utiliser des tables externes pour les opérations de requête, de jointure et de tri.

L'édition compatible avec Amazon Aurora PostgreSQL ne fournit pas de fonctionnalités similaires à celles des tables externes d'Oracle. Vous devez plutôt recourir à la modernisation pour développer une solution évolutive qui répond aux exigences fonctionnelles et qui soit économe.

Ce modèle décrit les étapes à suivre pour migrer différents types de tables externes Oracle vers l'édition compatible Aurora PostgreSQL sur le cloud Amazon Web Services (AWS) à l'aide de l'extension. `aws_s3`

Nous vous recommandons de tester minutieusement cette solution avant de l'implémenter dans un environnement de production.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Interface de ligne de commande AWS (AWS CLI)
- Une instance de base de données compatible Aurora PostgreSQL disponible.
- Une base de données Oracle sur site avec une table externe
- API PG.Client
- Fichiers de données

Limites

- Ce modèle ne fournit pas les fonctionnalités nécessaires pour remplacer les tables externes Oracle. Toutefois, les étapes et les exemples de code peuvent être encore améliorés pour atteindre les objectifs de modernisation de votre base de données.
- Les fichiers ne doivent pas contenir le caractère utilisé comme délimiteur dans les fonctions `aws_s3` d'exportation et d'importation.

Versions du produit

- Pour effectuer une importation depuis Amazon S3 vers RDS pour PostgreSQL, la base de données doit exécuter PostgreSQL version 10.7 ou ultérieure.

Architecture

Pile technologique source

- Oracle

Architecture source

Pile technologique cible

- Compatible avec Amazon Aurora PostgreSQL
- Amazon CloudWatch
- AWS Lambda
- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)

Architecture cible

Le schéma suivant montre une représentation de haut niveau de la solution.

1. Les fichiers sont chargés dans le compartiment S3.
2. La fonction Lambda est lancée.

3. La fonction Lambda lance l'appel de fonction de base de données.
4. Secrets Manager fournit les informations d'identification pour accéder à la base de données.
5. En fonction de la fonction de base de données, une alarme SNS est créée.

Automatisation et mise à l'échelle

Tout ajout ou modification aux tables externes peut être géré grâce à la maintenance des métadonnées.

Outils

- Compatible avec Amazon Aurora PostgreSQL — Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré, compatible avec PostgreSQL et conforme à l'ACID qui associe la vitesse et la fiabilité des bases de données commerciales haut de gamme à la rentabilité des bases de données open source.
- AWS CLI — AWS Command Line Interface (AWS CLI) est un outil unifié permettant de gérer vos services AWS. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs services AWS depuis la ligne de commande et les automatiser par le biais de scripts.
- Amazon CloudWatch — Amazon CloudWatch surveille les ressources et l'utilisation d'Amazon S3.
- AWS Lambda — AWS Lambda est un service de calcul sans serveur qui permet d'exécuter du code sans provisionner ni gérer de serveurs, de créer une logique de dimensionnement des clusters adaptée à la charge de travail, de gérer les intégrations d'événements ou de gérer les temps d'exécution. Dans ce modèle, Lambda exécute la fonction de base de données chaque fois qu'un fichier est chargé sur Amazon S3.
- AWS Secrets Manager — AWS Secrets Manager est un service de stockage et de récupération des informations d'identification. À l'aide de Secrets Manager, vous pouvez remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) fournit une couche de stockage permettant de recevoir et de stocker des fichiers destinés à être consommés et transmis vers et depuis le cluster compatible Aurora PostgreSQL.
- aws_s3 — L'`aws_s3`extension intègre la compatibilité avec Amazon S3 et Aurora PostgreSQL.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients. Dans ce modèle, Amazon SNS est utilisé pour envoyer des notifications.

Code

Chaque fois qu'un fichier est placé dans le compartiment S3, une fonction de base de données doit être créée et appelée depuis l'application de traitement ou la fonction Lambda. Pour plus de détails, consultez le code (ci-joint).

Épopées

Création d'un fichier externe

Tâche	Description	Compétences requises
Ajoutez un fichier externe à la base de données source.	Créez un fichier externe et déplacez-le vers le `oracle` répertoire.	DBA

Configuration de la cible (compatible avec Aurora PostgreSQL)

Tâche	Description	Compétences requises
Créez une base de données Aurora PostgreSQL.	Créez une instance de base de données dans votre cluster compatible Amazon Aurora PostgreSQL.	DBA
Créez un schéma, une extension aws_s3 et des tables.	Utilisez le code ci-dessou s `ext_tbl_scripts` dans la section Informati ons supplémentaires. Les tables incluent des tables réelles, des tables intermédi aires, des tables d'erreurs et de journaux, ainsi qu'une métatable.	DBA, Développeur
Créez la fonction de base de données.	Pour créer la fonction de base de données, utilisez le code sous `load_exte`	DBA, Développeur

Tâche	Description	Compétences requises
	`rnal_table_latest` fonction dans la section Informations supplémentaires.	

Création et configuration de la fonction Lambda

Tâche	Description	Compétences requises
Créez un rôle.	Créez un rôle avec des autorisations pour accéder à Amazon S3 et Amazon Relational Database Service (Amazon RDS). Ce rôle sera attribué à Lambda pour exécuter le modèle.	DBA
Créez la fonction Lambda.	Créez une fonction Lambda qui lit le nom du fichier depuis Amazon S3 (par exemple`file_key = info.get('object', {}).get('key') )` et appelle la fonction de base de données (par exemple,`curs.call proc("load_externa l_tables", [file_key ]) )` avec le nom du fichier comme paramètre d'entrée. En fonction du résultat de l'appel de fonction, une notification SNS sera lancée (par exemple,`client.pu blish(TopicArn='ar`	DBA

Tâche	Description	Compétences requises
	`n:',Message='filel oadsuccess',Subjec t='fileloadsuccess ') )`. En fonction des besoins de votre entreprise, vous pouvez créer une fonction Lambda avec du code supplémen taire si nécessaire. Pour plus d'informations, consultez la documentation Lambda.	
Configurez un déclencheur d'événement du compartiment S3.	Configurez un mécanisme pour appeler la fonction Lambda pour tous les événements de création d'objets dans le compartiment S3.	DBA
Créez un secret.	Créez un nom secret pour les informations d'identification de la base de données à l'aide de Secrets Manager. Transmett ez le secret dans la fonction Lambda.	DBA
Téléchargez les fichiers de support Lambda.	Téléchargez un fichier .zip contenant les packages de support Lambda et le script Python joint pour vous connecter à Aurora PostgreSQ L compatible. Le code Python appelle la fonction que vous avez créée dans la base de données.	DBA

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Créez une rubrique SNS pour envoyer un e-mail en cas de réussite ou d'échec du chargement des données.	DBA

Ajouter une intégration avec Amazon S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	Sur la console Amazon S3, créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS.	DBA
Créez des politiques IAM.	Pour créer les politiques AWS Identity and Access Management (IAM), utilisez le code ci-dessous `s3bucketpolicy_for_import` dans la section Informations supplémentaires.	DBA
Créez des rôles.	Créez deux rôles pour la compatibilité avec Aurora PostgreSQL, un rôle pour l'importation et un rôle pour l'exportation. Assignez les politiques correspondantes aux rôles.	DBA

Tâche	Description	Compétences requises
Associez les rôles au cluster compatible avec Aurora PostgreSQL.	Sous Gérer les rôles, attachez les rôles d'importation et d'exportation au cluster Aurora PostgreSQL.	DBA
Créez des objets de support compatibles avec Aurora PostgreSQL.	Pour les scripts de table, utilisez le code ci-dessous `ext_tbl_scripts` dans la section Informations supplémentaires. Pour la fonction personnalisée, utilisez le code ci-dessous `load_external_Table_latest` dans la section Informations supplémentaires.	DBA

Traiter un fichier de test

Tâche	Description	Compétences requises
Téléchargez un fichier dans le compartiment S3.	Pour télécharger un fichier de test dans le compartiment S3, utilisez la console ou la commande suivante dans l'AWS CLI. `aws s3 cp /Users/Desktop/ukpost/exttbl/"testing files"/aps s3://s3importtest/inputext/aps` Dès que le fichier est chargé, un événement de bucket	DBA

Tâche	Description	Compétences requises
	lance la fonction Lambda, qui exécute la fonction compatible avec Aurora PostgreSQL.	
Vérifiez les données, le journal et les fichiers d'erreurs.	La fonction compatible avec Aurora PostgreSQL charge les fichiers dans la table principal e `.log` et crée des `.bad` fichiers dans le compartiment S3.	DBA
Surveillez la solution.	Dans la CloudWatch console Amazon, surveillez la fonction Lambda.	DBA

Ressources connexes

- Intégration avec Amazon S3
- Amazon S3
- Utilisation de l'édition compatible avec Amazon Aurora PostgreSQL
- AWS Lambda
- Amazon CloudWatch
- AWS Secrets Manager
- Configuration des notifications Amazon SNS

Informations supplémentaires

ext_table_scripts

```
CREATE EXTENSION aws_s3 CASCADE;
CREATE TABLE IF NOT EXISTS meta_EXTERNAL_TABLE
(
    table_name_stg character varying(100) ,
    table_name character varying(100)  ,
    col_list character varying(1000)  ,
```

```
    data_type character varying(100)  ,
    col_order numeric,
    start_pos numeric,
    end_pos numeric,
    no_position character varying(100)  ,
    date_mask character varying(100)  ,
    delimeter character(1)  ,
    directory character varying(100)  ,
    file_name character varying(100)  ,
    header_exist character varying(5)
);
CREATE TABLE IF NOT EXISTS ext_tbl_stg
(
    col1 text
);
CREATE TABLE IF NOT EXISTS error_table
(
    error_details text,
    file_name character varying(100),
    processed_time timestamp without time zone
);
CREATE TABLE IF NOT EXISTS log_table
(
    file_name character varying(50) COLLATE pg_catalog."default",
    processed_date timestamp without time zone,
    tot_rec_count numeric,
    proc_rec_count numeric,
    error_rec_count numeric
);
sample insert scripts of meta data:
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'source_filename', 'character varying', 2, 8, 27, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'record_type_identifier', 'character varying', 3, 28, 30, NULL, NULL, NULL,
 'databasedev', 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
```

```
 'fad_code', 'numeric', 4, 31, 36, NULL, NULL, NULL, 'databasedev', 'externalinterface/
loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'session_sequence_number', 'numeric', 5, 37, 42, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
INSERT INTO meta_EXTERNAL_TABLE (table_name_stg, table_name, col_list, data_type,
 col_order, start_pos, end_pos, no_position, date_mask, delimeter, directory,
 file_name, header_exist) VALUES ('F_EX_APS_TRANSACTIONS_STG', 'F_EX_APS_TRANSACTIONS',
 'transaction_sequence_number', 'numeric', 6, 43, 48, NULL, NULL, NULL, 'databasedev',
 'externalinterface/loaddir/APS', 'NO');
```

s3bucketpolicy_for import

```
---Import role policy
--Create an IAM policy to allow, Get,  and list actions on S3 bucket
 {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3import",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest",
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
--Export Role policy
--Create an IAM policy to allow, put,  and list actions on S3 bucket
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "s3export",
            "Action": [
                "S3:PutObject",
```

```
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::s3importtest/*"
            ]
        }
    ]
}
```

Exemple de fonction de base de données load_external_tables_latest

```
CREATE OR REPLACE FUNCTION public.load_external_tables(pi_filename text)
 RETURNS character varying
 LANGUAGE plpgsql
AS $function$
/* Loading data from S3 bucket into a APG table */
DECLARE
 v_final_sql TEXT;
 pi_ext_table TEXT;
 r refCURSOR;
 v_sqlerrm text;
 v_chunk numeric;
 i integer;
 v_col_list TEXT;
 v_postion_list CHARACTER VARYING(1000);
 v_len  integer;
 v_delim varchar;
 v_file_name CHARACTER VARYING(1000);
 v_directory CHARACTER VARYING(1000);
 v_table_name_stg CHARACTER VARYING(1000);
 v_sql_col TEXT;
 v_sql TEXT;
 v_sql1 TEXT;
 v_sql2 TEXT;
 v_sql3 TEXT;
 v_cnt integer;
 v_sql_dynamic TEXT;
 v_sql_ins TEXT;
 proc_rec_COUNT integer;
 error_rec_COUNT integer;
 tot_rec_COUNT integer;
 v_rec_val integer;
```

```
 rec record;
 v_col_cnt integer;
 kv record;
 v_val text;
 v_header text;
 j integer;
 ERCODE VARCHAR(5);
 v_region text;
 cr CURSOR FOR
 SELECT distinct DELIMETER,
   FILE_NAME,
   DIRECTORY
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
   AND DELIMETER IS NOT NULL;


 cr1 CURSOR FOR
   SELECT   col_list,
   data_type,
   start_pos,
   END_pos,
   concat_ws('',' ',TABLE_NAME_STG) as TABLE_NAME_STG,
   no_position,date_mask
 FROM  meta_EXTERNAL_TABLE
 WHERE table_name = pi_ext_table
 order by col_order asc;
cr2 cursor FOR
SELECT  distinct table_name,table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);


BEGIN
 -- PERFORM utl_file_utility.init();
   v_region := 'us-east-1';
   /* find tab details from file name */


   --DELETE FROM  ERROR_TABLE WHERE file_name= pi_filename;
  -- DELETE FROM  log_table WHERE file_name= pi_filename;


 BEGIN
```

```
   SELECT distinct table_name,table_name_stg INTO strict pi_ext_table,v_table_name_stg
   FROM  meta_EXTERNAL_TABLE
   WHERE upper(file_name) = upper(pi_filename);
 EXCEPTION
   WHEN NO_DATA_FOUND THEN
    raise notice 'error 1,%',sqlerrm;
    pi_ext_table := null;
    v_table_name_stg := null;
      RAISE USING errcode = 'NTFIP' ;
    when others then
        raise notice 'error others,%',sqlerrm;
 END;
 j :=1 ;

for rec in  cr2
 LOOP




  pi_ext_table     := rec.table_name;
  v_table_name_stg := rec.table_name_stg;
  v_col_list := null;


 IF pi_ext_table IS NOT NULL
  THEN
    --EXECUTE concat_ws('','truncate table  ' ,pi_ext_table) ;
   EXECUTE concat_ws('','truncate table  ' ,v_table_name_stg) ;




       SELECT distinct DELIMETER INTO STRICT v_delim
       FROM  meta_EXTERNAL_TABLE
       WHERE table_name = pi_ext_table;


       IF v_delim IS NOT NULL THEN
     SELECT distinct DELIMETER,
       FILE_NAME,
       DIRECTORY ,
```

```
      concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
    INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table
      AND DELIMETER IS NOT NULL;


    IF    upper(v_delim) = 'CSV'
    THEN
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3 ( ''',
      v_table_name_stg,''','''',
      ''DELIMITER '''','''' CSV HEADER QUOTE '''''''''', aws_commons.create_s3_uri
( ''',
      v_directory,''','''',v_file_name,''', ''',v_region,'''))');
      ELSE
      v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
          v_table_name_stg, ''','''', ''DELIMITER AS ''''^''''',''',','
         aws_commons.create_s3_uri
          ( ''',v_directory, ''','''',
          v_file_name, ''',',
           '''',v_region,''')
         )');
         raise notice 'v_sql , %',v_sql;
      begin
       EXECUTE  v_sql;
      EXCEPTION
        WHEN OTHERS THEN
          raise notice 'error 1';
        RAISE USING errcode = 'S3IMP' ;
      END;


      select count(col_list) INTO v_col_cnt
      from  meta_EXTERNAL_TABLE where table_name = pi_ext_table;









       -- raise notice 'v_sql 2, %',concat_ws('','update ',v_table_name_stg, ' set
col1 = col1||''',v_delim,''''');
```

```
      execute concat_ws('','update ',v_table_name_stg, ' set col1 =
col1||''',v_delim,''''); 




      i :=1;
      FOR rec in cr1
      loop
      v_sql1 := concat_ws('',v_sql1,'split_part(col1,''',v_delim,''',', i,')',' as
',rec.col_list,',');
      v_sql2 := concat_ws('',v_sql2,rec.col_list,',');
  --    v_sql3 := concat_ws('',v_sql3,'rec.',rec.col_list,'::',rec.data_type,',');


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                coalesce((trim(split_part(col1,''',v_delim,''',',
i,')))::NUMERIC,0)::',rec.data_type,' END as ',rec.col_list,',') ;
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''99990101''),''YYYYMMDD'')::',rec.data_type,' END as ',rec.col_list,',');
        WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
 'MM/DD/YYYY hh24:mi:ss'
        THEN v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
               THEN null
                ELSE
                to_date(coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''01/01/9999 0024:00:00''),''MM/DD/YYYY hh24:mi:ss'')::',rec.data_type,' END as
',rec.col_list,',');
         ELSE
       v_sql3 := concat_ws('',v_sql3,' case WHEN
length(trim(split_part(col1,''',v_delim,''',', i,'))) =0
```

```
                THEN null
                 ELSE
                  coalesce((trim(split_part(col1,''',v_delim,''',',
i,'))),''''):',rec.data_type,' END as ',rec.col_list,',') ;
      END case;


      i :=i+1;
      end loop;


        -- raise notice 'v_sql 3, %',v_sql3;


      SELECT trim(trailing ' ' FROM v_sql1) INTO v_sql1;
      SELECT trim(trailing ',' FROM v_sql1) INTO v_sql1;


      SELECT trim(trailing ' ' FROM v_sql2) INTO v_sql2;
      SELECT trim(trailing ',' FROM v_sql2) INTO v_sql2;


      SELECT trim(trailing ' ' FROM v_sql3) INTO v_sql3;
      SELECT trim(trailing ',' FROM v_sql3) INTO v_sql3;


      END IF;
     raise notice 'v_delim , %',v_delim;


    EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)  INTO v_cnt;


   raise notice 'stg cnt , %',v_cnt;


   /* if upper(v_delim) = 'CSV' then
      v_sql_ins := concat_ws('', ' SELECT * from ' ,v_table_name_stg );
    else
     -- v_sql_ins := concat_ws('',' SELECT ',v_sql1,'  from (select col1 from
' ,v_table_name_stg , ')sub ');
      v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
' ,v_table_name_stg , ')sub ');
      END IF;*/
```

```
v_chunk := v_cnt/100;




for i in 1..101
loop
     BEGIN
    -- raise notice 'v_sql , %',v_sql;
       -- raise notice 'Chunk number , %',i;
       v_sql_ins := concat_ws('',' SELECT ',v_sql3,'  from (select col1 from
 ' ,v_table_name_stg , ' offset ',v_chunk*(i-1), ' limit ',v_chunk,') sub ');


     v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
     -- raise notice 'select statement , %',v_sql_ins;
          -- v_sql := null;
     -- EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins, 'offset
 ',v_chunk*(i-1), ' limit ',v_chunk );
     --v_sql := concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins );


     -- raise notice 'insert statement , %',v_sql;


    raise NOTICE 'CHUNK START %',v_chunk*(i-1);
   raise NOTICE 'CHUNK END %',v_chunk;


     EXECUTE v_sql;


  EXCEPTION
       WHEN OTHERS THEN
       -- v_sql_ins := concat_ws('',' SELECT ',v_sql1, '  from (select col1 from
 ' ,v_table_name_stg , ' )sub ');
         -- raise notice 'Chunk number for cursor , %',i;


    raise NOTICE 'Cursor - CHUNK START %',v_chunk*(i-1);
   raise NOTICE 'Cursor -  CHUNK END %',v_chunk;
```

```
        v_sql_ins := concat_ws('',' SELECT ',v_sql3, '  from (select col1 from
 ' ,v_table_name_stg , ' )sub ');


        v_final_sql := REPLACE (v_sql_ins, ''''::text, ''''''::text);
       -- raise notice 'v_final_sql %',v_final_sql;
        v_sql :=concat_ws('','do $a$ declare  r refcursor;v_sql text; i
 numeric;v_conname text;  v_typ  ',pi_ext_table,'[]; v_rec  ','record',';
          begin









          open r for execute ''select col1 from ',v_table_name_stg ,'  offset
 ',v_chunk*(i-1), ' limit ',v_chunk,''';
          loop
          begin
          fetch r into v_rec;
          EXIT WHEN NOT FOUND;




          v_sql := concat_ws('''','insert into  ',pi_ext_table,' SELECT ',REPLACE
 (v_sql3, ''''::text, ''''''::text) , '  from ( select ''''''',v_rec.col1,''''''' as
 col1) v'');
           execute v_sql;


          exception
           when others then
         v_sql := ''INSERT INTO  ERROR_TABLE VALUES (concat_ws(''''''''','''Error
 Name: ''',$$''||SQLERRM||''$$,'''Error State: ''',''''''||
SQLSTATE||'''''',''''record : ''',$$''||v_rec.col1||''$$),'''''||
pi_filename||'''''',now())'';


             execute v_sql;
            continue;
          end ;
          end loop;
          close r;
```

```
          exception
          when others then
        raise;
          end ; $a$');
     -- raise notice ' inside excp v_sql %',v_sql;
         execute v_sql;
     --  raise notice 'v_sql %',v_sql;
      END;
 END LOOP;
    ELSE


    SELECT distinct DELIMETER,FILE_NAME,DIRECTORY ,concat_ws('',' ',table_name_stg),
      case  header_exist when 'YES' then 'CSV HEADER' else 'CSV' end as header_exist
      INTO STRICT v_delim,v_file_name,v_directory,v_table_name_stg,v_header
    FROM  meta_EXTERNAL_TABLE
    WHERE table_name = pi_ext_table                  ;
    v_sql := concat_ws('','SELECT aws_s3.table_import_FROM_s3(''',
      v_table_name_stg, ''','''', ''DELIMITER AS ''''#'''' ',v_header,' '','','
     aws_commons.create_s3_uri
      ( ''',v_directory, ''','''',
      v_file_name, ''',',
       '''',v_region,''')
     )');
        EXECUTE  v_sql;


    FOR rec in cr1
    LOOP


     IF rec.start_pos IS NULL AND rec.END_pos IS NULL AND rec.no_position = 'recnum'
     THEN
       v_rec_val := 1;
     ELSE


      case
        WHEN upper(rec.data_type) = 'NUMERIC'
        THEN v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
               THEN null
                ELSE
```

```
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1')))::NUMERIC,0)::',rec.data_type,' END as
',rec.col_list,',') ;
       WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDD'
       THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
              THEN null
               ELSE
               to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1'))),''99990101''),''YYYYMMDD''):::',rec.data_type,'
END as ',rec.col_list,',');
       WHEN UPPER(rec.data_type) = 'TIMESTAMP WITHOUT TIME ZONE' AND rec.date_mask =
'YYYYMMDDHH24MISS'
       THEN v_sql1 := concat_ws('','case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1))) =0
              THEN null
               ELSE
               to_date(coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1'))),''9999010100240000''),''YYYYMMDDHH24MISS''):::',rec.data_
END as ',rec.col_list,',');
        ELSE
      v_sql1 := concat_ws('',' case WHEN length(trim(substring(COL1,
',rec.start_pos ,',', rec.END_pos,'-',rec.start_pos ,'+1'))) =0
              THEN null
               ELSE
                coalesce((trim(substring(COL1, ',rec.start_pos ,',',
rec.END_pos,'-',rec.start_pos ,'+1'))),''''):::',rec.data_type,' END as
',rec.col_list,',') ;
     END case;


    END IF;
    v_col_list := concat_ws('',v_col_list ,v_sql1);
   END LOOP;




         SELECT trim(trailing ' ' FROM v_col_list) INTO v_col_list;
         SELECT trim(trailing ',' FROM v_col_list) INTO v_col_list;
```

```
          v_sql_col   :=  concat_ws('',trim(trailing ',' FROM v_col_list) , ' FROM
 ',v_table_name_stg,' WHERE col1 IS NOT NULL AND length(col1)>0 ');




          v_sql_dynamic := v_sql_col;


          EXECUTE  concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg) INTO v_cnt;




        IF v_rec_val = 1 THEN
            v_sql_ins := concat_ws('',' select row_number() over(order by ctid) as
line_number ,' ,v_sql_dynamic) ;


        ELSE
              v_sql_ins := concat_ws('',' SELECT' ,v_sql_dynamic) ;
          END IF;


    BEGIN
      EXECUTE concat_ws('','insert into  ', pi_ext_table ,' ', v_sql_ins);
          EXCEPTION
             WHEN OTHERS THEN
         IF v_rec_val = 1 THEN
                v_final_sql := ' select row_number() over(order by ctid) as
line_number ,col1 from ';
               ELSE
                v_final_sql := ' SELECT col1 from';
              END IF;
      v_sql :=concat_ws('','do $a$ declare  r refcursor;v_rec_val numeric :=
',coalesce(v_rec_val,0),';line_number numeric; col1 text; v_typ  ',pi_ext_table,'[];
v_rec  ',pi_ext_table,';
            begin
            open r for execute ''',v_final_sql, ' ',v_table_name_stg,' WHERE col1 IS
NOT NULL AND length(col1)>0 '' ;
            loop
            begin
            if   v_rec_val = 1 then
            fetch r into line_number,col1;
```

```
            else
            fetch r into col1;
            end if;


            EXIT WHEN NOT FOUND;
             if v_rec_val = 1 then
             select line_number,',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             else
               select ',trim(trailing ',' FROM v_col_list) ,' into v_rec;
             end if;


            insert into  ',pi_ext_table,' select v_rec.*;
             exception
             when others then
              INSERT INTO  ERROR_TABLE VALUES (concat_ws('''','Error Name:
'',SQLERRM,''Error State: '',SQLSTATE,''record : '',v_rec),''',pi_filename,''',now());
              continue;
             end ;
              end loop;
            close r;
             exception
             when others then
             raise;
             end ; $a$');
        execute v_sql;


    END;


        END IF;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  ' ,pi_ext_table)   INTO proc_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM  error_table WHERE file_name
=''',pi_filename,''' and processed_time::date = clock_timestamp()::date')  INTO
error_rec_COUNT;


  EXECUTE concat_ws('','SELECT COUNT(*) FROM ',v_table_name_stg)   INTO tot_rec_COUNT;
```

```
   INSERT INTO  log_table values(pi_filename,now(),tot_rec_COUNT,proc_rec_COUNT,
 error_rec_COUNT);


   raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT
 replace(trim(substring(error_details,position(''('' in
 error_details)+1),'')''),'','','';''),file_name,processed_time FROM  error_table WHERE
 file_name = '''||pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );


raise notice 'v_directory, %',v_directory;


   raise notice 'pi_filename, %',pi_filename;


   raise notice 'v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  log_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.log', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );




   END IF;
 j := j+1;
```

```
 END LOOP;


       RETURN 'OK';
EXCEPTION
    WHEN  OTHERS THEN
  raise notice 'error %',sqlerrm;
   ERCODE=SQLSTATE;
   IF ERCODE = 'NTFIP' THEN
     v_sqlerrm := concat_Ws('',sqlerrm,'No data for the filename');
   ELSIF ERCODE = 'S3IMP' THEN
    v_sqlerrm := concat_Ws('',sqlerrm,'Error While exporting the file from S3');
   ELSE
      v_sqlerrm := sqlerrm;
   END IF;


 select distinct directory into v_directory from  meta_EXTERNAL_TABLE;




 raise notice 'exc v_directory, %',v_directory;


   raise notice 'exc pi_filename, %',pi_filename;


   raise notice 'exc v_region, %',v_region;


  perform aws_s3.query_export_to_s3('SELECT * FROM  error_table WHERE file_name = '''||
pi_filename||'''',
   aws_commons.create_s3_uri(v_directory, pi_filename||'.bad', v_region),
   options :='FORmat csv, header, delimiter $$,$$'
   );
    RETURN null;
END;
$function$
```

Migrer les index basés sur les fonctions d'Oracle vers PostgreSQL

Créée par Veeranjaneyulu Grandhi (AWS) et Navakanth Talluri (AWS)

Récapitulatif

Les index constituent un moyen courant d'améliorer les performances des bases de données. Un index permet au serveur de base de données de rechercher et de récupérer des lignes spécifiques bien plus rapidement qu'il ne le pourrait sans index. Mais les index alourdissent également le système de base de données dans son ensemble, ils doivent donc être utilisés judicieusement. Les index basés sur une fonction, qui sont basés sur une fonction ou une expression, peuvent comporter plusieurs colonnes et expressions mathématiques. Un index basé sur une fonction améliore les performances des requêtes qui utilisent l'expression d'index.

En mode natif, PostgreSQL ne prend pas en charge la création d'index basés sur des fonctions à l'aide de fonctions dont la volatilité est définie comme stable. Cependant, vous pouvez créer des fonctions de volatilité similaires `IMMUTABLE` et les utiliser dans la création d'index.

Une `IMMUTABLE` fonction ne peut pas modifier la base de données et il est garanti qu'elle renverra toujours les mêmes résultats avec les mêmes arguments. Cette catégorie permet à l'optimiseur de préévaluer la fonction lorsqu'une requête l'appelle avec des arguments constants.

Ce modèle facilite la migration des index basés sur les fonctions Oracle lorsqu'ils sont utilisés avec des fonctions telles que `to_charto_date`, et vers `to_number` l'équivalent de PostgreSQL.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif
- Une instance de base de données Oracle source avec le service d'écoute configuré et en cours d'exécution
- Connaissance des bases de données PostgreSQL

Limites

- La limite de taille de la base de données est de 64 To.
- Les fonctions utilisées dans la création d'index doivent être IMMUABLES.

Versions du produit

- Toutes les éditions de base de données Oracle pour les versions 11g (versions 11.2.0.3.v1 et ultérieures), 12.2 et 18c
- PostgreSQL 9.6 et versions ultérieures

Architecture

Pile technologique source

- Une base de données Oracle sur site ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2), ou une instance de base de données Amazon RDS for Oracle

Pile technologique cible

- N'importe quel moteur PostgreSQL

Outils

- pgAdmin 4 est un outil de gestion open source pour Postgres. L'outil pgAdmin 4 fournit une interface graphique pour créer, gérer et utiliser des objets de base de données.
- Oracle SQL Developer est un environnement de développement intégré (IDE) permettant de développer et de gérer Oracle Database dans le cadre de déploiements traditionnels et dans le cloud.

Épopées

Création d'un index basé sur une fonction à l'aide d'une fonction par défaut

Tâche	Description	Compétences requises
Créez un index basé sur une fonction sur une colonne à l'aide de la fonction to_char.	Utilisez le code suivant pour créer l'index basé sur les fonctions. `postgres=# create table funcindex( col1`	DBA, développeur d'applications

Tâche	Description	Compétences requises

	timestamp without time zone);
	CREATE TABLE
	postgres=# insert into funcindex values (now());
	INSERT 0 1
	postgres=# select * from funcindex;
	col1
	---------- 	
	2022-08-09 16:00:57.77414
	(1 rows)
	
	postgres=# create index funcindex_idx on funcindex(to_char(col1,'DD-MM-YYYY HH24:MI:SS'));
	ERROR: functions in index expression must be marked IMMUTABLE
	
	Note
	PostgreSQL n'autorise pas la création d'un index basé sur une fonction sans cette clause. `IMMUTABLE`	

Tâche	Description	Compétences requises
Vérifiez la volatilité de la fonction.	Pour vérifier la volatilité de la fonction, utilisez le code de la section Informations supplémentaires.	DBA

Créez des index basés sur les fonctions à l'aide d'une fonction wrapper

Tâche	Description	Compétences requises
Créez une fonction wrapper.	Pour créer une fonction wrapper, utilisez le code de la section Informations supplémentaires.	Développeur PostgreSQL
Créez un index à l'aide de la fonction wrapper.	Utilisez le code de la section Informations supplémentaires pour créer une fonction définie par l'utilisateur avec le mot-clé `IMMUTABLE` dans le même schéma que l'application, et faites-y référence dans le script de création d'index. Si une fonction définie par l'utilisateur est créée dans un schéma commun (dans l'exemple précédent), mettez-la à jour `search_path` comme indiqué. `ALTER ROLE <ROLENAME> set search_path=$user, COMMON;`	DBA, développeur PostgreSQL

Valider la création d'index

Tâche	Description	Compétences requises
Validez la création de l'index.	Vérifiez que l'index doit être créé, en fonction des modèles d'accès aux requêtes.	DBA
Vérifiez que l'index peut être utilisé.	Pour vérifier si l'index basé sur les fonctions est détecté par PostgreSQL Optimizer, exécutez une instruction SQL en utilisant explain ou explain analyze. Utilisez le code dans la section Informations supplémentaires. Si possible, rassemblez également les statistiques du tableau. **Note** Si vous remarquez le plan d'explication, cela signifie que l'optimis eur PostgreSQL a choisi un index basé sur les fonctions en raison de la condition du prédicat.	DBA

Ressources connexes

- Index basés sur les fonctions (documentation Oracle)
- Index des expressions (documentation PostgreSQL)
- Volatilité de PostgreSQL (documentation PostgreSQL)
- chemin de recherche PostgreSQL (documentation de PostgreSQL)

- Manuel de migration d'Oracle Database 19c vers Amazon Aurora PostgreSQL

Informations supplémentaires

Création d'une fonction wrapper

```
CREATE OR REPLACE FUNCTION myschema.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
```

Créez un index à l'aide de la fonction wrapper

```
postgres=# create function common.to_char(var1 timestamp without time zone, var2
 varchar) RETURNS varchar AS $BODY$ select to_char(var1, 'YYYYMMDD'); $BODY$ LANGUAGE
 sql IMMUTABLE;
CREATE FUNCTION
postgres=# create index funcindex_idx on funcindex(common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS'));
CREATE INDEX
```

Vérifiez la volatilité de la fonction

```
SELECT DISTINCT p.proname as "Name",p.provolatile as "volatility" FROM
 pg_catalog.pg_proc p
 LEFT JOIN pg_catalog.pg_namespace n ON n.oid = p.pronamespace
 LEFT JOIN pg_catalog.pg_language l ON l.oid = p.prolang
 WHERE n.nspname OPERATOR(pg_catalog.~) '^(pg_catalog)$' COLLATE pg_catalog.default AND
 p.proname='to_char'GROUP BY p.proname,p.provolatile
ORDER BY 1;
```

Validez que l'index peut être utilisé

```
explain analyze <SQL>


postgres=# explain select col1 from funcindex where common.to_char(col1,'DD-MM-YYYY
 HH24:MI:SS') = '09-08-2022 16:00:57';
                                                    QUERY PLAN
-------------------------------------------------------------------------------------------
 Index Scan using funcindex_idx on funcindex  (cost=0.42..8.44 rows=1 width=8)
```

```
   Index Cond: ((common.to_char(col1, 'DD-MM-YYYY HH24:MI:SS'::character
 varying))::text = '09-08-2022 16:00:57'::text)
(2 rows)
```

Migrer les fonctions natives d'Oracle vers PostgreSQL à l'aide d'extensions

Créée par Pinesh Singal (AWS)

Récapitulatif

Ce modèle de migration fournit des step-by-step conseils pour migrer une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle vers une base de données Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL compatible Edition en modifiant le code intégré natif et les extensions de PostgreSQL (). `aws_oracle_ext` `orafce` `psql` Cela permettra de gagner du temps de traitement.

Le modèle décrit une stratégie de migration manuelle hors ligne sans interruption pour une base de données source Oracle de plusieurs téraoctets comportant un grand nombre de transactions.

Le processus de migration utilise AWS Schema Conversion Tool (AWS SCT) avec les `orafce` extensions `aws_oracle_ext` et pour convertir un schéma de base de données Amazon RDS for Oracle en un schéma de base de données compatible avec Amazon RDS pour PostgreSQL ou Aurora PostgreSQL. Le code est ensuite modifié manuellement en code intégré natif compatible `psql` avec PostgreSQL. Cela est dû au fait que les appels d'extension ont un impact sur le traitement du code sur le serveur de base de données PostgreSQL et que le code d'extension n'est pas entièrement conforme ou compatible avec le code PostgreSQL.

Ce modèle se concentre principalement sur la migration manuelle de codes SQL à l'aide d'AWS SCT et des extensions `aws_oracle_ext` et. `orafce` Vous convertissez les extensions déjà utilisées en extensions natives de `psql` PostgreSQL (). Ensuite, vous supprimez toutes les références aux extensions et vous convertissez les codes en conséquence.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Système d'exploitation (Windows ou Mac) ou EC2 instance Amazon (en cours d'exécution)
- Orace

Limites

Toutes les fonctions Oracle utilisant `aws_oracle_ext` ou les `orafce` extensions ne peuvent pas être converties en fonctions PostgreSQL natives. Il peut nécessiter une refonte manuelle afin de le compiler avec les bibliothèques PostgreSQL.

L'un des inconvénients de l'utilisation des extensions AWS SCT est leur faible performance lors de l'exécution et de la récupération des résultats. Son coût peut être compris à partir d'un simple plan PostgreSQL EXPLAIN (plan d'exécution d'une instruction) relatif à la migration de la fonction `SYSDATE` Oracle vers la fonction `NOW()` PostgreSQL entre les trois codes `aws_oracle_ext` (`orafce`,, `psql` et default), comme expliqué dans la section Contrôle de comparaison des performances du document joint.

Versions du produit

- Source : base de données Amazon RDS pour Oracle 10.2 et versions ultérieures (pour 10.x), 11g (11.2.0.3.v1 et versions ultérieures) et jusqu'à 12.2, 18c et 19c (et versions ultérieures) pour Enterprise Edition, Standard Edition, Standard Edition 1 et Standard Edition 2
- Cible : base de données compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL 9.4 et versions ultérieures (pour 9.x), 10.x, 11.x, 12.x, 13.x et 14.x (et versions ultérieures)
- AWS SCT : dernière version (ce modèle a été testé avec 1.0.632)
- Oracle : dernière version (ce modèle a été testé avec 3.9.0)

Architecture

Pile technologique source

- Une instance de base de données Amazon RDS for Oracle avec la version 12.1.0.2.v18

Pile technologique cible

- Une instance de base de données compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL avec la version 11.5

Architecture de migration de base de données

Le schéma suivant représente l'architecture de migration de base de données entre les bases de données Oracle source et PostgreSQL cible. L'architecture comprend le cloud AWS, un cloud privé virtuel (VPC), des zones de disponibilité, un sous-réseau privé, une base de données Amazon RDS pour Oracle, AWS SCT, une base de données compatible Amazon RDS pour PostgreSQL ou Aurora

PostgreSQL, des extensions pour Oracle (et) et des fichiers de langage de requête structuré (SQL). `aws_oracle_ext` `orafce`

1. Lancez l'instance de base de données Amazon RDS pour Oracle (base de données source).
2. Utilisez AWS SCT avec les packs d'`orafce`extension `aws_oracle_ext` et pour convertir le code source d'Oracle vers PostreSQL.
3. La conversion produit des fichiers .sql migrés compatibles avec PostgreSQL.
4. Convertissez manuellement les codes d'extension Oracle non convertis en codes PostgreSQL (). `psql`
5. La conversion manuelle produit des fichiers .sql convertis compatibles avec PostgreSQL.
6. Exécutez ces fichiers .sql sur votre instance de base de données Amazon RDS for PostgreSQL (base de données cible).

Outils

Outils

Services AWS

- AWS SCT - AWS Schema Conversion Tool (AWS SCT) convertit votre schéma de base de données existant d'un moteur de base de données à un autre. Vous pouvez convertir un schéma de traitement transactionnel en ligne (OLTP) relationnel ou un schéma d'entrepôt de données. Votre schéma converti convient à une instance de base de données Amazon RDS pour MySQL, à un cluster de base de données Amazon Aurora, à une instance de base de données Amazon RDS pour PostgreSQL ou à un cluster Amazon Redshift. Le schéma converti peut également être utilisé avec une base de données sur une EC2 instance Amazon ou stocké sous forme de données dans un compartiment Amazon S3.

  AWS SCT fournit une interface utilisateur basée sur un projet pour convertir automatiquement le schéma de base de données de votre base de données source dans un format compatible avec votre instance Amazon RDS cible.

  Vous pouvez utiliser AWS SCT pour effectuer une migration d'une base de données source Oracle vers l'une des cibles répertoriées ci-dessus. À l'aide d'AWS SCT, vous pouvez exporter les définitions d'objets de base de données source, telles que le schéma, les vues, les procédures stockées et les fonctions.

Vous pouvez utiliser AWS SCT pour convertir des données d'Oracle vers Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL Compatible Edition.

Dans ce modèle, vous utilisez AWS SCT pour convertir et migrer le code Oracle vers PostgreSQL à l'aide des `aws_oracle_ext` extensions `orafce` et pour migrer manuellement les codes `psql` d'extension vers du code intégré par défaut ou natif.

- Le pack d'extension AWS SCT est un module complémentaire qui émule les fonctions présentes dans la base de données source qui sont requises lors de la conversion d'objets vers la base de données cible. Avant de pouvoir installer le pack d'extension AWS SCT, vous devez convertir le schéma de votre base de données.

  Lorsque vous convertissez votre schéma de base de données ou d'entrepôt de données, AWS SCT ajoute un schéma supplémentaire à votre base de données cible. Ce schéma met en œuvre les fonctions système SQL de la base de données source nécessaires lors de l'écriture du schéma converti dans la base de données cible. Ce schéma supplémentaire est appelé schéma du kit d'extension.

  Le schéma du pack d'extension pour les bases de données OLTP est nommé en fonction de la base de données source. Pour les bases de données Oracle, le schéma du pack d'extension est`AWS_ORACLE_EXT`.

Autres outils

- Oracle — Oracle est un module qui implémente des fonctions, des types de données et des packages compatibles avec Oracle. Il s'agit d'un outil open source avec une licence Berkeley Source Distribution (BSD) afin que tout le monde puisse l'utiliser. Le `orafce` module est utile pour migrer d'Oracle vers PostgreSQL car de nombreuses fonctions Oracle sont implémentées dans PostgreSQL.

Code

Pour obtenir une liste de tous les codes couramment utilisés et migrés d'Oracle vers PostgreSQL afin d'éviter l'utilisation du code d'extension AWS SCT, consultez le document ci-joint.

Épopées

Configuration de la base de données source Amazon RDS for Oracle

Tâche	Description	Compétences requises
Créez l'instance de base de données Oracle.	Créez une instance de base de données compatible avec Amazon RDS for Oracle ou Aurora PostgreSQL à partir de la console Amazon RDS.	AWS, DBA en général
Configurez les groupes de sécurité.	Configurez les groupes de sécurité entrants et sortants.	AWS général
Créez la base de données.	Créez la base de données Oracle avec les utilisateurs et les schémas nécessaires.	AWS, DBA en général
Créez les objets.	Créez des objets et insérez des données dans le schéma.	DBA

Configuration de la base de données cible Amazon RDS for PostgreSQL

Tâche	Description	Compétences requises
Créez l'instance de base de données PostgreSQL.	Créez une instance de base de données Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL à partir de la console Amazon RDS.	AWS, DBA en général
Configurez les groupes de sécurité.	Configurez les groupes de sécurité entrants et sortants.	AWS général
Créez la base de données.	Créez la base de données PostgreSQL avec les utilisate	AWS, DBA en général

Tâche	Description	Compétences requises
	urs et les schémas nécessair es.	
Validez les extensions.	Assurez-vous qu'`aws_oracle_ext orafce`ils sont correctement installés et configurés dans la base de données PostgreSQL.	DBA
Vérifiez que la base de données PostgreSQL est disponible.	Assurez-vous que la base de données PostgreSQL est opérationnelle.	DBA

Migrez le schéma Oracle vers PostgreSQL à l'aide d'AWS SCT et des extensions

Tâche	Description	Compétences requises
Installer AWS SCT.	Installez la dernière version d'AWS SCT.	DBA
Configurez AWS SCT.	Configurez AWS SCT avec les pilotes Java Database Connectivity (JDBC) pour Oracle () `ojdbc8.jar` et PostgreSQL (). `postgresql-42.2.5.jar`	DBA
Activez le pack ou le modèle d'extension AWS SCT.	Dans les paramètres du projet AWS SCT, activez l'implémentation de fonctions intégrées avec les `orafce` extensions `aws_oracle_ext` et pour le schéma de base de données Oracle.	DBA

Tâche	Description	Compétences requises
Convertissez le schéma.	Dans AWS SCT, choisisse z Convert Schema pour convertir le schéma d'Oracle en PostgreSQL et générer les fichiers .sql.	DBA

Convertir le code d'extension AWS SCT en code psql

Tâche	Description	Compétences requises
Convertissez le code manuellement.	Convertissez manuellem ent chaque ligne de code compatible avec les extension s en code intégré `psql` par défaut, comme indiqué dans le document ci-joint. Par exemple, modifier `AWS_ORACL E_EXT.SYSDATE()` ou `ORACLE.SYSDATE()` faire`NOW()`.	DBA
Validez le code	(Facultatif) Validez chaque ligne de code en l'exécutant temporairement dans la base de données PostgreSQL.	DBA
Créez des objets dans la base de données PostgreSQL.	Pour créer des objets dans la base de données PostgreSQ L, exécutez les fichiers .sql générés par AWS SCT et modifiés au cours des deux étapes précédentes.	DBA

Ressources connexes

- Base de données
  - Oracle sur Amazon RDS
  - PostgreSQL sur Amazon RDS
  - Utilisation d'Amazon Aurora PostgreSQL
  - Plan PostgreSQL EXPLAIN
- AWS SCT
  - Présentation de l'outil AWS Schema Conversion Tool
  - Guide de l'utilisateur d'AWS SCT
  - Utilisation de l'interface utilisateur AWS SCT
  - Utilisation de la base de données Oracle comme source pour AWS SCT
- Extensions pour AWS SCT
  - Utilisation du pack d'extension AWS SCT
  - Fonctionnalité Oracle (en)
  - PGXN ou
  - GitHub orafce

Informations supplémentaires

Pour plus d'informations, suivez les commandes détaillées, avec syntaxe et exemples, pour convertir manuellement le code dans le document joint.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer une base de données DB2 d'Amazon EC2 vers Aurora compatible avec MySQL à l'aide d'AWS DMS

Créée par Pinesh Singal (AWS)

Récapitulatif

Après avoir migré votre base de données IBM Db2 for LUW vers Amazon Elastic Compute Cloud EC2 (Amazon), envisagez de réorganiser l'architecture de la base de données en passant à une base de données native pour le cloud Amazon Web Services (AWS). Ce modèle couvre la migration d'une base de données IBM Db2 for LUW exécutée sur une EC2 instance Amazon vers une base de données Amazon Aurora MySQL compatible Edition sur AWS.

Le modèle décrit une stratégie de migration en ligne avec un temps d'arrêt minimal pour une base de données source DB2 de plusieurs téraoctets avec un nombre élevé de transactions.

Ce modèle utilise AWS Schema Conversion Tool (AWS SCT) pour convertir le schéma de base de données DB2 en un schéma compatible avec Aurora MySQL. Le modèle utilise ensuite AWS Database Migration Service (AWS DMS) pour migrer les données de la base de données DB2 vers la base de données compatible Aurora MySQL. Des conversions manuelles seront requises pour le code qui n'est pas converti par AWS SCT.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec un cloud privé virtuel (VPC)
- AWS SCT
- AWS DMS

Versions du produit

- Dernière version d'AWS SCT
- Db2 pour Linux version 11.1.4.4 et versions ultérieures

Architecture

Pile technologique source

- DB2/Linux x86-64 bits monté sur une instance EC2

Pile technologique cible

- Une instance de base de données Amazon Aurora compatible avec MySQL Edition

Architecture source et cible

Le schéma suivant montre l'architecture de migration des données entre la base de données source Db2 et la base de données cible compatible Aurora MySQL. L'architecture du cloud AWS comprend un cloud privé virtuel (VPC) (cloud privé virtuel), une zone de disponibilité, un sous-réseau public pour l'instance Db2 et l'instance de réplication AWS DMS, et un sous-réseau privé pour la base de données compatible Aurora MySQL.

Outils

Services AWS

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré conçu pour le cloud et compatible avec MySQL et PostgreSQL.
- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible. AWS SCT prend en charge en tant que source IBM Db2 pour LUW versions 9.1, 9.5, 9.7, 10.1, 10.5, 11.1 et 11.5.

Bonnes pratiques

Pour connaître les meilleures pratiques, consultez la section Meilleures pratiques pour AWS Database Migration Service.

Épopées

Configuration de la base de données IBM Db2 source

Tâche	Description	Compétences requises
Créez la base de données IBM Db2 sur Amazon EC2.	Vous pouvez créer une base de données IBM Db2 sur une EC2 instance en utilisant une Amazon Machine Image (AMI) d'AWS Marketplace ou en installant le logiciel Db2 sur une EC2 instance. Lancez une EC2 instance en sélectionnant une AMI pour IBM Db2 (par exemple, IBM Db2 v11.5.7 RHEL 7.9), similaire à une base de données sur site.	DBA, AWS général
Configurez les groupes de sécurité.	Configurez les règles entrantes du groupe de sécurité VPC pour SSH (Secure Shell) et TCP avec les ports 22 et 50000, respectiv ement.	AWS général
Créez l'instance de base de données.	Créez une nouvelle instance (utilisateur) et une nouvelle base de données (schéma), ou utilisez l'`db2inst1`instance par défaut et un exemple de base de données. 1. Connectez-vous à l' EC2 instance à l'aide du terminal pour vous connecter à la	DBA

Tâche	Description	Compétences requises
	base de données DB2. Vous pouvez également installer n'importe quel logiciel client de base de données qui se connectera à la base de données DB2. 2. Pour définir le mot de passe de l'utilisateur db2inst1, exécutez la commande. `sudo passwd db2inst1` 3. Pour vous connecter à l'instance db2inst1, exécutez la commande. `sudo su - db2inst1` 4. Pour vous connecter à la base de données DB2, exécutez la commande`db2`. 5. Pour vous connecter à la base de données d'exemple, utilisez la commande`connect to sample`. Vous pouvez également vous connecter à la base de données que vous avez créée. 6. Une fois connecté à l'instance de base de données, créez des objets et insérez des données dans ces objets à l'aide des instructions SQL DB2.	

Tâche	Description	Compétences requises
Vérifiez que l'instance de base de données DB2 est disponible.	Pour vérifier que l'instance de base de données DB2 est opérationnelle, utilisez la `Db2pd -` commande.	DBA

Configuration de la base de données cible compatible Aurora MySQL

Tâche	Description	Compétences requises
Créez la base de données compatible Aurora MySQL.	Création d'une base de données de compatibilité Amazon Aurora avec MySQL à partir du service AWS RDS • Créez une base de données sur Amazon Aurora compatible avec MySQL et avec la version de votre choix, par exemple Aurora (MySQL) —5.6.10a • Installez l'application MySQL Workbench ou votre logiciel client de base de données préféré qui vous permet de vous connecter à la base de données MySQL	DBA, AWS général
Configurez les groupes de sécurité.	Configurez les règles entrantes du groupe de sécurité VPC pour les connexions SSH et TCP.	AWS général
Vérifiez que la base de données Aurora est disponible.	Pour vous assurer que la base de données compatible Aurora	DBA

Tâche	Description	Compétences requises
	MySQL est opérationnelle, procédez comme suit : 1. Connectez-vous à l' EC2 instance via SSH. 2. Configurez et connectez-vous à l'instance compatible Aurora MySQL depuis MySQL Workbench. Utilisez le point de terminaison comme nom d'hôte, comme indiqué dans l'exemple suivant. `mysql-cluster-instance-1.cokmvis0v46q.us-east-1.rds.amazonaws.com` 3. Créez le nouveau schéma et connectez-vous à celui-ci (par exemple,`mysql-sample-db2`). 4. Exécutez les instructions MySQL pour vérifier les schémas et les objets de la base de données.	

Configuration et exécution d'AWS SCT

Tâche	Description	Compétences requises
Installer AWS SCT.	Téléchargez et installez la dernière version d'AWS SCT	AWS général

Tâche	Description	Compétences requises
	(la dernière version actuelle 1.0.628).	
Configurez AWS SCT.	1. Téléchargez les pilotes Java Database Connectivity (JDBC) pour IBM Db2 (version 4.22.X) et MySQL (8.x). 2. Pour configurer les pilotes dans AWS SCT, choisissez Paramètres, Paramètres globaux, Pilotes.	AWS général
Créez un projet AWS SCT.	Créez un projet et un rapport AWS SCT qui utilisent Db2 pour LUW comme moteur de base de données source et compatible Aurora MySQL pour le moteur de base de données cible. Pour identifier les privilèges nécessaires pour se connecter à une base de données DB2 pour LUW, consultez la section Utilisation de DB2 LUW comme source pour AWS SCT.	AWS général

Tâche	Description	Compétences requises
Validez les objets.	Choisissez Charger le schéma, puis validez les objets. Mettez à jour les objets incorrects dans la base de données cible : 1. Connectez-vous au serveur compatible Amazon Aurora MySQL en fournissant les informations de connexion , puis choisissez Tester la connexion. Les connexions source et cible doivent réussir avant qu'AWS SCT puisse démarrer le rapport de migration. 2. Une fois le rapport terminé, entrez le schéma à convertir, puis choisissez Terminer. AWS SCT répertorie tous les objets source et cible convertis et présentant des erreurs. 3. Vérifiez les erreurs et éliminez-les manuellement. 4. Une fois toutes les erreurs éliminées, ouvrez le menu contextuel (clic droit) du schéma, puis choisissez Charger le schéma.	DBA, AWS général

Tâche	Description	Compétences requises
	5. Choisissez Appliquer à la base de données. 6. Dans MySQL Workbench, connectez-vous à la base de données compatible Aurora MySQL et vérifiez le schéma et les objets.	

Configuration et exécution d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication.	Connectez-vous à l'AWS Management Console, accédez au service AWS DMS et créez une instance de réplication avec des paramètres valides pour le groupe de sécurité VPC que vous avez configuré pour les bases de données source et cible.	AWS général
Créez des points de terminaison.	Créez le point de terminaison source pour la base de données DB2 et créez le point de terminaison cible pour la base de données compatible Aurora MySQL : 1. Créez un point de terminaison pour IBM Db2 en tant que source en choisissant Select RDS DB instance, puis en choisissant l'instance Db2 que vous avez créée.	AWS général

Tâche	Description	Compétences requises
	Les détails de configuration du point de terminaison seront automatiquement renseignés. 2. Dans les paramètres spécifiques au point de terminaison, ajoutez les attributs de connexion supplémentaires suivants. `CurrentLSN=<scan>; MaxKBytesPerRead=64; SetDataCaptureChanges=true` Si vous ne mentionnez pas ces attributs, le test de connexion du point de terminaison source échouera. Pour plus d'informations, consultez la section Utilisation d'IBM Db2 LUW comme source pour AWS DMS. 3. Créez un point de terminaison pour Aurora MySQL compatible comme cible en choisissant Select RDS DB instance, puis en choisissant l'instance compatible Aurora MySQL que vous avez créée. Les détails de configuration du point de terminaison seront automatiquement renseigné	

Tâche	Description	Compétences requises
	s. Pour plus d'informations, consultez Utilisation d'une base de données compatible MySQL comme cible pour AWS Database Migration Service. 4. Testez les points de terminaison source et cible. Confirmez que les deux sont réussis et disponibles 5. Si le test échoue, assurez-vous que les règles entrantes du groupe de sécurité sont valides.	

Tâche	Description	Compétences requises
Créez des tâches de migration .	Créez une ou plusieurs tâches de migration pour le chargement complet et la validation CDC ou des données : 1. Pour créer une tâche de migration de base de données, choisissez l'instance de réplication, le point de terminaison de la base de données source et le point de terminaison de la base de données cible. Spécifiez le type de migration comme suit : Migrer les données existantes (chargeme nt complet), Répliquer les modifications des données uniquement (CDC) ou Migrer les données existantes et répliquer les modifications en cours (chargement complet et CDC). 2. Sous Mappages de tables, vous pouvez configurer les règles de sélection et les règles de transformation au format GUI ou JSON. 3. Sous Règles de sélection , sélectionnez le schéma, entrez le nom de la table,	AWS général

Tâche	Description	Compétences requises
	puis sélectionnez Action (Inclure/Exclure) à configure r (par exemple, Schéma : SAMPLE ; nom de la table : %, Action : Include). 4. Sous Règles de transform ation, sélectionnez la cible (schéma, table ou colonne). Sélectionnez le nom du schéma et choisissez l'action (majuscule, préfixe, suffixe) ; par exemple, Target : Schema `mysql-sample-db` ; Action : Make lowercase. 5. Activez la surveillance d'Amazon CloudWatch Logs.	
Planifiez le cycle de productio n.	Confirmez les interruptions de service auprès des parties prenantes telles que les propriétaires d'applications pour exécuter AWS DMS dans les systèmes de production.	Responsable de la migration
Exécutez les tâches de migration.	1. Démarrez la tâche AWS DMS dont le statut est Prêt. 2. Surveillez les journaux des tâches de migration dans Amazon CloudWatch Logs pour détecter toute erreur.	AWS général

Tâche	Description	Compétences requises
Validez les données.	Passez en revue les résultats et les données des tâches de migration dans les bases de données MySQL source et cible Db2 : 1. Si le statut est Chargement complet de la réplication en cours, le chargement complet avec migration des données CDC est terminé et la validation est en cours. 2. Connectez-vous à la base de données compatible Aurora MySQL et vérifiez les données. 3. Vérifiez les modifications en cours en insérant ou en mettant à jour des données dans la base de données DB2.	DBA
Arrêtez les tâches de migration.	Une fois la validation des données terminée avec succès, arrêtez les tâches de migration de validation.	AWS général

Résolution des problèmes

Problème	Solution
Les connexions de test source et cible AWS SCT échouent.	Configurez les versions du pilote JDBC et les règles entrantes du groupe de sécurité VPC pour accepter le trafic entrant.

Problème	Solution
L'exécution du test du point de terminaison source DB2 échoue.	Configurez le paramètre de connexion supplémentaire`CurrentLSN=<scan>;` .

Problème	Solution

La AWSDMS tâche ne parvient pas à se connecter à la source DB2 et l'erreur suivante est renvoyée.
 	
`database is recoverable if either or both of the database configuration parameters LOGARCHMETH1 and LOGARCHMETH2 are set to ON`
	Pour éviter cette erreur, exécutez les commandes suivantes :
	
	1. `$ db2 update db cfg for sample using LOGARCHMETH1 DISK:/home/db2inst1/logs`
	2. `$ db2stop`
	3. `$ db2start`
	4. `$ db2 connect to sample`
	
	`SQL1116N A connection to or activation of database "SAMPLE" cannot be made because of BACKUP PENDING. SQLSTATE=57019`
	
	5. `$ db2 backup database sample to ../logs`
	
	`SQL2036N The path for the file or device "../logs" is not valid`
	
	6. `$ cd`
	7. `$ pwd`
	
	`/home/db2inst1`
	
	8. `$ mkdir /tmp/backup`
	9. `$ db2 backup database sample to /tmp/backup`
	
	`Backup successful. The timestamp for this backup image is : 20190530084921`
	
	10. `$ db2 connect to sample`
	
	`Database Connection Information`

Problème	Solution

	`Database server = DB2/LINUX 9.7.1`
	`SQL authorization ID = DB2INST1`
	`Local database alias = SAMPLE`

Ressources connexes

Amazon EC2

- Amazon EC2
- Guides de EC2 l'utilisateur Amazon

Bases de données

- Base de données IBM Db2
- Amazon Aurora
- Utilisation d'Amazon Aurora MySQL

AWS SCT

- Conversion du schéma AWS DMS
- Guide de l'utilisateur de l'outil AWS Schema Conversion Tool
- Utilisation de l'interface utilisateur AWS SCT
- Utilisation d'IBM Db2 LUW comme source pour AWS SCT

AWS DMS

- AWS Database Migration Service
- Guide de l'utilisateur d'AWS Database Migration Service
- Sources pour la migration des données
- Objectifs de migration des données
- AWS Database Migration Service et AWS Schema Conversion Tool prennent désormais en charge IBM Db2 LUW en tant que source (article de blog)

- Migration d'applications exécutant des bases de données relationnelles vers AWS

Migrer une base de données Microsoft SQL Server d'Amazon EC2 vers Amazon DocumentDB à l'aide d'AWS DMS

Créée par Umamaheswara Nooka (AWS)

Récapitulatif

Ce modèle décrit comment utiliser AWS Database Migration Service (AWS DMS) pour migrer une base de données Microsoft SQL Server hébergée sur une instance Amazon Elastic Compute Cloud (Amazon EC2) vers une base de données Amazon DocumentDB (compatible avec MongoDB).

La tâche de réplication AWS DMS lit la structure des tables de la base de données SQL Server, crée la collection correspondante dans Amazon DocumentDB et effectue une migration à chargement complet.

Vous pouvez également utiliser ce modèle pour migrer une instance de base de données SQL Server sur site ou Amazon Relational Database Service (Amazon RDS) pour SQL Server vers Amazon DocumentDB. Pour plus d'informations, consultez le guide Migration des bases de données Microsoft SQL Server vers le cloud AWS sur le site Web AWS Prescriptive Guidance.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une base de données SQL Server existante sur une EC2 instance.
- Rôle de base de données fixe (db_owner) attribué à AWS DMS dans la base de données SQL Server. Pour plus d'informations, consultez la section Rôles au niveau de la base de données dans la documentation de SQL Server.
- Connaissance de l'utilisation des `mongoimport` utilitaires `mongodumpmongorestore`,`mongoexport`, et pour déplacer des données vers et depuis un cluster Amazon DocumentDB.
- Microsoft SQL Server Management Studio, installé et configuré.

Limites

- La limite de taille du cluster dans Amazon DocumentDB est de 64 To. Pour plus d'informations, consultez la section Limites de cluster dans la documentation Amazon DocumentDB.

- AWS DMS ne prend pas en charge la fusion de plusieurs tables sources en une seule collection Amazon DocumentDB.
- Si AWS DMS traite des modifications depuis une table source sans clé primaire, il ignorera les colonnes de grands objets (LOB) de la table source.

Architecture

Pile technologique source

- Amazon EC2

Architecture cible

Pile technologique cible

- Amazon DocumentDB

Outils

- AWS DMS — AWS Database Migration Service (AWS DMS) vous aide à migrer des bases de données facilement et en toute sécurité.
- Amazon DocumentDB — Amazon DocumentDB (compatible avec MongoDB) est un service de base de données rapide, fiable et entièrement géré.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS.
- Microsoft SQL Server — SQL Server est un système de gestion de base de données relationnelle.
- SQL Server Management Studio (SSMS) : SSMS est un outil de gestion de SQL Server, y compris l'accès, la configuration et l'administration des composants de SQL Server.

Épopées

Création et configuration d'un VPC

Tâche	Description	Compétences requises
Créez un VPC.	Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. Créez un cloud privé virtuel (VPC) avec une plage de blocs IPv4 CIDR.	Administrateur système
Créez des groupes de sécurité et un réseau ACLs.	Sur la console Amazon VPC, créez des groupes de sécurité et des listes de contrôle d'accès réseau (réseau ACLs) pour votre VPC, en fonction de vos besoins. Vous pouvez également utiliser les paramètres par défaut pour ces configurations. Pour plus d'informations à ce sujet et sur d'autres articles, consultez la section « Ressources connexes ».	Administrateur système

Création et configuration du cluster Amazon DocumentDB

Tâche	Description	Compétences requises
Créez un cluster Amazon DocumentDB.	Ouvrez la console Amazon DocumentDB et choisisse z « Clusters ». Choisissez « Create » et créez un cluster Amazon DocumentDB avec une instance. Important :	Administrateur système

Tâche	Description	Compétences requises
	assurez-vous de configurer ce cluster avec les groupes de sécurité de votre VPC.	
Installez le shell Mongo.	Le shell mongo est un utilitaire de ligne de commande que vous utilisez pour vous connecter à votre cluster Amazon DocumentDB et l'interroger. Pour l'installer, exécutez la commande «/etc/yum.repos.d/mongodb-org-3.6.repo » afin de créer le fichier de dépôt. Exécutez la commande « sudo yum install -y mongodb-org-shell » pour installer le shell mongo. Pour chiffrer les données en transit, téléchargez la clé publique pour Amazon DocumentDB, puis connectez-vous à votre instance Amazon DocumentDB. Pour plus d'informations sur ces étapes, consultez la section « Ressources associées ».	Administrateur système
Créez une base de données dans le cluster Amazon DocumentDB.	Exécutez la commande « use » avec le nom de votre base de données pour créer une base de données dans votre cluster Amazon DocumentDB.	Administrateur système

Création et configuration de l'instance de réplication AWS DMS

Tâche	Description	Compétences requises
Créez l'instance de réplication AWS DMS.	Ouvrez la console AWS DMS et choisissez « Créer une instance de réplication ». Entrez le nom et la description de votre tâche de réplication. Choisissez la classe d'instanc e, la version du moteur, le stockage, le VPC, le Multi-AZ et rendez-les accessibles au public. Choisissez l'onglet « Avancé » pour définir les paramètres réseau et de chiffrement. Spécifiez les paramètres de maintenance, puis choisissez « Créer une instance de réplication ».	Administrateur système
Configurez la base de données SQL Server.	Connectez-vous à Microsoft SQL Server et ajoutez une règle entrante pour la communication entre le point de terminaison source et l'instance de réplication AWS DMS. Utilisez l'adresse IP privée de l'instance de réplicati on comme source. Important : L'instance de réplication et le point de terminaison cible doivent se trouver sur le même VPC. Utilisez une autre source dans le groupe de sécurité si les instances de	Administrateur système

Tâche	Description	Compétences requises
	source et de réplication VPCs sont différentes.	

Création et test des points de terminaison source et cible dans AWS DMS

Tâche	Description	Compétences requises
Créez les points de terminaison de base de données source et cible.	Ouvrez la console AWS DMS et choisissez « Connect les points de terminaison de base de données source et cible ». Spécifiez les informations de connexion pour les bases de données source et cible. Si nécessaire, choisissez l'onglet « Avancé » pour définir les valeurs des « Attributs de connexion supplémentaires ». Téléchargez et utilisez le bundle de certificats dans la configuration de votre point de terminaison.	Administrateur système
Testez la connexion du point de terminaison.	Choisissez « Exécuter le test » pour tester la connexion . Résolvez les messages d'erreur en vérifiant les paramètres du groupe de sécurité et les connexions à l'instance de réplication AWS DMS à partir des instances de base de données source et cible.	Administrateur système

Migrer les données

Tâche	Description	Compétences requises
Créez la tâche de migration AWS DMS.	Sur la console AWS DMS, choisissez « Tâches », « Créer une tâche ». Spécifiez les options de tâche, y compris les noms des points de terminaison source et de destination, ainsi que les noms des instances de réplication. Sous « Type de migration », choisissez « Migrer les données existantes » et « Répliquer uniquement les modifications apportées aux données ». Choisissez « Démarrer la tâche ».	Administrateur système
Exécutez la tâche de migration vers AWS DMS.	Sous « Paramètres des tâches », spécifiez les paramètres du mode de préparation des tables, tels que « Ne rien faire », « Supprimer les tables sur la cible », « Tronquer » et « Inclure les colonnes LOB dans la réplication ». Définissez une taille LOB maximale acceptée par AWS DMS et choisissez « Activer la journalisation ». Conservez les valeurs par défaut des « Paramètres avancés » et choisissez « Créer une tâche ».	Administrateur système

Tâche	Description	Compétences requises
Surveillez la migration.	Sur la console AWS DMS, choisissez « Tâches » et choisissez votre tâche de migration. Choisissez « Surveillance des tâches » pour surveiller votre tâche. La tâche s'arrête lorsque la migration complète est terminée et que les modificat ions mises en cache sont appliquées.	Administrateur système

Tester et vérifier la migration

Tâche	Description	Compétences requises
Connectez-vous au cluster Amazon DocumentDB à l'aide du shell mongo.	Ouvrez la console Amazon DocumentDB, choisissez votre cluster sous « Clusters ». Dans l'onglet « Connectivité et sécurité », choisissez « Se connecter à ce cluster avec le shell mongo ».	Administrateur système
Vérifiez les résultats de votre migration.	Exécutez la commande « use » avec le nom de votre base de données, puis exécutez la commande « show collections ». Exécutez la commande « db. .count () ; » avec le nom de votre base de données. Si les résultats correspondent à ceux de votre base de données	Administrateur système

Tâche	Description	Compétences requises
	source, cela signifie que votre migration est réussie.	

Ressources connexes

Création et configuration d'un VPC

- Créez un groupe de sécurité pour votre VPC
- Création d'une ACL réseau

Création et configuration du cluster Amazon DocumentDB

- Création d'un cluster Amazon DocumentDB
- Installation du shell mongo pour Amazon DocumentDB
- Connectez-vous à votre cluster Amazon DocumentDB

Création et configuration de l'instance de réplication AWS DMS

- Utiliser des instances de réplication publiques et privées

Création et test des points de terminaison source et cible dans AWS DMS

- Utiliser Amazon DocumentDB comme cible pour AWS DMS
- Utiliser une base de données SQL Server comme source pour AWS DMS
- Utiliser les points de terminaison AWS DMS

Migrer les données

- Migrer vers Amazon DocumentDB

Autres ressources

- Limitations relatives à l'utilisation de SQL Server comme source pour AWS DMS
- Comment utiliser Amazon DocumentDB pour créer et gérer des applications à grande échelle

Migrer une base de données ThoughtSpot Falçon sur site vers Amazon Redshift

Créée par Battulga Purevragchaa (AWS) et Antony Prasad Thevaraj (AWS)

Récapitulatif

Les entrepôts de données sur site nécessitent beaucoup de temps et de ressources d'administration, en particulier pour les grands ensembles de données. Le coût financier de la construction, de l'entretien et de la croissance de ces entrepôts est également très élevé. Pour vous aider à gérer les coûts, à réduire la complexité de l'extraction, de la transformation et du chargement (ETL) et à optimiser les performances à mesure que vos données augmentent, vous devez constamment choisir les données à charger et les données à archiver.

En migrant vos bases de données ThoughtSpot Falçon sur site vers le cloud Amazon Web Services (AWS), vous pouvez accéder à des lacs de données et à des entrepôts de données basés sur le cloud qui améliorent l'agilité, la sécurité et la fiabilité des applications de votre entreprise, tout en réduisant vos coûts d'infrastructure globaux. Amazon Redshift permet de réduire de manière significative les coûts et les frais opérationnels d'un entrepôt de données. Vous pouvez également utiliser Amazon Redshift Spectrum pour analyser de grandes quantités de données dans son format natif sans les charger.

Ce modèle décrit les étapes et le processus de migration d'une base de données ThoughtSpot Falçon d'un centre de données sur site vers une base de données Amazon Redshift sur le cloud AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données ThoughtSpot Falçon hébergée dans un centre de données sur site

Versions du produit

- ThoughtSpot version 7.0.1

Architecture

Le schéma suivant illustre le flux de travail suivant :

1. Les données sont hébergées dans une base de données relationnelle sur site.
2. AWS Schema Conversion Tool (AWS SCT) convertit le langage de définition de données (DDL) compatible avec Amazon Redshift.
3. Une fois les tables créées, vous pouvez migrer les données à l'aide d'AWS Database Migration Service (AWS DMS).
4. Les données sont chargées dans Amazon Redshift.
5. Les données sont stockées dans Amazon Simple Storage Service (Amazon S3) si vous utilisez Redshift Spectrum ou si vous hébergez déjà les données dans Amazon S3.

Outils

- AWS DMS — AWS Data Migration Service (AWS DMS) vous aide à migrer rapidement et en toute sécurité des bases de données vers AWS.
- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données rapide, entièrement géré et de plusieurs pétaoctets qui permet d'analyser de manière simple et rentable toutes vos données à l'aide de vos outils de business intelligence existants.
- AWS SCT — AWS Schema Conversion Tool (AWS SCT) convertit votre schéma de base de données existant d'un moteur de base de données à un autre.

Épopées

Préparez-vous à la migration

Tâche	Description	Compétences requises
Identifiez la configuration Amazon Redshift appropriée.	Identifiez la configuration de cluster Amazon Redshift appropriée en fonction de vos besoins et du volume de données. Pour plus d'informations, consultez les clusters Amazon	DBA

Tâche	Description	Compétences requises
	Redshift dans la documenta tion Amazon Redshift.	
Faites des recherches sur Amazon Redshift pour déterminer s'il répond à vos besoins.	Utilisez Amazon Redshift FAQs pour comprendre et évaluer si Amazon Redshift répond à vos exigences.	DBA

Préparez le cluster Amazon Redshift cible

Tâche	Description	Compétences requises
Créez un cluster Amazon Redshift.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon Redshift, puis créez un cluster Amazon Redshift dans un cloud privé virtuel (VPC). Pour plus d'informations, consultez la section Création d'un cluster dans un VPC dans la documentation Amazon Redshift.	DBA
Réalisez un PoC pour la conception de votre base de données Amazon Redshift.	Suivez les meilleures pratiques d'Amazon Redshift en effectuant une preuve de concept (PoC) pour la conception de votre base de données. Pour plus d'informations, consultez la section Réalisati on d'une preuve de concept pour Amazon Redshift dans	DBA

Tâche	Description	Compétences requises
	la documentation Amazon Redshift.	
Créez des utilisateurs de base de données.	Créez les utilisateurs dans votre base de données Amazon Redshift et accordez les rôles appropriés pour accéder au schéma et aux tables. Pour plus d'informations, consultez la section Accorder des privilèges d'accès à un utilisateur ou à un groupe d'utilisateurs dans la documentation Amazon Redshift.	DBA
Appliquez les paramètres de configuration à la base de données cible.	Appliquez les paramètres de configuration à la base de données Amazon Redshift en fonction de vos besoins. Pour plus d'informations sur l'activation des paramètre s de base de données, de session et de niveau serveur, consultez la référence de configuration dans la documentation Amazon Redshift.	DBA

Création d'objets dans le cluster Amazon Redshift

Tâche	Description	Compétences requises
Créez manuellement des tables avec DDL dans Amazon Redshift.	(Facultatif) Si vous utilisez AWS SCT, les tables sont créées automatiquement. Toutefois, en cas d'échec lors de la réplication DDLs, vous devez créer les tables manuellement	DBA
Créez des tables externes pour Redshift Spectrum.	Créez une table externe avec un schéma externe pour Amazon Redshift Spectrum. Pour créer des tables externes, vous devez être le propriétaire du schéma externe ou un superutilisateur de base de données. Pour plus d'informations, consultez la section Création de tables externes pour Amazon Redshift Spectrum dans la documentation Amazon Redshift.	DBA

Migrer des données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Utilisez AWS DMS pour migrer les données.	Après avoir créé le DDL des tables dans la base de données Amazon Redshift, migrez vos données vers	DBA

Tâche	Description	Compétences requises
	Amazon Redshift à l'aide d'AWS DMS. Pour obtenir des instructions et des étapes détaillées, consultez la section Utilisation d'une base de données Amazon Redshift comme cible pour AWS DMS dans la documentation AWS DMS.	
Utilisez la commande COPY pour charger les données.	Utilisez la `COPY` commande Amazon Redshift pour charger les données d'Amazon S3 vers Amazon Redshift. Pour plus d'informations, consultez la section Utilisation de la commande COPY pour charger depuis Amazon S3 dans la documentation Amazon Redshift.	DBA

Valider le cluster Amazon Redshift

Tâche	Description	Compétences requises
Validez les enregistrements source et cible.	Validez le nombre de tables pour les enregistrements source et cible chargés depuis votre système source.	DBA
Mettez en œuvre les meilleures pratiques d'Amazon Redshift pour optimiser les performances.	Mettez en œuvre les meilleures pratiques d'Amazon Redshift pour la conception de tables et de bases de données.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez le billet de blog Les 10 meilleures techniques d'optimisation des performances pour Amazon Redshift.	
Optimisez les performances des requêtes.	Amazon Redshift utilise des requêtes SQL pour interagir avec les données et les objets du système. Le langage de manipulation de données (DML) est le sous-ensemble du langage SQL que vous pouvez utiliser pour afficher, ajouter, modifier et supprimer des données. Le DDL est le sous-ensemble de SQL que vous utilisez pour ajouter, modifier et supprimer des objets de base de données tels que des tables et des vues. Pour plus d'informations, consultez la section Optimisation des performances des requêtes dans la documentation Amazon Redshift.	DBA

Tâche	Description	Compétences requises
Implémentez le WLM.	Vous pouvez utiliser la gestion de la charge de travail (WLM) pour définir plusieurs files d'attente de requêtes et acheminer les requêtes vers les files d'attente appropriées lors de l'exécution. Pour plus d'informations, consultez Implémentation de la gestion de la charge de travail dans la documentation Amazon Redshift.	DBA
Travaillez avec la mise à l'échelle simultanée.	En utilisant la fonctionnalité Concurrency Scaling, vous pouvez prendre en charge un nombre pratiquement illimité d'utilisateurs simultanés et de requêtes simultanées, avec des performances de requête toujours rapides. Pour plus d'informations, consultez la section Utilisation du dimensionnement simultané dans la documentation Amazon Redshift.	DBA

Tâche	Description	Compétences requises
Utilisez les meilleures pratiques d'Amazon Redshift pour la conception des tables.	Lorsque vous planifiez votre base de données, certaines décisions importantes relatives à la conception des tables peuvent fortement influencer les performances globales des requêtes. Pour plus d'informations sur le choix de l'option de conception de table la plus appropriée, consultez les meilleures pratiques d'Amazon Redshift pour la conception de tables dans la documentation Amazon Redshift.	DBA
Créez des vues matérialisées dans Amazon Redshift.	Une vue matérialisée contient un ensemble de résultats précalculés basé sur une requête SQL sur une ou plusieurs tables de base. Vous pouvez émettre `SELECT` des instructions pour interroge r une vue matérialisée de la même manière que vous interrogez d'autres tables ou vues de la base de données. Pour plus d'informations, consultez la section Création de vues matérialisées dans Amazon Redshift dans la documentation Amazon Redshift.	DBA

Tâche	Description	Compétences requises
Définissez les jointures entre les tables.	Pour effectuer une recherche dans plusieurs tables à la fois ThoughtSpot, vous devez définir les jointures entre les tables en spécifian t les colonnes contenant les données correspon dantes dans deux tables. Ces colonnes représentent la fin `primary key` `foreign key` de la jointure. Vous pouvez les définir à l'aide de la `ALTER TABLE` commande dans Amazon Redshift ou. ThoughtSpot Pour plus d'informations, consultez ALTER TABLE dans la documentation Amazon Redshift.	DBA

Configurer la ThoughtSpot connexion à Amazon Redshift

Tâche	Description	Compétences requises
Ajoutez une connexion Amazon Redshift.	Ajoutez une connexion Amazon Redshift à votre base de données Falçon sur site. ThoughtSpot Pour plus d'informations, consultez la section Ajouter une connexion Amazon	DBA

Tâche	Description	Compétences requises
	Redshift dans la ThoughtSpot documentation.	
Modifiez la connexion Amazon Redshift.	Vous pouvez modifier la connexion Amazon Redshift pour ajouter des tables et des colonnes. Pour plus d'informations, consultez Modifier une connexion Amazon Redshift dans la ThoughtSpot documentation.	DBA

Tâche	Description	Compétences requises
Remappez la connexion Amazon Redshift.	Modifiez les paramètres de connexion en modifiant le fichier de mappage source .yaml créé lorsque vous avez ajouté la connexion Amazon Redshift. Par exemple, vous pouvez remapper la table ou la colonne existante à une autre table ou colonne dans une connexion à une base de données existante. ThoughtSpot recommande de vérifier les dépendances avant et après le remappage d'une table ou d'une colonne dans une connexion afin de s'assurer qu'elles s'affichent comme prévu. Pour plus d'informations, consultez Remapper une connexion Amazon Redshift dans ThoughtSpot la documentation.	DBA

Tâche	Description	Compétences requises
Supprimez une table de la connexion Amazon Redshift.	(Facultatif) Si vous tentez de supprimer une table dans une connexion Amazon Redshift, vérifiez ThoughtSpot les dépendances et affiche une liste des objets dépendants. Vous pouvez choisir les objets répertoriés pour les supprimer ou supprimer la dépendance. Vous pouvez ensuite retirer le tableau. Pour plus d'informations, consultez Supprimer une table d'une connexion Amazon Redshift dans la ThoughtSpot documentation.	DBA

Tâche	Description	Compétences requises
Supprimez une table contenant des objets dépendants d'une connexion Amazon Redshift.	(Facultatif) Si vous essayez de supprimer un tableau contenant des objets dépendants, l'opération est bloquée. Une `Cannot delete` fenêtre apparaît, avec une liste de liens vers des objets dépendants. Lorsque toutes les dépendances sont supprimées, vous pouvez supprimer la table Pour plus d'informations, consultez Supprimer une table contenant des objets dépendants d'une connexion Amazon Redshift dans la ThoughtSpot documentation.	DBA
Supprimez une connexion Amazon Redshift.	(Facultatif) Comme une connexion peut être utilisée dans plusieurs sources de données ou visualisations, vous devez supprimer toutes les sources et tâches qui utilisent cette connexion avant de pouvoir supprimer la connexion Amazon Redshift. Pour plus d'informations, consultez Supprimer une connexion Amazon Redshift dans la ThoughtSpot documentation.	DBA

Tâche	Description	Compétences requises
Vérifiez la référence de connexion pour Amazon Redshift.	Assurez-vous de fournir les informations requises pour votre connexion Amazon Redshift en utilisant la référence de connexion figurant dans la ThoughtSpot documentation.	DBA

Informations supplémentaires

- Analyses basées sur l'IA à n'importe quelle échelle avec Amazon ThoughtSpot Redshift
- Tarification d'Amazon Redshift
- Commencer à utiliser AWS SCT
- Commencer à utiliser Amazon Redshift
- Utilisation d'agents d'extraction de données
- Chick-fil-A accélère l'obtention d'informations grâce ThoughtSpot à AWS

Migrer une base de données Oracle vers Amazon DynamoDB à l'aide d'AWS DMS

Créée par Rambabu Karnena (AWS)

Récapitulatif

Ce modèle explique les étapes de migration d'une base de données Oracle vers Amazon DynamoDB à l'aide d'AWS Database Migration Service (AWS DMS). Il couvre trois types de bases de données sources :

- Bases de données Oracle sur site
- Bases de données Oracle sur Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Relational Database Service (Amazon RDS) pour les instances de base de données Oracle

Dans cette preuve de concept, ce modèle met l'accent sur la migration depuis une instance de base de données Amazon RDS pour Oracle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une application se connectant à une base de données Amazon RDS for Oracle
- Une table créée dans la base de données source Amazon RDS for Oracle avec une clé primaire et des exemples de données

Limites

- Les objets de base de données Oracle, tels que les procédures, les fonctions, les packages et les déclencheurs, ne sont pas pris en compte pour la migration car Amazon DynamoDB ne prend pas en charge ces objets de base de données.

Versions du produit

- Ce modèle s'applique à toutes les éditions et versions des bases de données Oracle prises en charge par AWS DMS. Pour plus d'informations, consultez les sections Utilisation d'une base de

données Oracle comme source pour AWS DMS et Utilisation d'une base de données Amazon DynamoDB comme cible pour AWS DMS. Nous vous recommandons d'utiliser les dernières versions d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.

Architecture

Pile technologique source

- Instances de bases de données Amazon RDS for Oracle, Oracle sur EC2 Amazon ou bases de données Oracle sur site

Pile technologique cible

- Amazon DynamoDB

Architecture de migration de données AWS

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS. Ce modèle utilise Amazon RDS for Oracle.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Créez un VPC.	Dans votre compte AWS, créez un cloud privé virtuel	Administrateur de systèmes

Tâche	Description	Compétences requises
	(VPC) et un sous-réseau privé.	
Créez des groupes de sécurité et des listes de contrôle d'accès au réseau.	Pour plus d'informations, consultez la documentation AWS.	Administrateur de systèmes
Configurez et démarrez l'instance de base de données Amazon RDS for Oracle.	Pour plus d'informations, consultez la documentation AWS.	DBA, administrateur système

Migrer les données

Tâche	Description	Compétences requises
Créez un rôle IAM pour accéder à DynamoDB.	Dans la console AWS Identity and Access Management (IAM), créez le rôle, attachez la politique `AmazonDynamoDBFullAccess to it` et sélectionnez AWS DMS comme service.	Administrateur de systèmes
Créez une instance de réplication AWS DMS pour la migration.	L'instance de réplication doit se trouver dans la même zone de disponibilité et le même VPC que la base de données source.	Administrateur de systèmes
Créez des points de terminaison source et cible dans AWS DMS.	Pour créer le point de terminaison de la base de données source, deux options s'offrent à vous : • Sur la console Amazon RDS, choisissez Databases,	Administrateur de systèmes

Tâche	Description	Compétences requises
	DB identifier, Connectivity & Security, puis choisissez le point de terminaison. • Sur la console AWS DMS, choisissez Select RDS DB instance. Pour créer le point de terminaison de base de données cible, choisissez le rôle Amazon Resource Name (ARN) dans la tâche précédente pour accéder à DynamoDB.	
Créez une tâche AWS DMS pour charger les tables de base de données Oracle source dans DynamoDB.	Choisissez les noms des points de terminaison source et de destination ainsi que l'instance de réplication à partir des étapes précédent es. Le type peut être à pleine charge. Choisissez le schéma Oracle et spécifiez % pour sélectionner toutes les tables.	Administrateur de systèmes
Validez les tables dans DynamoDB.	Pour afficher les résultats de la migration, choisissez Tables dans le volet de navigatio n de gauche de la console DynamoDB.	DBA

Migrer l'application

Tâche	Description	Compétences requises
Modifiez le code de l'application.	Pour vous connecter à DynamoDB et récupérer des données depuis DynamoDB, mettez à jour le code de l'application.	Propriétaire de l'application, DBA, administrateur système

Découper

Tâche	Description	Compétences requises
Changez les clients de l'application pour qu'ils utilisent DynamoDB.		DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS.	Par exemple, l'arrêt de l'instance Amazon RDS pour Oracle, DynamoDB et de l'instance de réplication AWS DMS.	DBA, administrateur système
Collectez des statistiques.	Les indicateurs incluent le temps de migration, les pourcentages de travail manuel et de travail effectué par l'outil, ainsi que les économies de coûts.	DBA, propriétaire de l'application, administrateur système

Ressources connexes

- AWS Database Migration Service et Amazon DynamoDB : ce que vous devez savoir (article de blog)
- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Utilisation d'une base de données Amazon DynamoDB comme cible pour AWS Database Migration Service
- Bonnes pratiques pour la migration d'un SGBDR vers Amazon DynamoDB (livre blanc)

Migrer une table partitionnée Oracle vers PostgreSQL à l'aide d'AWS DMS

Créée par Saurav Mishra (AWS) et Eduardo Valentim (AWS)

Récapitulatif

Ce modèle décrit comment accélérer le chargement d'une table partitionnée d'Oracle vers PostgreSQL à l'aide d'AWS Database Migration Service (AWS DMS), qui ne prend pas en charge le partitionnement natif. La base de données PostgreSQL cible peut être installée sur Amazon Elastic Compute Cloud (Amazon), ou il peut s'agir d'une instance de base de données EC2 Amazon Relational Database Service (Amazon RDS) pour PostgreSQL ou d'une instance de base de données Amazon Aurora PostgreSQL Edition compatible.

Le téléchargement d'une table partitionnée inclut les étapes suivantes :

1. Créez une table parent similaire à la table de partition Oracle, mais n'incluez aucune partition.
2. Créez des tables enfants qui hériteront de la table parent que vous avez créée à l'étape 1.
3. Créez une fonction de procédure et un déclencheur pour gérer les insertions dans la table parent.

Cependant, comme le déclencheur est déclenché à chaque insertion, le chargement initial à l'aide d'AWS DMS peut être très lent.

Pour accélérer les chargements initiaux d'Oracle vers PostgreSQL 9.0, ce modèle crée une tâche AWS DMS distincte pour chaque partition et charge les tables enfants correspondantes. Vous créez ensuite un déclencheur lors du passage.

La version 10 de PostgreSQL prend en charge le partitionnement natif. Toutefois, vous pouvez décider d'utiliser le partitionnement hérité dans certains cas. Pour plus d'informations, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle source avec une table partitionnée
- Une base de données PostgreSQL sur AWS

Versions du produit

- PostgreSQL 9.0

Architecture

Pile technologique source

- Une table partitionnée dans Oracle

Pile technologique cible

- Une table partitionnée dans PostgreSQL (sur EC2 Amazon, Amazon RDS pour PostgreSQL ou Aurora PostgreSQL)

Architecture cible

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.

Épopées

Configuration d'AWS DMS

Tâche	Description	Compétences requises
Créez les tables dans PostgreSQL.	Créez les tables parent et enfant correspondantes dans PostgreSQL avec les conditions de vérification requises pour les partitions.	DBA
Créez la tâche AWS DMS pour chaque partition.	Incluez la condition de filtre de la partition dans la tâche AWS DMS. Mappez les partitions aux tables enfants PostgreSQL correspondantes.	DBA

Tâche	Description	Compétences requises
Exécutez les tâches AWS DMS en utilisant le chargement complet et la capture des données de modification (CDC).	Assurez-vous que le `StopTaskCachedChanges Applied` paramètre est défini sur `true` et que le `StopTaskCachedChanges NotApplied` paramètre est défini sur`false`.	DBA

Découper

Tâche	Description	Compétences requises
Arrêtez les tâches de réplication.	Avant d'arrêter les tâches, vérifiez que la source et la destination sont synchronisées.	DBA
Créez un déclencheur sur la table parent.	Étant donné que la table parent recevra toutes les commandes d'insertion et de mise à jour, créez un déclencheur qui achemine ces commandes vers les tables enfants respectives en fonction de la condition de partitionnement.	DBA

Ressources connexes

- AWS DMS
- Partitionnement de tables (documentation PostgreSQL)

Informations supplémentaires

Bien que PostgreSQL version 10 prenne en charge le partitionnement natif, vous pouvez décider d'utiliser le partitionnement hérité dans les cas d'utilisation suivants :

- Le partitionnement impose une règle selon laquelle toutes les partitions doivent avoir le même ensemble de colonnes que le parent, mais l'héritage des tables permet aux enfants d'avoir des colonnes supplémentaires.
- L'héritage de tables prend en charge les héritages multiples.
- Le partitionnement déclaratif ne prend en charge que le partitionnement par liste et par plage. Grâce à l'héritage des tables, vous pouvez diviser les données comme vous le souhaitez. Toutefois, si l'exclusion des contraintes ne permet pas d'élaguer efficacement les partitions, les performances des requêtes en pâtiront.
- Certaines opérations nécessitent un verrou plus fort lors de l'utilisation du partitionnement déclaratif que lors de l'utilisation de l'héritage de tables. Par exemple, l'ajout ou la suppression d'une partition dans ou depuis une table partitionnée nécessite un `ACCESS EXCLUSIVE` verrou sur la table parent, alors qu'un `SHARE UPDATE EXCLUSIVE` verrou suffit pour un héritage normal.

Lorsque vous utilisez des partitions de travail distinctes, vous pouvez également recharger les partitions en cas de problème de validation AWS DMS. Pour améliorer les performances et le contrôle de la réplication, exécutez les tâches sur des instances de réplication distinctes.

Migrer d'Amazon RDS for Oracle vers Amazon RDS for MySQL

Créée par Jitender Kumar (AWS), Neha Sharma (AWS) et Srini Ramaswamy (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle vers une instance de base de données Amazon RDS for MySQL sur Amazon Web Services (AWS). Le modèle utilise AWS Database Migration Service (AWS DMS) et AWS Schema Conversion Tool (AWS SCT).

Le modèle fournit les meilleures pratiques pour gérer la migration des procédures stockées. Il couvre également et modifie le code pour prendre en charge la couche d'application.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une base de données source Amazon RDS for Oracle.
- Une base de données cible Amazon RDS for MySQL. Les bases de données source et cible doivent se trouver dans le même cloud privé virtuel (VPC). Si vous en utilisez plusieurs VPCs, ou si vous devez disposer des autorisations d'accès requises.
- Groupes de sécurité qui permettent la connectivité entre les bases de données source et cible, AWS SCT, le serveur d'applications et AWS DMS.
- Un compte utilisateur doté des privilèges requis pour exécuter AWS SCT sur la base de données source.
- La journalisation supplémentaire est activée pour exécuter AWS DMS sur la base de données source.

Limites

- La limite de taille des bases de données Amazon RDS source et cible est de 64 To. Pour obtenir des informations sur la taille d'Amazon RDS, consultez la documentation AWS.
- Oracle ne fait pas la distinction majuscules/majuscules pour les objets de base de données, mais pas MySQL. AWS SCT peut gérer ce problème lors de la création d'un objet. Cependant, un certain travail manuel est nécessaire pour pallier l'indifférence totale entre majuscules et minuscules.

- Cette migration n'utilise pas les extensions MySQL pour activer les fonctions natives d'Oracle. AWS SCT gère la majeure partie de la conversion, mais certains travaux sont nécessaires pour modifier le code manuellement.
- Les modifications du pilote Java Database Connectivity (JDBC) sont requises dans l'application.

Versions du produit

- Amazon RDS pour Oracle 12.2.0.1 et versions ultérieures. Pour connaître les versions RDS pour Oracle actuellement prises en charge, consultez la documentation AWS.
- Amazon RDS for MySQL 8.0.15 et versions ultérieures. Pour connaître les versions de RDS pour MySQL actuellement prises en charge, consultez la documentation AWS.
- AWS DMS version 3.3.0 et versions ultérieures. Consultez la documentation AWS pour plus d'informations sur les points de terminaison source et les points de terminaison cibles pris en charge par AWS DMS.
- AWS SCT version 1.0.628 et versions ultérieures. Consultez la matrice de prise en charge des points de terminaison source et cible AWS SCT dans la documentation AWS.

Architecture

Pile technologique source

- Amazon RDS pour Oracle. Pour plus d'informations, consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS.

Pile technologique cible

- Amazon RDS pour MySQL. Pour plus d'informations, consultez la section Utilisation d'une base de données compatible MySQL comme cible pour AWS DMS.

Architecture de migration

Dans le schéma suivant, AWS SCT copie et convertit des objets de schéma depuis la base de données source Amazon RDS for Oracle et envoie les objets vers la base de données cible Amazon RDS for MySQL. AWS DMS réplique les données de la base de données source et les envoie à l'instance Amazon RDS for MySQL.

Outils

- AWS Data Migration Service vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS. Ce modèle utilise Amazon RDS pour Oracle et Amazon RDS pour MySQL.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Épopées

Préparation à la migration

Tâche	Description	Compétences requises
Validez les versions et les moteurs de base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, SysAdmin
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d'instance approprié (capacité, fonctionnalités de stockage, fonctionnalités réseau).		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin

Tâche	Description	Compétences requises
Choisissez une stratégie de migration d'applications.	Déterminez si vous souhaitez un temps d'arrêt complet ou partiel pour les activités de transition.	DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un VPC et des sous-réseaux.		SysAdmin
Créez des groupes de sécurité et des listes de contrôle d'accès au réseau (ACLs).		SysAdmin
Configurez et démarrez l'instance Amazon RDS for Oracle.		DBA, SysAdmin
Configurez et démarrez l'instance Amazon RDS for MySQL.		DBA, SysAdmin
Préparez un scénario de test pour la validation de la conversion de code.	Cela facilitera les tests unitaires pour le code converti.	DBA, Développeur
Configurez l'instance AWS DMS.		
Configurez les points de terminaison source et cible dans AWS DMS.		

Migrer les données

Tâche	Description	Compétences requises
Générez le script de base de données cible à l'aide d'AWS SCT.	Vérifiez l'exactitude du code converti par AWS SCT. Certains travaux manuels seront nécessaires.	DBA, Développeur
Dans AWS SCT, choisissez le paramètre « Insensible aux majuscules et minuscules ».	Dans AWS SCT, choisisse z Paramètres du projet, Target Case Sensibility, Case Insensitive.	DBA, Développeur
Dans AWS SCT, choisissez de ne pas utiliser la fonction native d'Oracle.	Dans les paramètres du projet, cochez les fonctions TO_ CHAR/TO_NUMBER/TO _DATE.	DBA, Développeur
Modifiez le code « sql%notfo und ».	Vous devrez peut-être convertir le code manuellem ent.	
Interrogez les tables et les objets dans les procédures stockées (utilisez des requêtes en minuscules).		DBA, Développeur
Créez le script principal une fois que toutes les modificat ions ont été apportées, puis déployez le script principal sur la base de données cible.		DBA, Développeur
Testez les procédures stockées et les appels d'application unitaires à l'aide d'échantillons de données.		

Tâche	Description	Compétences requises
Nettoyez les données créées lors des tests unitaires.		DBA, Développeur
Supprimez les contraintes liées aux clés étrangères sur la base de données cible.	Cette étape est nécessaire pour charger les données initiales. Si vous ne souhaitez pas supprimer les contraintes liées aux clés étrangères, vous devez créer une tâche de migration pour les données spécifiques aux tables principale et secondaire.	DBA, Développeur
Supprimez les clés primaires et les clés uniques dans la base de données cible.	Cette étape permet d'obtenir de meilleures performances pour le chargement initial.	DBA, Développeur
Activez la journalisation supplémentaire sur la base de données source.		DBA
Créez une tâche de migration pour le chargement initial dans AWS DMS, puis exécutez-la.	Choisissez l'option permettant de migrer les données existantes.	DBA
Ajoutez les clés primaires et les clés étrangères à la base de données cible.	Les contraintes doivent être ajoutées après le chargement initial.	DBA, Développeur
Créez une tâche de migration pour une réplication continue.	La réplication continue permet de synchroniser la base de données cible avec la base de données source.	DBA

Migrer des applications

Tâche	Description	Compétences requises
Remplacez les fonctions natives d'Oracle par des fonctions natives de MySQL.		Propriétaire de l'application
Assurez-vous que seuls les noms en minuscules sont utilisés pour les objets de base de données dans les requêtes SQL.		DBA, propriétaire de SysAdmin l'application

Passez à la base de données cible

Tâche	Description	Compétences requises
Arrêtez le serveur d'applica tions.		Propriétaire de l'application
Vérifiez que les bases de données source et cible sont synchronisées.		DBA, propriétaire de l'applica tion
Arrêtez l'instance de base de données Amazon RDS for Oracle.		DBA
Arrêtez la tâche de migration.	Cela s'arrêtera automatiq uement une fois que vous aurez terminé l'étape précédente.	DBA
Changez la connexion JDBC d'Oracle à MySQL.		Propriétaire de l'application, DBA

Tâche	Description	Compétences requises
Lancez l'application.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Passez en revue et validez les documents du projet.		DBA, SysAdmin
Collectez des indicateurs sur le temps de migration , le pourcentage de tâches manuelles par rapport aux tâches liées aux outils, les économies de coûts, etc.		DBA, SysAdmin
Arrêtez et supprimez les instances AWS DMS.		DBA
Supprimez les points de terminaison source et cible.		DBA
Supprimez les tâches de migration.		DBA
Prenez un instantané de l'instance de base de données Amazon RDS for Oracle.		DBA
Supprimez l'instance de base de données Amazon RDS for Oracle.		DBA
Arrêtez et supprimez toutes les autres ressources AWS		DBA, SysAdmin

Tâche	Description	Compétences requises
temporaires que vous avez utilisées.		
Clôturez le projet et faites part de vos commentaires.		DBA

Ressources connexes

- AWS DMS
- AWS SCT
- Tarification d'Amazon RDS
- Commencer à utiliser AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)

Migrez d'IBM Db2 sur Amazon vers une version compatible avec Aurora PostgreSQL EC2 à l'aide d'AWS DMS et d'AWS SCT

Créée par Sirsendu Halder (AWS) et Abhimanyu Chhabra (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données IBM Db2 sur une instance Amazon Elastic Compute Cloud EC2 (Amazon) vers une instance de base de données Amazon Aurora PostgreSQL Edition compatible. Ce modèle utilise AWS Database Migration Service (AWS DMS) et AWS Schema Conversion Tool (AWS SCT) pour la migration des données et la conversion de schéma.

Le modèle cible une stratégie de migration en ligne avec peu ou pas de temps d'arrêt pour une base de données IBM Db2 de plusieurs téraoctets comportant un grand nombre de transactions. Nous vous recommandons de convertir les colonnes en clés primaires (PKs) et en clés étrangères (FKs) avec le type de données `NUMERIC` vers `INT` ou `BIGINT` dans PostgreSQL pour de meilleures performances.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données IBM Db2 source sur une instance EC2

Versions du produit

- DB2/LINUXX8664 version 11.1.4.4 et versions ultérieures

Architecture

Pile technologique source

- Une base de données DB2 sur une instance EC2

Pile technologique cible

- Une instance de base de données compatible avec Aurora PostgreSQL version 10.18 ou ultérieure

Architecture de migration de base de données

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des bases de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site. La base de données source reste pleinement opérationnelle pendant la migration, minimisant ainsi les interruptions de service pour les applications qui dépendent de la base de données. Vous pouvez utiliser AWS DMS pour migrer vos données vers et depuis les bases de données commerciales et open source les plus utilisées. AWS DMS prend en charge les migrations hétérogènes entre différentes plateformes de base de données, telles qu'IBM Db2 vers la version 10.18 ou supérieure compatible avec Aurora PostgreSQL. Pour plus de détails, consultez les sections Sources pour la migration des données et cibles pour la migration des données dans la documentation AWS DMS.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité des objets du code de base de données, y compris les vues, les procédures stockées et les fonctions, dans un format compatible avec la base de données cible. Tous les objets qui ne sont pas automatiquement convertis sont clairement marqués afin de pouvoir être convertis manuellement pour terminer la migration. AWS SCT peut également analyser le code source de l'application à la recherche d'instructions SQL intégrées et les convertir.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Créez une instance de base de données compatible avec Aurora PostgreSQL.	Pour créer l'instance de base de données, suivez les instructions de la documentation AWS. Pour le type de moteur, choisissez Amazon Aurora. Pour l'édition, choisissez l'édition compatible avec Amazon Aurora PostgreSQL.	Amazon RDS

Tâche	Description	Compétences requises
	L'instance de base de données compatible Aurora PostgreSQL version 10.18 ou ultérieure doit se trouver dans le même cloud privé virtuel (VPC) que la base de données IBM Db2 source.	

Convertissez le schéma de votre base de données

Tâche	Description	Compétences requises
Installez et vérifiez AWS SCT.	1. Installez AWS SCT en suivant les étapes décrites dans la documentation AWS SCT. 2. Vérifiez l'installation en suivant les procédures décrites dans la documentation AWS SCT.	Administrateur AWS, DBA, ingénieur en migration
Démarrez AWS SCT et créez un projet.	Pour démarrer l'outil AWS SCT et créer un nouveau projet afin d'exécuter un rapport d'évaluation de la migration de base de données, suivez les instructions de la documentation AWS SCT.	Ingénieur en migration
Ajoutez des serveurs de base de données et créez une règle de mappage.	1. Ajoutez des serveurs de base de données source et cible en suivant les instructions de la documentation AWS SCT.	Ingénieur en migration

Tâche	Description	Compétences requises
	2. Créez une règle de mappage pour définir la plate-forme de base de données cible pour votre base de données source. Pour obtenir des instructions, consultez la documentation AWS SCT.	
Créez un rapport d'évaluation de la migration de base de données.	Créez le rapport d'évaluation de la migration de base de données en suivant les étapes de la documentation AWS SCT.	Ingénieur en migration
Consultez le rapport d'évaluation.	Utilisez l'onglet Résumé du rapport d'évaluation de la migration de base de données pour consulter le rapport et analyser les données. Cette analyse vous aidera à déterminer la complexité de la migration. Pour plus d'informations, consultez la documentation AWS SCT.	Ingénieur en migration

Tâche	Description	Compétences requises
Convertissez le schéma.	Pour convertir les schémas de votre base de données source : 1. Sur la console AWS SCT, choisissez View, puis Main view. 2. Sélectionnez l'objet ou le nœud parent dans votre schéma source, ouvrez le menu contextuel (clic droit), puis choisissez Convertir le schéma. Pour plus d'informations, consultez la documentation AWS SCT.	Ingénieur en migration
Appliquez le schéma de base de données converti à l'instance de base de données cible.	1. Choisissez l'élément de schéma dans le panneau droit de votre projet, qui présente le schéma planifié de l'instance DB cible. 2. Ouvrez le menu contextuel (clic droit) pour l'élément de schéma, puis choisissez Apply to database. Pour plus d'informations, consultez la documentation AWS SCT.	Ingénieur en migration

Migrez vos données

Tâche	Description	Compétences requises
Configurez un VPC et des groupes de paramètres de base de données.	Configurez un VPC et des groupes de paramètres de base de données, et configure z les règles et paramètre s entrants requis pour la migration. Pour obtenir des instructions, consultez la documentation AWS DMS. Pour le groupe de sécurité VPC, sélectionnez à la fois l' EC2 instance pour Db2 et l'instance de base de données compatible Aurora PostgreSQ L. Cette instance de réplicati on doit se trouver dans le même VPC que les instances de base de données source et cible.	Ingénieur en migration
Préparez les instances de base de données source et cible.	Préparez les instances de base de données source et cible pour la migration . Dans un environnement de production, la base de données source existe déjà. Pour la base de données source, le nom du serveur doit être le système de noms de domaine (DNS) public de l' EC2 instance sur laquelle Db2 est exécuté. Pour le nom d'utilisateur, vous pouvez	Ingénieur en migration

Tâche	Description	Compétences requises
	utiliser `db2inst1` suivi du port, qui sera 5000 pour IBM Db2.	
Créez un EC2 client Amazon et des points de terminaison.	1. Créez un EC2 client Amazon. Vous utilisez ce client pour remplir la base de données source avec des données à répliquer . Vous utilisez également ce client pour vérifier la réplication en exécutant des requêtes sur la base de données cible. 2. Créez des points de terminaison pour la base de données source et l'instance de base de données cible à utiliser pour les étapes suivantes. Pour obtenir des instructions, consultez la documentation AWS DMS. Vous devez créer des points de terminaison distincts pour les bases de données source et cible. Pour la version 10.18 ou ultérieure compatible avec Aurora PostgreSQL, le port sera 5432, et vous pouvez obtenir le nom du serveur à partir du point de terminaison de l'instance de base de données.	Ingénieur en migration

Tâche	Description	Compétences requises
Créez une instance de réplication.	Créez une instance de réplication à l'aide de la console AWS DMS et spécifiez les points de terminaison source et cible. L'instance de réplication effectue la migration des données entre les points de terminaison. Pour en savoir plus, consultez la documentation AWS DMS.	Ingénieur en migration

Tâche	Description	Compétences requises
Créez une tâche AWS DMS pour migrer les données.	Créez une tâche pour charger les tables IBM Db2 source sur l'instance de base de données PostgreSQL cible en suivant les étapes de la documentation AWS DMS. • Pour la source et la cible, utilisez les noms des points de terminaison source et de destination. • Le type de migration peut être à chargement complet. • Pour la règle de schéma, vous pouvez utiliser le `inst1` schéma de la base de données DB2. • Pour le nom de la table, indiquez que toutes les tables doivent `%` être migrées. Une fois le chargement terminé, vous verrez les tables DB2 du `inst1` schéma apparaître dans la base de données compatible Aurora PostgreSQL.	Ingénieur en migration

Ressources connexes

Références

- Documentation Amazon Aurora
- Documentation sur le wrapper de données étrangères (FDW) PostgreSQL

- Documentation relative à l'importation de schémas étrangers dans PostgreSQL
- Documentation AWS DMS
- Documentation AWS SCT

Tutoriels et vidéos

- Mise en route avec AWS DMS (procédure pas à pas)
- Présentation d'Amazon EC2 - Serveur cloud élastique et hébergement avec AWS (vidéo)

Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide d'AWS DMS SharePlex

Créée par Kumar Babu PG (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Oracle 8i ou 9i sur site vers Amazon Relational Database Service (Amazon RDS) pour PostgreSQL ou Amazon Aurora PostgreSQL. AWS Database Migration Service (AWS DMS) ne prend pas en charge Oracle 8i ou 9i en tant que source. Quest SharePlex réplique donc les données d'une base de données 8i ou 9i sur site vers une base de données Oracle intermédiaire (Oracle 10g ou 11g), compatible avec AWS DMS.

À partir de l'instance Oracle intermédiaire, le schéma et les données sont migrés vers la base de données PostgreSQL sur AWS à l'aide d'AWS Schema Conversion Tool (AWS SCT) et d'AWS DMS. Cette méthode permet de diffuser en continu les données de la base de données Oracle source vers l'instance de base de données PostgreSQL cible avec un délai de réplication minimal. Dans cette implémentation, le temps d'arrêt est limité au temps nécessaire pour créer ou valider l'ensemble des clés étrangères, des déclencheurs et des séquences sur la base de données PostgreSQL cible.

La migration utilise une instance Amazon Elastic Compute Cloud (Amazon EC2) sur laquelle Oracle 10g ou 11g est installé pour héberger les modifications depuis la base de données Oracle source. AWS DMS utilise cette instance Oracle intermédiaire comme source pour diffuser les données vers Amazon RDS for PostgreSQL ou Aurora PostgreSQL. La réplication des données peut être suspendue et reprise depuis la base de données Oracle locale vers l'instance Oracle intermédiaire. Il peut également être suspendu et repris depuis l'instance Oracle intermédiaire vers la base de données PostgreSQL cible afin que vous puissiez valider les données à l'aide de la validation des données AWS DMS ou d'un outil de validation de données personnalisé.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle 8i ou 9i source dans un centre de données sur site
- AWS Direct Connect configuré entre le centre de données sur site et AWS
- Pilotes de connectivité de base de données Java (JDBC) pour les connecteurs AWS SCT installés soit sur une machine locale, soit sur l'instance EC2 où AWS SCT est installé

- Connaissance de l'utilisation d'une base de données Oracle en tant que source AWS DMS
- Connaissance de l'utilisation d'une base de données PostgreSQL en tant que cible AWS DMS
- Connaissance de la réplication de SharePlex données Quest

Limites

- La limite de taille de base de données est de 64 To
- La base de données Oracle sur site doit être Enterprise Edition

Versions du produit

- Oracle 8i ou 9i pour la base de données source
- Oracle 10g ou 11g pour la base de données intermédiaire
- PostgreSQL 9.6 ou version ultérieure

Architecture

Pile technologique source

- Base de données Oracle 8i ou 9i
- Quête SharePlex

Pile technologique cible

- Amazon RDS pour PostgreSQL ou Aurora PostgreSQL

Architecture source et cible

Outils

- AWS DMS — AWS Database Migration Service (AWS DMS) vous aide à migrer des bases de données rapidement et en toute sécurité. La base de données source reste pleinement

opérationnelle pendant la migration, minimisant ainsi les interruptions de service pour les applications qui dépendent de la base de données. AWS DMS peut migrer vos données vers et depuis les bases de données commerciales et open source les plus utilisées.

- AWS SCT — AWS Schema Conversion Tool (AWS SCT) rend les migrations de bases de données hétérogènes prévisibles en convertissant automatiquement le schéma de base de données source et la majorité des objets du code de base de données, y compris les vues, les procédures stockées et les fonctions, dans un format compatible avec la base de données cible. Les objets qui ne peuvent pas être convertis automatiquement sont clairement marqués afin de pouvoir être convertis manuellement pour terminer la migration. AWS SCT peut également scanner le code source de votre application à la recherche d'instructions SQL intégrées et les convertir dans le cadre d'un projet de conversion de schéma de base de données. Au cours de ce processus, AWS SCT optimise le code natif du cloud en convertissant les anciennes fonctions Oracle et SQL Server en leurs équivalents AWS, afin de vous aider à moderniser vos applications lors de la migration de vos bases de données. Lorsque la conversion du schéma est terminée, AWS SCT peut aider à migrer les données de différents entrepôts de données vers Amazon Redshift en utilisant des agents de migration de données intégrés.
- Quest SharePlex — SharePlexQuest est un outil de réplication de Oracle-to-Oracle données permettant de déplacer des données avec un minimum de temps d'arrêt et sans perte de données.

Épopées

Créez l' EC2 instance et installez Oracle

Tâche	Description	Compétences requises
Configurez le réseau pour Amazon EC2.	Créez le cloud privé virtuel (VPC), les sous-réseaux, la passerelle Internet, les tables de routage et les groupes de sécurité.	AWS SysAdmin
Créez la nouvelle EC2 instance.	Sélectionnez l'Amazon Machine Image (AMI) pour l' EC2 instance. Choisissez la taille de l'instance et configure z les détails de l'instance : le nombre d'instances (1),	AWS SysAdmin

Tâche	Description	Compétences requises
	le VPC et le sous-réseau de l'étape précédente, l'attribution automatique d'une adresse IP publique et d'autres options. Ajoutez du stockage, configure z les groupes de sécurité et lancez l'instance. Lorsque vous y êtes invité, créez et enregistrez une paire de clés pour l'étape suivante.	
Installez Oracle sur l' EC2 instance.	Procurez-vous les licences et les fichiers binaires Oracle requis, puis installez Oracle 10g ou 11g sur l'instance. EC2	DBA

Installation SharePlex sur une EC2 instance et configuration de la réplication des données

Tâche	Description	Compétences requises
Configurez SharePlex.	Créez une EC2 instance Amazon et installez les SharePlex fichiers binaires compatibles avec Oracle 8i ou 9i.	AWS SysAdmin, ADMINISTR ATEUR DE BASE DE DONNÉES
Configurez la réplication des données.	Suivez les SharePlex meilleures pratiques pour configurer la réplication des données d'une base de données Oracle 8i/9i sur site vers une instance Oracle 10g/11g.	DBA

Convertir le schéma de base de données Oracle en PostgreSQL

Tâche	Description	Compétences requises
Configurez AWS SCT.	Créez un nouveau rapport, puis connectez-vous à Oracle en tant que source et à PostgreSQL en tant que cible. Dans les paramètres du projet, ouvrez l'onglet SQL Scripting et remplacez le script SQL cible par Multiple Files.	DBA
Convertissez le schéma de base de données Oracle.	Dans l'onglet Action, choisissez Générer le rapport, Convertir le schéma, puis Enregistrer en tant que SQL.	DBA
Modifiez les scripts SQL générés par AWS SCT.		DBA

Création et configuration de l'instance de base de données Amazon RDS

Tâche	Description	Compétences requises
Créez l'instance de base de données Amazon RDS.	Dans la console Amazon RDS, créez une nouvelle instance de base de données PostgreSQL.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES
Configurez l'instance de base de données.	Spécifiez la version du moteur de base de données, la classe d'instance de base de données, le déploiement multi-AZ, le type de stockage et le stockage alloué. Entrez l'identifiant de l'instance de	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES

Tâche	Description	Compétences requises
	base de données, un nom d'utilisateur principal et un mot de passe principal.	
Configurez le réseau et la sécurité.	Spécifiez le VPC, le groupe de sous-réseaux, l'accessibilité publique, la préférence de zone de disponibilité et les groupes de sécurité.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES
Configurez les options de base de données	Spécifiez le nom de la base de données, le port, le groupe de paramètres, le chiffrement et la clé principale.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES
Configurez des sauvegardes.	Spécifiez la période de conservation des sauvegardes, la fenêtre de sauvegarde, l'heure de début, la durée et indiquez s'il faut copier les balises dans les instantanés.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES
Configurez les options de surveillance.	Activez ou désactivez la surveillance améliorée et les informations sur les performances.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES
Configurez les options de maintenance.	Spécifiez la mise à niveau automatique de la version mineure, la fenêtre de maintenance, ainsi que le jour, l'heure et la durée de début.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES

Tâche	Description	Compétences requises
Exécutez les scripts de pré-migration depuis AWS SCT.	Sur l'instance Amazon RDS, exécutez les scripts suivants : create_database.sql, create_sequence.sql, create_table.sql, create_view.sql et create_function.sql.	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES

Migrer les données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication dans AWS DMS.	Renseignez les champs relatifs au nom, à la classe d'instance, au VPC (comme pour l' EC2 instance), au Multi-AZ et à l'accessibilité publique. Dans la section de configuration avancée, spécifiez le stockage alloué, le groupe de sous-réseaux, la zone de disponibilité, les groupes de sécurité VPC et la clé racine AWS Key Management Service (AWS KMS).	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES
Créez le point de terminaison de la base de données source.	Spécifiez le nom du point de terminaison, le type, le moteur source (Oracle), le nom du serveur (nom DNS EC2 privé Amazon), le port, le mode SSL, le nom d'utilisateur, le mot de passe, le SID, le VPC (spécifiez le VPC qui possède l'instance de réplication) et	AWS SysAdmin, ADMINISTRATEUR DE BASE DE DONNÉES

Tâche	Description	Compétences requises
	l'instance de réplication. Pour tester la connexion, choisisse z Run Test, puis créez le point de terminaison. Vous pouvez également configurer les paramètres avancés suivants : maxFileSize et numberDat aType Scale.	
Créez la tâche de réplication AWS DMS.	Spécifiez le nom de la tâche, l'instance de réplication, les points de terminaison source et cible, ainsi que l'instance de réplication. Pour le type de migration, choisissez « Migrer les données existantes et répliquer les modifications en cours ». Décochez la case « Démarrer la tâche lors de la création ».	AWS SysAdmin, ADMINISTR ATEUR DE BASE DE DONNÉES
Configurez les paramètres des tâches de réplication AWS DMS.	Pour le mode de préparation de la table cible, choisissez « Ne rien faire ». Arrêtez la tâche une fois le chargemen t complet terminé pour créer des clés primaires. Spécifiez le mode LOB limité ou complet et activez les tables de contrôle. Vous pouvez éventuellement configurer le paramètre CommitRate avancé.	DBA

Tâche	Description	Compétences requises
Configurez les mappages de tables.	Dans la section mappages de tables, créez une règle d'inclusion pour toutes les tables de tous les schémas inclus dans la migration, puis créez une règle d'exclusi on. Ajoutez trois règles de transformation pour convertir les noms de schéma, de table et de colonne en minuscule s, et ajoutez toutes les autres règles nécessaires à cette migration spécifique.	DBA
Lancez la tâche.	Lancez la tâche de réplicati on. Assurez-vous que le chargement complet est en cours. Exécutez ALTER SYSTEM SWITCH LOGFILE sur la base de données Oracle principale pour démarrer la tâche.	DBA
Exécutez les scripts de mi-migration depuis AWS SCT.	Dans Amazon RDS for PostgreSQL, exécutez les scripts suivants : create_in dex.sql et create_constraint. sql.	DBA

Tâche	Description	Compétences requises
Redémarrez la tâche pour poursuivre la capture des données de modification (CDC).	Dans l'instance de base de données Amazon RDS for PostgreSQL, exécutez VACUUM et redémarrez la tâche AWS DMS pour appliquer les modifications CDC mises en cache.	DBA

Passez à la base de données PostgreSQL

Tâche	Description	Compétences requises
Consultez les journaux et les tables de métadonnées AWS DMS.	Validez les erreurs et corrigez-les si nécessaire.	DBA
Arrêtez toutes les dépendances Oracle.	Arrêtez les écouteurs de la base de données Oracle et exécutez ALTER SYSTEM SWITCH LOGFILE. Arrêtez la tâche AWS DMS lorsqu'elle ne montre aucune activité.	DBA
Exécutez les scripts de post-migration depuis AWS SCT.	Dans Amazon RDS for PostgreSQL, exécutez les scripts suivants : create_foreign_key_constraint.sql et create_triggers.sql.	DBA
Effectuez toutes les étapes supplémentaires relatives à Amazon RDS for PostgreSQL.	Incrémentez les séquences pour qu'elles correspondent à Oracle si nécessaire, exécutez VACUUM et ANALYZE, puis	DBA

Tâche	Description	Compétences requises
	prenez un instantané pour vérifier la conformité.	
Ouvrez les connexions à Amazon RDS for PostgreSQL.	Supprimez les groupes de sécurité AWS DMS d'Amazon RDS for PostgreSQL, ajoutez des groupes de sécurité de production et dirigez vos applications vers la nouvelle base de données.	DBA
Nettoyez les ressources AWS DMS.	Supprimez les points de terminaison, les tâches de réplication, les instances de réplication et l' EC2 instance.	SysAdmin, DBA

Ressources connexes

- Documentation AWS DMS
- Documentation AWS SCT
- Tarification d'Amazon RDS for PostgreSQL
- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS
- SharePlex Documentation sur les quêtes

Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide de vues matérialisées et d'AWS DMS

Créée par Kumar Babu PG (AWS) et Pragnesh Patel (AWS)

Récapitulatif

Ce modèle décrit comment migrer une ancienne base de données Oracle 8i ou 9i sur site vers Amazon Relational Database Service (Amazon RDS) pour PostgreSQL ou Amazon Aurora PostgreSQL compatible Edition.

AWS Database Migration Service (AWS DMS) ne prend pas en charge Oracle 8i ou 9i en tant que source. Ce modèle utilise donc une instance de base de données Oracle intermédiaire compatible avec AWS DMS, telle qu'Oracle 10g ou 11g. Il utilise également la fonctionnalité de vues matérialisées pour migrer les données de l'instance Oracle 8i/9i source vers l'instance Oracle 10g/11g intermédiaire.

AWS Schema Conversion Tool (AWS SCT) convertit le schéma de base de données et AWS DMS migre les données vers la base de données PostgreSQL cible.

Ce modèle aide les utilisateurs qui souhaitent migrer à partir de bases de données Oracle existantes avec un temps d'arrêt minimal des bases de données. Dans cette implémentation, le temps d'arrêt serait limité au temps nécessaire pour créer ou valider toutes les clés étrangères, tous les déclencheurs et toutes les séquences sur la base de données cible.

Le modèle utilise des instances Amazon Elastic Compute Cloud (Amazon EC2) avec une base de données Oracle 10g/11g installée pour aider AWS DMS à diffuser les données. Vous pouvez suspendre temporairement la réplication en continu depuis la base de données Oracle sur site vers l'instance Oracle intermédiaire afin de permettre à AWS DMS de rattraper son retard en matière de validation des données ou d'utiliser un autre outil de validation des données. L'instance de base de données PostgreSQL et la base de données Oracle intermédiaire disposeront des mêmes données lorsque AWS DMS aura terminé la migration des modifications en cours.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle 8i ou 9i source dans un centre de données sur site

- AWS Direct Connect configuré entre le centre de données sur site et AWS
- Pilotes de connectivité de base de données Java (JDBC) pour les connecteurs AWS SCT installés soit sur une machine locale, soit sur l'instance EC2 où AWS SCT est installé
- Connaissance de l'utilisation d'une base de données Oracle en tant que source AWS DMS
- Connaissance de l'utilisation d'une base de données PostgreSQL en tant que cible AWS DMS

Limites

- La limite de taille de base de données est de 64 To

Versions du produit

- Oracle 8i ou 9i pour la base de données source
- Oracle 10g ou 11g pour la base de données intermédiaire
- PostgreSQL 10.17 ou version ultérieure

Architecture

Pile technologique source

- Base de données Oracle 8i ou 9i

Pile technologique cible

- Compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL

Architecture cible

Outils

- AWS DMS permet de migrer les bases de données rapidement et en toute sécurité. La base de données source reste pleinement opérationnelle pendant la migration, minimisant ainsi les interruptions de service pour les applications qui dépendent de la base de données. AWS DMS peut migrer vos données vers et depuis les bases de données commerciales et open source les plus utilisées.

- AWS SCT convertit automatiquement le schéma de base de données source et la majorité des objets du code de base de données, y compris les vues, les procédures stockées et les fonctions, dans un format compatible avec la base de données cible. Les objets qui ne peuvent pas être convertis automatiquement sont clairement marqués afin de pouvoir être convertis manuellement pour terminer la migration. AWS SCT peut également scanner le code source de votre application à la recherche d'instructions SQL intégrées et les convertir dans le cadre d'un projet de conversion de schéma de base de données. Au cours de ce processus, AWS SCT optimise le code natif du cloud en convertissant les anciennes fonctions Oracle et SQL Server en leurs équivalents AWS, afin de vous aider à moderniser vos applications lors de la migration de vos bases de données. Lorsque la conversion du schéma est terminée, AWS SCT peut aider à migrer les données de différents entrepôts de données vers Amazon Redshift en utilisant des agents de migration de données intégrés.

Bonnes pratiques

Pour connaître les meilleures pratiques relatives à l'actualisation des vues matérialisées, consultez la documentation Oracle suivante :

- Actualisation des vues matérialisées
- Actualisation rapide pour les vues matérialisées

Épopées

Installez Oracle sur une EC2 instance et créez des vues matérialisées

Tâche	Description	Compétences requises
Configurez le réseau pour l' EC2 instance.	Créez le cloud privé virtuel (VPC), les sous-réseaux, la passerelle Internet, les tables de routage et les groupes de sécurité.	AWS SysAdmin
Créez l' EC2 instance.	Sélectionnez l'Amazon Machine Image (AMI) pour l' EC2 instance. Choisissez la taille de l'instance et configure	AWS SysAdmin

Tâche	Description	Compétences requises
	z les détails de l'instance : le nombre d'instances (1), le VPC et le sous-réseau de l'étape précédente, l'attribution automatique d'une adresse IP publique et d'autres options. Ajoutez du stockage, configure z les groupes de sécurité et lancez l'instance. Lorsque vous y êtes invité, créez et enregistrez une paire de clés pour l'étape suivante.	
Installez Oracle sur l' EC2 instance.	Procurez-vous les licences et les fichiers binaires Oracle requis, puis installez Oracle 10g ou 11g sur l'instance. EC2	DBA
Configurez le réseau Oracle.	Modifiez ou ajoutez des entrées `listener.ora` pour vous connecter à la base de données source Oracle 8i/9i locale, puis créez les liens de base de données.	DBA
Créez des vues matérialisées.	Identifiez les objets de base de données à répliquer dans la base de données Oracle 8i/9i source, puis créez des vues matérialisées pour tous les objets à l'aide du lien de base de données.	DBA

Tâche	Description	Compétences requises
Déployez des scripts pour actualiser les vues matérialisées aux intervalles requis.	Développez et déployez des scripts pour actualiser les vues matérialisées aux intervalles requis sur l'instance Amazon EC2 Oracle 10g/11g. Utilisez l'option d'actualisation incrémentielle pour actualiser les vues matérialisées.	DBA

Convertir le schéma de base de données Oracle en PostgreSQL

Tâche	Description	Compétences requises
Configurez AWS SCT.	Créez un nouveau rapport, puis connectez-vous à Oracle en tant que source et à PostgreSQL en tant que cible. Dans les paramètres du projet, ouvrez l'onglet SQL Scripting. Modifiez le script SQL cible en plusieurs fichiers. (AWS SCT ne prend pas en charge les bases de données Oracle 8i/9i. Vous devez donc restaurer le dump basé uniquement sur le schéma sur l'instance Oracle 10g/11g intermédiaire et l'utiliser comme source pour AWS SCT.)	DBA
Convertissez le schéma de base de données Oracle.	Dans l'onglet Action, choisissez Générer le rapport, Convertir	DBA

Tâche	Description	Compétences requises
	le schéma, puis Enregistrer en tant que SQL.	
Modifiez les scripts SQL.	Apportez des modifications conformément aux meilleure s pratiques. Par exemple, passez aux types de données appropriés et développez des équivalents PostgreSQL pour les fonctions spécifiques à Oracle.	DBA, DevDBA

Création et configuration de l'instance de base de données Amazon RDS pour héberger la base de données convertie

Tâche	Description	Compétences requises
Créez l'instance de base de données Amazon RDS.	Dans la console Amazon RDS, créez une nouvelle instance de base de données PostgreSQL.	AWS SysAdmin, DBA
Configurez l'instance de base de données.	Spécifiez la version du moteur de base de données, la classe d'instance de base de données, le déploiement multi-AZ, le type de stockage et le stockage alloué. Entrez l'identifiant de l'instance de base de données, un nom d'utilisateur principal et un mot de passe principal.	AWS SysAdmin, DBA
Configurez le réseau et la sécurité.	Spécifiez le VPC, le groupe de sous-réseaux, l'accessi	DBA, SysAdmin

Tâche	Description	Compétences requises
	bilité publique, la préférence de zone de disponibilité et les groupes de sécurité.	
Configurer les options de base de données.	Spécifiez le nom de la base de données, le port, le groupe de paramètres, le chiffrement et la clé principale.	ADMINISTRATEUR DE BASES DE DONNÉES, AWS SysAdmin
Configurez des sauvegardes.	Spécifiez la période de conservation des sauvegard es, la fenêtre de sauvegard e, l'heure de début, la durée et indiquez s'il faut copier les balises dans les instantanés.	AWS SysAdmin, DBA
Configurez les options de surveillance.	Activez ou désactivez la surveillance améliorée et les informations sur les performan ces.	AWS SysAdmin, DBA
Configurez les options de maintenance.	Spécifiez la mise à niveau automatique de la version mineure, la fenêtre de maintenance, ainsi que le jour, l'heure et la durée de début.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Exécutez les scripts de pré-migration depuis AWS SCT.	Sur l'instance Amazon RDS for PostgreSQL cible, créez le schéma de base de données en utilisant les scripts SQL d'AWS SCT avec d'autres modifications. Cela peut inclure l'exécution de plusieurs scripts, notamment la création d'utilisateurs, la création de bases de données, la création de schémas, de tables, de vues, de fonctions et d'autres objets de code.	AWS SysAdmin, DBA

Migrer les données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication dans AWS DMS.	Renseignez les champs relatifs au nom, à la classe d'instance, au VPC (comme pour l' EC2 instance), au Multi-AZ et à l'accessibilité publique. Dans la section de configura tion avancée, spécifiez le stockage alloué, le groupe de sous-réseaux, la zone de disponibilité, les groupes de sécurité VPC et la clé AWS Key Management Service (AWS KMS).	AWS SysAdmin, DBA
Créez le point de terminaison de la base de données source.	Spécifiez le nom du point de terminaison, le type, le moteur	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
	source (Oracle), le nom du serveur (nom DNS privé de l' EC2 instance), le port, le mode SSL, le nom d'utilisateur, le mot de passe, le SID, le VPC (spécifiez le VPC qui possède l'instance de réplication) et l'instance de réplication. Pour tester la connexion, choisissez Run Test, puis créez le point de terminaison. Vous pouvez également configurer les paramètres avancés suivants : maxFileSizeet numberDataTypeScale.	
Connectez AWS DMS à Amazon RDS pour PostgreSQL.	Créez un groupe de sécurité de migration pour les connexions entre celles-ci VPCs, si votre base de données PostgreSQL se trouve dans un autre VPC.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Créez le point de terminaison de base de données cible.	Spécifiez le nom du point de terminaison, le type, le moteur source (PostgreSQL), le nom du serveur (point de terminaison Amazon RDS), le port, le mode SSL, le nom d'utilisateur, le mot de passe, le nom de la base de données, le VPC (spécifiez le VPC qui possède l'instance de réplication) et l'instance de réplication. Pour tester la connexion, choisissez Run Test, puis créez le point de terminaison. Vous pouvez également configurer les paramètres avancés suivants : maxFileSizeet numberDataTypeScale.	AWS SysAdmin, DBA
Créez la tâche de réplication AWS DMS.	Spécifiez le nom de la tâche, l'instance de réplication, les points de terminaison source et cible, ainsi que l'instance de réplication. Pour le type de migration, choisissez Migrer les données existantes et répliquer les modifications en cours. Désactivez la case à cocher Démarrer la tâche lors de la création.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Configurez les paramètres des tâches de réplication AWS DMS.	Pour le mode de préparation de la table cible, choisissez Ne rien faire. Arrêtez la tâche une fois le chargement complet terminé (pour créer des clés primaires). Spécifiez le mode LOB limité ou complet et activez les tables de contrôle. Vous pouvez éventuellement configurer le paramètre CommitRateavancé.	DBA
Configurez les mappages de tables.	Dans la section Mappages de tables, créez une règle d'inclusion pour toutes les tables de tous les schémas inclus dans la migration, puis créez une règle d'exclusi on. Ajoutez trois règles de transformation pour convertir les noms de schéma, de table et de colonne en minuscule s, et ajoutez toutes les autres règles dont vous avez besoin pour cette migration spécifiqu e.	DBA
Lancez la tâche.	Lancez la tâche de réplicati on. Assurez-vous que le chargement complet est en cours. Exécutez `ALTER SYSTEM SWITCH LOGFILE` sur la base de données Oracle principale pour démarrer la tâche.	DBA

Tâche	Description	Compétences requises
Exécutez les scripts de mi-migration depuis AWS SCT.	Dans Amazon RDS for PostgreSQL, exécutez les `create_index.sql` scripts suivants `create_constraint.sql` : et (si le schéma complet n'a pas été créé initialement).	DBA
Reprenez la tâche pour continuer la saisie des données de modification (CDC).	Exécutez `VACUUM` sur l'instance de base de données Amazon RDS for PostgreSQL et redémarrez la tâche AWS DMS pour appliquer les modifications CDC mises en cache.	DBA

Passez à la base de données PostgreSQL

Tâche	Description	Compétences requises
Consultez les journaux et les tables de validation d'AWS DMS.	Vérifiez et corrigez les erreurs de réplication ou de validation.	DBA
Arrêtez d'utiliser la base de données Oracle locale et ses dépendances.	Arrêtez toutes les dépendances Oracle, arrêtez les écouteurs de la base de données Oracle et exécutez`ALTER SYSTEM SWITCH LOGFILE`. Arrêtez la tâche AWS DMS lorsqu'elle ne montre aucune activité.	DBA
Exécutez les scripts de post-migration depuis AWS SCT.	Dans Amazon RDS for PostgreSQL, exécutez les	DBA

Tâche	Description	Compétences requises
	scripts suivants :. `create_foreign_key_constraint.sql and create_triggers.sql` Assurez-vous que les séquences sont à jour.	
Effectuez les étapes supplémentaires relatives à Amazon RDS for PostgreSQL.	Incrémentez les séquences pour qu'elles correspondent à Oracle si nécessaire, `ANALYZE` exécutez-les `VACUUM` et prenez un instantané pour garantir la conformité.	DBA
Ouvrez les connexions à Amazon RDS for PostgreSQL.	Supprimez les groupes de sécurité AWS DMS d'Amazon RDS for PostgreSQL, ajoutez des groupes de sécurité de production et dirigez vos applications vers la nouvelle base de données.	DBA
Nettoyez les objets AWS DMS.	Supprimez les points de terminaison, les tâches de réplication, les instances de réplication et l' EC2 instance.	SysAdmin, DBA

Ressources connexes

- Documentation AWS DMS
- Documentation AWS SCT
- Tarification d'Amazon RDS for PostgreSQL
- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS

Migrez d'Oracle sur Amazon EC2 vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT

Créée par Anil Kunapareddy (AWS) et Harshad Gohil

Récapitulatif

La gestion des bases de données Oracle sur les instances Amazon Elastic Compute Cloud (Amazon EC2) nécessite des ressources et peut s'avérer coûteuse. Le déplacement de ces bases de données vers une instance de base de données Amazon Relational Database Service (Amazon RDS) pour MySQL vous facilitera la tâche en optimisant le budget informatique global. Amazon RDS for MySQL propose également des fonctionnalités telles que le multi-AZ, l'évolutivité et les sauvegardes automatiques.

Ce modèle vous guide tout au long de la migration d'une base de données Oracle source sur Amazon EC2 vers une instance de base de données Amazon RDS for MySQL cible. Il utilise AWS Database Migration Service (AWS DMS) pour migrer les données, et AWS Schema Conversion Tool (AWS SCT) pour convertir le schéma et les objets de la base de données source dans un format compatible avec Amazon RDS for MySQL.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source avec des services d'instance et d'écoute exécutés, en mode ARCHIVELOG
- Une base de données Amazon RDS for MySQL cible, dotée d'un espace de stockage suffisant pour la migration des données

Limites

- AWS DMS ne crée pas de schéma sur la base de données cible ; c'est ce que vous devez faire. Le nom du schéma doit déjà exister pour la cible. Les tables du schéma source sont importées dans user/schema, qu'AWS DMS utilise pour se connecter à l'instance cible. Vous devez créer plusieurs tâches de réplication si vous avez plusieurs schémas à migrer.

Versions du produit

- Toutes les éditions de base de données Oracle pour les versions 10.2 et ultérieures, 11g et versions ultérieures, 12.2 et 18c. Pour obtenir la dernière liste des versions prises en charge, consultez les sections Utilisation d'une base de données Oracle comme source pour AWS DMS et Utilisation d'une base de données compatible MySQL comme cible pour AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités. Pour plus d'informations sur les versions de base de données Oracle prises en charge par AWS SCT, consultez la documentation AWS SCT.
- AWS DMS prend en charge les versions 5.5, 5.6 et 5.7 de MySQL.

Architecture

Pile technologique source

- Une base de données Oracle sur une EC2 instance

Pile technologique cible

- Instance de base de données Amazon RDS pour MySQL

Architecture de migration des données

Architecture source et cible

Outils

- AWS DMS - AWS Database Migration Service (AWS DMS) est un service Web que vous pouvez utiliser pour migrer les données de votre base de données sur site, sur une instance de base de données Amazon RDS ou d'une base de données sur une EC2 instance, vers une base de données sur un service AWS tel qu'Amazon RDS for MySQL ou une instance. EC2 Vous pouvez également migrer une base de données d'un service AWS vers une base de données sur site. Vous pouvez migrer des données entre des moteurs de base de données hétérogènes ou homogènes.
- AWS SCT - AWS Schema Conversion Tool (AWS SCT) rend les migrations de bases de données hétérogènes prévisibles en convertissant automatiquement le schéma de base de données source et la majorité des objets du code de base de données, y compris les vues, les procédures stockées

et les fonctions, dans un format compatible avec la base de données cible. Après avoir converti le schéma de votre base de données et les objets de code à l'aide d'AWS SCT, vous pouvez utiliser AWS DMS pour migrer les données de la base de données source vers la base de données cible afin de terminer vos projets de migration.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Identifiez les versions et les moteurs de base de données source et cible.		DBA/Développeur
Identifiez l'instance de réplication DMS.		DBA/Développeur
Identifiez les exigences de stockage telles que le type et la capacité de stockage.		DBA/Développeur
Identifiez les exigences du réseau telles que la latence et la bande passante.		DBA/Développeur
Identifiez les exigences matérielles pour les instances du serveur source et cible (sur la base de la liste de compatibilité Oracle et des exigences de capacité).		DBA/Développeur
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA/Développeur

Tâche	Description	Compétences requises
Installez les pilotes AWS SCT et Oracle.		DBA/Développeur
Déterminez une stratégie de sauvegarde.		DBA/Développeur
Déterminez les exigences de disponibilité.		DBA/Développeur
Identifiez la stratégie de migration et de transition des applications.		DBA/Développeur
Sélectionnez le type d'instance de base de données approprié en fonction de la capacité, du stockage et des fonctionnalités réseau.		DBA/Développeur

Configuration de l'environnement

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC) La source, la cible et l'instance de réplication doivent se trouver dans le même VPC. Il est également bon de les avoir dans la même zone de disponibilité.		Developer
Créez les groupes de sécurité nécessaires pour accéder à la base de données.		Developer

Tâche	Description	Compétences requises
Générez et configurez une paire de clés.		Developer
Configurez les sous-réseaux, les zones de disponibilité et les blocs CIDR.		Developer

Configurer la source : base de données Oracle sur EC2 instance

Tâche	Description	Compétences requises
Installez Oracle Database sur Amazon EC2 avec les utilisateurs et les rôles requis.		DBA
Effectuez les trois étapes de la colonne suivante pour accéder à Oracle depuis l'extérieur de l' EC2 instance.	1. Remplacez l'hôte local par le DNS EC2 public Amazon. `tnsnames` 2. Remplacez l'hôte local par le DNS EC2 public Amazon. `listener` 3. Arrêtez et redémarrez l'écouteur.	DBA
Lorsque Amazon EC2 est redémarré, le DNS public change. Assurez-vous de mettre à jour le DNS EC2 public d'Amazon dans « tnsnames » et « listener » ou d'utiliser une adresse IP élastique.		DBA/Développeur
Configurez le groupe de sécurité de l' EC2 instance afin		DBA/Développeur

Tâche	Description	Compétences requises
que l'instance de réplication et les clients requis puissent accéder à la base de données source.		

Configuration de la cible : Amazon RDS for MySQL

Tâche	Description	Compétences requises
Configurez et démarrez l'instance de base de données Amazon RDS for MySQL.		Developer
Créez le tablespace nécessaire dans l'instance de base de données Amazon RDS for MySQL.		DBA
Configurez le groupe de sécurité afin que l'instance de réplication et les clients requis puissent accéder à la base de données cible.		Developer

Configurer AWS SCT et créer un schéma dans la base de données cible

Tâche	Description	Compétences requises
Installez les pilotes AWS SCT et Oracle.		Developer
Entrez les paramètres appropriés et connectez-vous à la source et à la cible.		Developer

Tâche	Description	Compétences requises
Générez un rapport de conversion de schéma.		Developer
Corrigez le code et le schéma selon les besoins, en particuli er les tablespaces et les guillemets, et exécutez-les sur la base de données cible.		Developer
Validez le schéma sur la source par rapport à la cible avant de migrer les données.		Developer

Migrer des données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Pour le chargement complet et la capture des données (CDC) ou uniquement pour le CDC, vous devez définir un attribut de connexion supplémentaire.		Developer
L'utilisateur spécifié dans les définitions de la base de données Oracle source AWS DMS doit disposer de tous les privilèges requis. Pour une liste complète, voir https://docs.aws.amazon.com /dms/ latest/userguide/C HAP _source.oracle.html #CHAP_Source .Oracle.Self-Managed.		DBA/Développeur

Tâche	Description	Compétences requises
Activez la journalisation supplémentaire dans la base de données source.		DBA/Développeur
Pour le chargement complet et la capture des données (CDC) ou simplement pour le CDC, activez le mode ARCHIVELOG dans la base de données source.		DBA
Créez des points de terminaison source et cible et testez les connexions.		Developer
Lorsque les points de terminaison sont correctement connectés, créez une tâche de réplication.		Developer
Sélectionnez CDC uniquement (ou) pleine charge plus CDC dans la tâche pour capturer les modifications pour une réplication continue uniquement (ou) charge complète plus modifications en cours, respectivement.		Developer
Exécutez la tâche de réplication et surveillez CloudWatch les journaux Amazon.		Developer
Validez les données dans les bases de données source et cible.		Developer

Migrez votre application et réduisez les dépenses

Tâche	Description	Compétences requises
Suivez les étapes de votre stratégie de migration d'applications.		DBA, développeur, propriétaire de l'application
Suivez les étapes de votre stratégie de transfert et de transition d'applications.		DBA, développeur, propriétaire de l'application

Fermez le projet

Tâche	Description	Compétences requises
Validez le schéma et les données dans les bases de données source par rapport aux bases de données cibles.		DBA/Développeur
Collectez des indicateurs concernant le délai de migration, le pourcentage de manuel par rapport à l'outil, les économies de coûts, etc.		DBA/Developer/AppOwner
Passez en revue les documents et les artefacts du projet.		DBA/Developer/AppOwner
Arrêtez les ressources AWS temporaires.		DBA/Développeur
Clôturez le projet et faites part de vos commentaires.		DBA/Developer/AppOwner

Ressources connexes

- Documentation AWS DMS
- Site Web AWS DMS
- Articles de blog AWS DMS
- Stratégies de migration d'une base de données Oracle vers AWS
- Amazon RDS for Oracle FAQs
- FAQ sur Oracle
- Amazon EC2
- Amazon EC2 FAQs
- Octroi de licences aux logiciels Oracle dans un environnement de cloud computing

Migrer d'Oracle vers Amazon DocumentDB à l'aide d'AWS DMS

Créée par Sashikanta Pattanayak (AWS) et Munesh Siddappa (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données Oracle vers une base de données Amazon DocumentDB (compatible avec MongoDB) à l'aide d'AWS Database Migration Service (AWS DMS). Cette approche peut être appliquée à une base de données source Oracle sur site ainsi qu'à une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle. Ce modèle utilise une instance de source de base de données Oracle Amazon RDS comme exemple.

Amazon DocumentDB (compatible avec MongoDB) est un service de base de données de documents entièrement géré et compatible avec MongoDB qui facilite le stockage, l'interrogation et l'indexation des données JSON.

Le cas d'utilisation de ce modèle est la one-to-one réplication d'une table de base de données Oracle vers une collection Amazon DocumentDB. Le modèle utilise les tâches de réplication AWS DMS pour lire la structure des tables de la base de données Oracle, créer la collection correspondante dans Amazon DocumentDB et effectuer une migration à chargement complet. Vous pouvez consulter et interroger vos données dans Amazon DocumentDB, comme vous le feriez dans MongoDB.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Connaissance de l'utilisation des bases de données Oracle
- Connaissance de l'utilisation d'Amazon DocumentDB
- Pour l'utilisateur Oracle, `SELECT ANY TABLE` privilège
- Pour l'utilisation d'Amazon DocumentDB, le privilège requis pour transférer des données

Limites

Les limites suivantes s'appliquent lors de l'utilisation d'Amazon DocumentDB comme cible pour AWS DMS :

- Dans Amazon DocumentDB, les noms de collection ne peuvent pas contenir le symbole du dollar ($). En outre, les noms de base de données ne peuvent pas contenir de caractères Unicode.
- AWS DMS ne prend pas en charge la fusion de plusieurs tables sources en une seule collection Amazon DocumentDB.
- Lorsqu'AWS DMS traite des modifications provenant d'une table source qui ne possède pas de clé primaire, toutes les grandes colonnes d'objets binaires (LOB) de cette table sont ignorées.
- Si l'option Modifier la table est activée et qu'AWS DMS rencontre une colonne source nommée « _id », cette colonne apparaît sous la forme « __id » (deux traits de soulignement) dans la table des modifications.
- Si vous choisissez Oracle comme point de terminaison source, la journalisation supplémentaire complète de la source Oracle doit être activée. Sinon, si certaines colonnes de la source n'ont pas été modifiées, les données sont chargées dans Amazon DocumentDB sous forme de valeurs nulles.

Versions du produit

- Amazon RDS pour Oracle version 11.2.0.3 ou ultérieure
- AWS DMS version 3.1.3 ou ultérieure (pour obtenir les informations les plus récentes sur la version, consultez la section Utilisation d'Amazon DocumentDB comme cible pour AWS DMS dans la documentation AWS DMS)

Architecture

Pile technologique source

- Instance de base de données Amazon RDS pour Oracle

Pile technologique cible

- Amazon DocumentDB

Architecture source et cible

Outils

- AWS DMS — AWS Database Migration Service (AWS DMS) est un service Web que vous pouvez utiliser pour migrer des données d'un magasin de données source vers un magasin de données cible. Le guide de l'utilisateur d'AWS DMS indique les versions et éditions de la base de données source Oracle prises en charge pour une utilisation avec AWS DMS. Pour plus d'informations relatives à ce modèle, consultez la section Utilisation d'Amazon DocumentDB comme cible pour AWS DMS.
- Amazon EC2 — Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Votre cluster Amazon DocumentDB doit être exécuté dans votre cloud privé virtuel (VPC) par défaut. Pour interagir avec votre cluster Amazon DocumentDB, vous devez lancer une EC2 instance dans votre VPC par défaut, dans la même région AWS où vous avez créé votre cluster Amazon DocumentDB. Pour plus de détails, consultez la section Lancer une EC2 instance Amazon dans la documentation Amazon DocumentDB.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions et les moteurs de base de données source et cible.		Administrateur AWS
Choisissez le type d'instance approprié (capacité, fonctionnalités de stockage, fonctionnalités réseau).		Administrateur AWS
Identifiez les exigences de sécurité d'accès au réseau/hôte pour les bases de données source et cible.		Administrateur AWS

Tâche	Description	Compétences requises
Créez un groupe de sécurité sortant pour les bases de données source et cible.		Administrateur AWS
Créez et configurez une EC2 instance pour Amazon DocumentDB.		Administrateur AWS

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un VPC et des sous-réseaux.		Administrateur AWS
Créez des groupes de sécurité et des listes de contrôle d'accès au réseau (ACLs).		Administrateur AWS
Configurez et démarrez l'instance Amazon RDS for Oracle source.		Administrateur AWS
Configurez et démarrez l'instance Amazon DocumentDB.		Administrateur AWS

Préparation de la base de données source

Tâche	Description	Compétences requises
Vérifiez que la base de données Oracle peut être		Administrateur AWS

Tâche	Description	Compétences requises
connectée à l'aide des informations de connexion.		
Vérifiez que l'utilisateur Oracle possède le privilège SELECT ANY TABLE.		Administrateur AWS

Préparation de la base de données cible

Tâche	Description	Compétences requises
Créez le cluster Amazon DocumentDB en choisissant la classe d'instance et le nombre d'instances appropriés.		Administrateur AWS

Configuration d'Amazon EC2

Tâche	Description	Compétences requises
Configurez l' EC2 instance.	Pour interagir avec votre cluster Amazon DocumentDB, vous devez lancer une EC2 instance dans votre VPC par défaut, dans la même région AWS où vous avez créé votre cluster Amazon DocumentDB. Configurez la région AWS VPCs, les zones de disponibilité et les sous-réseaux de l' EC2 instance.	Administrateur AWS
Configurez la paire de clés.	Une paire de clés publique/privée vous permet de vous	Administrateur AWS

Tâche	Description	Compétences requises
	connecter en toute sécurité à l' EC2 instance après son lancement.	
Définissez les plages CIDR de l'hôte bastion (facultatif).	Définissez la plage d'adresses IP CIDR autorisée pour l'accès Secure Shell (SSH) externe aux instances hôtes Bastion.	Administrateur AWS

Migrer les données — chargement complet

Tâche	Description	Compétences requises
Créez une instance de réplication AWS DMS.		Administrateur AWS
Créez des points de terminaison source et cible.		Administrateur AWS
Créez des tâches de réplication AWS DMS pour un chargement complet.		Administrateur AWS

Testez la migration

Tâche	Description	Compétences requises
Connectez-vous au cluster Amazon DocumentDB via l' EC2 instance.		Administrateur AWS
Connectez-vous au cluster à l'aide du shell mongo.	Pour obtenir des instructions, consultez les liens Amazon DocumentDB dans la section Références et aide.	Administrateur AWS

Tâche	Description	Compétences requises
Vérifiez les résultats de la migration.		Administrateur AWS

Ressources connexes

- Comment fonctionne AWS DMS
- Migration vers Amazon DocumentDB
- Utilisation d'Amazon DocumentDB comme cible pour AWS DMS
- Présentation d'Amazon DocumentDB
- Accédez à votre cluster Amazon DocumentDB et utilisez-le à l'aide du shell mongo
- Migrer de MongoDB vers Amazon DocumentDB à l'aide de la méthode hors ligne (article de blog)
- Comment utiliser Amazon DocumentDB (compatible avec MongoDB) pour créer et gérer des applications à grande échelle (article de blog)

Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for MariaDB à l'aide d'AWS DMS et d'AWS SCT

Créée par Veeranjaneyulu Grandhi (AWS) et Vinod Kumar (AWS)

Récapitulatif

Ce modèle explique les étapes de migration d'une base de données Oracle sur une instance Amazon Elastic Compute Cloud (Amazon EC2) vers une instance de base de données Amazon Relational Database Service (Amazon RDS) pour MariaDB. Le modèle utilise AWS Data Migration Service (AWS DMS) pour la migration des données et AWS Schema Conversion Tool (AWS SCT) pour la conversion de schéma.

La gestion des bases de données Oracle sur des EC2 instances nécessite davantage de ressources et est plus coûteuse que l'utilisation d'une base de données sur Amazon RDS. Amazon RDS facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud. Amazon RDS fournit une capacité rentable et redimensionnable tout en automatisant les tâches d'administration fastidieuses telles que le provisionnement du matériel, la configuration de bases de données, l'application de correctifs et les sauvegardes.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une base de données Oracle source avec des services d'instance et d'écoute opérationnels. Cette base de données doit être en mode ARCHIVELOG.
- Connaissance de l'utilisation d'une base de données Oracle comme source pour AWS DMS.
- Connaissance de l'utilisation d'Oracle comme source pour AWS SCT.

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- Toutes les éditions de base de données Oracle pour les versions 10.2 et ultérieures, 11g et versions ultérieures, 12.2 et 18c. Pour obtenir la dernière liste des versions prises en charge,

consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS et le tableau des versions d'AWS SCT dans la documentation AWS.

- Amazon RDS prend en charge les versions 10.3, 10.4, 10.5 et 10.6 du serveur communautaire MariaDB Server. Pour obtenir la dernière liste des versions prises en charge, consultez la documentation Amazon RDS.

Architecture

Pile technologique source

- Une base de données Oracle sur une EC2 instance

Pile technologique cible

- Amazon RDS for MariaDB

Architecture de migration des données

Architecture cible

Outils

- AWS Schema Conversion Tool (AWS SCT) rend les migrations de bases de données hétérogènes prévisibles en convertissant automatiquement le schéma de base de données source et la majorité des objets du code de base de données (y compris les vues, les procédures stockées et les fonctions) dans un format compatible avec la base de données cible. Après avoir converti le schéma de votre base de données et les objets de code à l'aide d'AWS SCT, vous pouvez utiliser AWS DMS pour migrer les données de la base de données source vers la base de données cible afin de terminer vos projets de migration. Pour plus d'informations, consultez la section Utilisation d'Oracle comme source pour AWS SCT dans la documentation AWS SCT.
- AWS Database Migration Service (AWS DMS) vous aide à migrer des bases de données vers AWS rapidement et en toute sécurité. La base de données source reste pleinement opérationnelle pendant la migration, minimisant ainsi les interruptions de service pour les applications qui dépendent de la base de données. AWS DMS peut migrer vos données vers et depuis les bases de données commerciales et open source les plus utilisées. AWS DMS prend en charge les

migrations homogènes telles qu'Oracle vers Oracle, ainsi que les migrations hétérogènes entre différentes plateformes de base de données, telles qu'Oracle ou Microsoft SQL Server vers Amazon Aurora. Pour en savoir plus sur la migration des bases de données Oracle, consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS dans la documentation AWS DMS.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Identifiez les versions et les moteurs de base de données.	Identifiez les versions et les moteurs de base de données source et cible.	DBA, Développeur
Identifiez l'instance de réplicati on.	Identifiez l'instance de réplicati on AWS DMS.	DBA, Développeur
Identifiez les besoins en matière de stockage.	Identifiez le type et la capacité de stockage.	DBA, Développeur
Identifiez les exigences du réseau.	Identifiez la latence et la bande passante du réseau.	DBA, Développeur
Identifiez les exigences matérielles.	Identifiez les exigences matérielles pour les instances du serveur source et cible (sur la base de la liste de compatibi lité Oracle et des exigences de capacité).	DBA, Développeur
Identifiez les exigences en matière de sécurité.	Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.	DBA, Développeur

Tâche	Description	Compétences requises
Installez les pilotes.	Installez les derniers pilotes AWS SCT et Oracle.	DBA, Développeur
Déterminez une stratégie de sauvegarde.		DBA, Développeur
Déterminez les exigences de disponibilité.		DBA, Développeur
Choisissez une stratégie de migration/transition d'applications.		DBA, Développeur
Sélectionnez le type d'instance .	Sélectionnez le type d'instance approprié en fonction de la capacité, du stockage et des fonctionnalités réseau.	DBA, Développeur

Configuration de l'environnement

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)	Les instances source, cible et de réplication doivent se trouver dans le même VPC et dans la même zone de disponibilité (recommandé).	Developer
Créez des groupes de sécurité.	Créez les groupes de sécurité nécessaires pour accéder à la base de données.	Developer
Générez une paire de clés.	Générez et configurez une paire de clés.	Developer

Tâche	Description	Compétences requises
Configurez d'autres ressources.	Configurez les sous-réseaux, les zones de disponibilité et les blocs CIDR.	Developer

Configuration de la source

Tâche	Description	Compétences requises
Lancez l' EC2 instance.	Pour obtenir des instructions, consultez la EC2 documentation Amazon.	Developer
Installez la base de données Oracle.	Installez la base de données Oracle sur l' EC2 instance, avec les utilisateurs et les rôles requis.	DBA
Suivez les étapes décrites dans la description de la tâche pour accéder à Oracle depuis l'extérieur de l' EC2 instance.	1. Remplacez l'hôte local par le DNS EC2 public Amazon. `tnsnames` 2. Remplacez l'hôte local par le DNS EC2 public Amazon. `listener` 3. Arrêtez et redémarrez l'écouteur.	DBA
Mettez à jour le DNS EC2 public d'Amazon.	Après le redémarrage de l' EC2 instance, le DNS public change. Assurez-vous de mettre à jour le DNS EC2 public `tnsnames` d'Amazon dans `listener` et/ou d'utiliser une adresse IP élastique.	DBA, Développeur

Tâche	Description	Compétences requises
Configurez le groupe de sécurité de l' EC2 instance.	Configurez le groupe de sécurité de l' EC2 instance afin que l'instance de réplication et les clients requis puissent accéder à la base de données source.	DBA, Développeur

Configuration de l'environnement Amazon RDS pour MariaDB cible

Tâche	Description	Compétences requises
Démarrez l'instance de base de données RDS.	Configurez et démarrez l'instance de base de données Amazon RDS for MariaDB.	Developer
Créez des tablespaces.	Créez tous les espaces de table nécessaires dans la base de données Amazon RDS MariaDB.	DBA
Configurez un groupe de sécurité.	Configurez un groupe de sécurité afin que l'instance de réplication et les clients requis puissent accéder à la base de données cible.	Developer

Configuration d'AWS SCT

Tâche	Description	Compétences requises
Installez les pilotes.	Installez les derniers pilotes AWS SCT et Oracle.	Developer

Tâche	Description	Compétences requises
Connexion.	Entrez les paramètres appropriés, puis connectez-vous à la source et à la cible.	Developer
Générez un rapport de conversion de schéma.	Générez un rapport de conversion du schéma AWS SCT.	Developer
Corrigez le code et le schéma si nécessaire.	Apportez les corrections nécessaires au code et au schéma (en particulier aux tablespaces et aux guillemets).	DBA, Développeur
Validez le schéma.	Validez le schéma sur la source par rapport à la cible avant de charger les données.	Developer

Migrer des données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Définissez un attribut de connexion.	Pour le chargement complet et la capture des données modifiées (CDC) ou simplement pour le CDC, définissez un attribut de connexion supplémentaire. Pour plus d'informations, consultez la documentation Amazon RDS.	Developer
Activez la journalisation supplémentaire.	Activez la journalisation supplémentaire sur la base de données source.	DBA, Développeur

Tâche	Description	Compétences requises
Activez le mode journal d'archivage.	Pour le chargement complet et le CDC (ou simplement pour le CDC), activez le mode journal d'archivage sur la base de données source.	DBA
Créez et testez des points de terminaison.	Créez des points de terminaison source et cible et testez les connexions. Pour plus d'informations, consultez la documentation Amazon DMS.	Developer
Créez une tâche de réplication.	Lorsque les points de terminaison sont correctement connectés, créez une tâche de réplication. Pour plus d'informations, consultez la documentation Amazon DMS.	Developer
Choisissez le type de réplication.	Choisissez CDC uniquement ou Chargement complet plus CDC dans la tâche pour capturer les modifications pour la réplication continue uniquement, ou pour le chargement complet et les modifications en cours, respectivement.	Developer
Démarrez et surveillez la tâche.	Lancez la tâche de réplication et surveillez CloudWatch les journaux Amazon. Pour plus d'informations, consultez la documentation Amazon DMS.	Developer

Tâche	Description	Compétences requises
Validez les données.	Validez les données dans les bases de données source et cible.	Developer

Migrez les applications et passez à la base de données cible

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications choisie.		DBA, propriétaire de l'application, développeur
Suivez la stratégie de découpe/commutation d'applications choisie.		DBA, propriétaire de l'application, développeur

Fermez le projet

Tâche	Description	Compétences requises
Validez le schéma et les données.	Assurez-vous que le schéma et les données sont validés avec succès dans la source par rapport à la cible avant la clôture du projet.	DBA, Développeur
Collectez des statistiques.	Collectez des indicateurs concernant le temps de migration, le pourcentage de tâches manuelles par rapport aux tâches liées aux outils, les économies de coûts et des critères similaires.	DBA, propriétaire de l'application, développeur

Tâche	Description	Compétences requises
Consultez la documentation.	Passez en revue les documents et les artefacts du projet.	DBA, propriétaire de l'application, développeur
Arrêtez les ressources.	Arrêtez les ressources AWS temporaires.	DBA, Développeur
Fermez le projet.	Clôturez le projet de migration et faites part de vos commentaires.	DBA, propriétaire de l'application, développeur

Ressources connexes

- Présentation de MariaDB Amazon RDS
- Détails du produit Amazon RDS for MariaDB
- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Stratégies de migration des bases de données Oracle vers AWS
- Octroi de licences aux logiciels Oracle dans un environnement de cloud computing
- Amazon RDS for Oracle FAQs
- Présentation d'AWS DMS
- Articles de blog AWS DMS
- EC2 Présentation d'Amazon
- Amazon EC2 FAQs
- Documentation AWS SCT

Migrer une base de données Oracle sur site vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT

Créée par Sergey Dmitriev (AWS) et Naresh Damera (AWS)

Récapitulatif

Ce modèle vous guide tout au long de la migration d'une base de données Oracle sur site vers une instance de base de données Amazon Relational Database Service (Amazon RDS) pour MySQL. Il utilise AWS Database Migration Service (AWS DMS) pour migrer les données, et AWS Schema Conversion Tool (AWS SCT) pour convertir le schéma et les objets de la base de données source dans un format compatible avec Amazon RDS for MySQL.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle source dans un centre de données sur site

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- Toutes les éditions de base de données Oracle pour les versions 11g (versions 11.2.0.3.v1 et ultérieures), 12.2 et 18c. Pour obtenir la dernière liste des versions prises en charge, consultez Utilisation d'une base de données Oracle comme source pour AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités. Pour plus d'informations sur les versions de base de données Oracle prises en charge par AWS SCT, consultez la documentation AWS SCT.
- AWS DMS prend actuellement en charge les versions 5.5, 5.6 et 5.7 de MySQL. Pour obtenir la dernière liste des versions prises en charge, consultez la section Utilisation d'une base de données compatible MySQL comme cible pour AWS DMS dans la documentation AWS.

Architecture

Pile technologique source

- Base de données Oracle sur site

Pile technologique cible

- Instance de base de données Amazon RDS pour MySQL

Architecture de migration des données

Outils

- AWS DMS - AWS Database Migration Services (AWS DMS) vous aide à migrer des bases de données relationnelles, des entrepôts de données, des bases de données NoSQL et d'autres types de magasins de données. Vous pouvez utiliser AWS DMS pour migrer vos données dans le cloud AWS, entre plusieurs instances sur site (via une configuration AWS Cloud) ou entre différentes combinaisons de configurations cloud et sur site.
- AWS SCT - AWS Schema Conversion Tool (AWS SCT) est utilisé pour convertir le schéma de votre base de données d'un moteur de base de données à un autre. Le code personnalisé converti par l'outil inclut les vues, les procédures stockées et les fonctions. Tout code que l'outil ne peut pas convertir automatiquement est clairement indiqué afin que vous puissiez le convertir vous-même.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez la version et le moteur de la base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, SysAdmin

Tâche	Description	Compétences requises
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d'instanc e approprié en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin
Identifiez la stratégie de migration des applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		SysAdmin
Créez les groupes de sécurité et les listes de contrôle d'accès au réseau (ACLs).		SysAdmin
Configurez et démarrez une instance de base de données Amazon RDS.		DBA, SysAdmin

Migrer les données

Tâche	Description	Compétences requises
Migrez le schéma de base de données à l'aide d'AWS SCT.		DBA
Migrez les données à l'aide d'AWS DMS.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Utilisez AWS SCT pour analyser et convertir le code SQL contenu dans le code de l'application.	Pour plus d'informations, consultez https://docs.aws.amazon.com/SchemaConversionTool/ latest/userguide/ CHAP _converting.app.html.	Propriétaire de l'application
Suivez la stratégie de migration des applications.		DBA, propriétaire de SysAdmin l'application

Découper

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, SysAdmin
Passez en revue et validez les documents du projet.		DBA, SysAdmin
Collectez des indicateurs concernant le délai de migration, le pourcentage de manuel par rapport à l'outil, les économies de coûts, etc.		DBA, SysAdmin
Clôturez le projet et faites part de vos commentaires.		

Ressources connexes

Références

- Documentation AWS DMS
- Documentation AWS SCT
- Tarification d'Amazon RDS

Tutoriel et vidéos

- Commencer à utiliser AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)
- AWS DMS (vidéo)
- Amazon RDS (vidéo)

Migrer une base de données Oracle sur site vers Amazon RDS for PostgreSQL à l'aide d'un assistant Oracle et d'AWS DMS

Créée par Cady Motyka (AWS)

Récapitulatif

Ce modèle décrit comment vous pouvez migrer une base de données Oracle sur site vers l'un des services de base de données AWS compatibles avec PostgreSQL suivants avec un temps d'arrêt minimal :

- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL
- Amazon Aurora PostgreSQL-Compatible Edition

La solution utilise AWS Database Migration Service (AWS DMS) pour migrer les données, AWS Schema Conversion Tool (AWS SCT) pour convertir le schéma de base de données et une base de données Oracle Bystander pour aider à gérer la migration. Dans cette implémentation, le temps d'arrêt est limité au temps nécessaire pour créer ou valider toutes les clés étrangères de la base de données.

La solution utilise également des instances Amazon Elastic Compute Cloud (Amazon EC2) associées à une base de données Oracle Bystander pour aider à contrôler le flux de données via AWS DMS. Vous pouvez suspendre temporairement la réplication en continu depuis la base de données Oracle sur site vers le périphérique Oracle pour activer AWS DMS afin de rattraper le retard en matière de validation des données, ou pour utiliser un autre outil de validation des données. L'instance de base de données Amazon RDS for PostgreSQL ou l'instance de base de données compatible Aurora PostgreSQL et la base de données externe disposeront des mêmes données lorsque AWS DMS aura terminé de migrer les modifications en cours.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle source dans un centre de données sur site avec une base de données de secours Active Data Guard configurée
- AWS Direct Connect configuré entre le centre de données sur site et AWS Secrets Manager pour stocker les secrets de base de données

- Pilotes de connectivité de base de données Java (JDBC) pour les connecteurs AWS SCT, installés soit sur une machine locale, soit sur l'instance EC2 où AWS SCT est installé
- Connaissance de l'utilisation d'une base de données Oracle comme source pour AWS DMS
- Connaissance de l'utilisation d'une base de données PostgreSQL comme cible pour AWS DMS

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- AWS DMS prend en charge toutes les éditions de base de données Oracle pour les versions 10.2 et ultérieures (pour les versions 10.x), 11g et versions supérieures à 12.2, 18c et 19c. Pour obtenir la dernière liste des versions prises en charge, consultez Utilisation d'une base de données Oracle comme source pour AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités. Pour plus d'informations sur les versions de base de données Oracle prises en charge par AWS SCT, consultez la documentation AWS SCT.
- AWS DMS prend en charge les versions 9.4 et ultérieures de PostgreSQL (pour les versions 9.x), 10.x, 11.x, 12.x et 13.x. Pour obtenir les informations les plus récentes, consultez la section Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS dans la documentation AWS.

Architecture

Pile technologique source

- Une base de données Oracle sur site
- Une EC2 instance qui contient un témoin pour la base de données Oracle

Pile technologique cible

- Instance Amazon RDS pour PostgreSQL ou Aurora PostgreSQL, PostgreSQL 9.3 et versions ultérieures

Architecture cible

Le schéma suivant montre un exemple de flux de travail pour la migration d'une base de données Oracle vers une base de données AWS compatible avec PostgreSQL à l'aide d'AWS DMS et d'un assistant Oracle :

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.

Épopées

Convertir le schéma de base de données Oracle en PostgreSQL

Tâche	Description	Compétences requises
Configurez AWS SCT.	Créez un nouveau rapport et connectez-vous à Oracle en tant que source et à PostgreSQL en tant que cible. Dans les paramètres du projet, accédez à l'onglet SQL Scripting. Remplacez le script SQL cible par plusieurs fichiers. Ces fichiers seront utilisés ultérieurement et nommés comme suit : • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql	DBA

Tâche	Description	Compétences requises
	• create_function.sql	
Convertissez le schéma de base de données Oracle.	Dans l'onglet Action, choisissez Générer un rapport. Choisissez ensuite Convertir le schéma, puis Enregistrer en tant que SQL.	DBA
Modifiez les scripts.	Par exemple, vous souhaiterez peut-être modifier le script si un nombre du schéma source a été converti au format numérique dans PostgreSQL, mais vous souhaitez plutôt utiliser BIGINT pour de meilleures performances.	DBA

Création et configuration de l'instance de base de données Amazon RDS

Tâche	Description	Compétences requises
Créez l'instance de base de données Amazon RDS.	Dans la région AWS appropriée, créez une nouvelle instance de base de données PostgreSQL. Pour plus d'informations, consultez Création d'une instance de base de données PostgreSQL et connexion à une base de données sur une instance de base de données PostgreSQL dans la documentation Amazon RDS.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Configurez les spécifications de l'instance DB.	Spécifiez la version du moteur de base de données, la classe d'instance de base de données, le déploiement multi-AZ, le type de stockage et le stockage alloué. Entrez l'identifiant de l'instance de base de données, un nom d'utilisateur principal et un mot de passe principal.	AWS SysAdmin, DBA
Configurez le réseau et la sécurité.	Spécifiez le cloud privé virtuel (VPC), le groupe de sous-réseaux, l'accessibilité publique, la préférence de zone de disponibilité et les groupes de sécurité.	DBA, SysAdmin
Configurez les options de base de données	Spécifiez le nom de la base de données, le port, le groupe de paramètres, le chiffrement et la clé KMS.	AWS SysAdmin, DBA
Configurez des sauvegardes.	Spécifiez la période de conservation des sauvegardes, la fenêtre de sauvegarde, l'heure de début, la durée et indiquez s'il faut copier les balises dans les instantanés.	AWS SysAdmin, DBA
Configurez les options de surveillance.	Activez ou désactivez une surveillance améliorée et des informations sur les performances.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Configurez les options de maintenance.	Spécifiez la mise à niveau automatique de la version mineure, la fenêtre de maintenance, ainsi que le jour, l'heure et la durée de début.	AWS SysAdmin, DBA
Exécutez les scripts de pré-migration depuis AWS SCT.	Sur l'instance Amazon RDS, exécutez les scripts suivants générés par AWS SCT : • create_database.sql • create_sequence.sql • create_table.sql • create_view.sql • create_function.sql	AWS SysAdmin, DBA

Configuration de l'Oracle Bystander dans Amazon EC2

Tâche	Description	Compétences requises
Configurez le réseau pour Amazon EC2.	Créez le nouveau VPC, les sous-réseaux, la passerelle Internet, les tables de routage et les nouveaux groupes de sécurité.	AWS SysAdmin
Créez l' EC2 instance.	Dans la région AWS approprié e, créez une nouvelle EC2 instance. Sélectionnez l'Amazon Machine Image (AMI), choisissez la taille de l'instance et configurez les détails de l'instance : nombre d'instances (1), VPC et sous-	AWS SysAdmin

Tâche	Description	Compétences requises
	réseau que vous avez créés lors de la tâche précédente, attribution automatique d'une adresse IP publique et autres options. Ajoutez de l'espace de stockage, configurez les groupes de sécurité et lancez-vous. Lorsque vous y êtes invité, créez et enregistrez une paire de clés pour l'étape suivante.	
Connectez la base de données source Oracle à l' EC2 instance.	Copiez l'adresse IP IPv4 publique et le DNS dans un fichier texte et connectez-vous en utilisant SSH comme suit : ssh -i « your_file.pem » EC2-User@<your-IP - -DNS>. address-or-public	AWS SysAdmin
Configurez l'hôte initial pour un spectateur sur Amazon. EC2	Configurez les clés SSH, le profil bash, ORATAB et les liens symboliques. Créez des annuaires Oracle.	AWS SysAdmin, administr ateur Linux
Configurer la copie de base de données pour un spectateur sur Amazon EC2	Utilisez RMAN pour créer une copie de base de données, activer la journalisation supplémentaire et créer le fichier de contrôle de secours. Une fois la copie terminée, placez la base de données en mode de restauration.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Configurez Oracle Data Guard.	Modifiez votre fichier listener.ora et démarrez l'écouteur. Configurez une nouvelle destination d'archivage. Placez le témoin en mode de restauration, remplacez les fichiers temporaires pour éviter toute corruption future, installez un crontab si nécessaire pour empêcher le répertoire d'archives de manquer d'espace et modifiez le fichier manage-trclog-files-oracle.cfg pour la source et le fichier de secours.	AWS SysAdmin, DBA
Préparez la base de données Oracle pour synchroniser les expéditions.	Ajoutez les fichiers journaux de secours et modifiez le mode de restauration. Modifiez le journal d'expédition en SYNC AFFIRM à la fois sur la source principale et sur la source de secours. Activez les journaux principaux, confirmez via le journal des alertes Amazon EC2 Bystander que vous utilisez les fichiers journaux de secours et confirmez que le flux de rétablissement circule en mode SYNC.	AWS SysAdmin, DBA

Migrer les données avec AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication dans AWS DMS.	Renseignez les champs relatifs au nom, à la classe d'instance, au VPC (identiqu e à l' EC2 instance Amazon), au Multi-AZ et à l'accessi bilité publique. Sous Advance, spécifiez le stockage alloué, le groupe de sous-réseaux, la zone de disponibilité, les groupes de sécurité VPC et la clé AWS Key Management Service (AWS KMS).	AWS SysAdmin, DBA
Créez le point de terminaison de la base de données source.	Spécifiez le nom du point de terminaison, le type, le moteur source (Oracle), le nom du serveur (nom DNS EC2 privé Amazon), le port, le mode SSL, le nom d'utilisateur, le mot de passe, le SID, le VPC (spécifiez le VPC qui possède l'instance de réplication) et l'instance de réplication. Pour tester la connexion, choisisse z Run Test, puis créez le point de terminaison. Vous pouvez également configurer les paramètres avancés suivants : maxFileSizeet numberDat aTypeScale.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Connectez AWS DMS à Amazon RDS pour PostgreSQL.	Créez un groupe de sécurité de migration pour les connexions entre elles VPCs.	AWS SysAdmin, DBA
Créez le point de terminaison de base de données cible.	Spécifiez le nom du point de terminaison, le type, le moteur source (PostgreSQL), le nom du serveur (point de terminaison Amazon RDS), le port, le mode SSL, le nom d'utilisateur, le mot de passe, le nom de la base de données, le VPC (spécifiez le VPC qui possède l'instance de réplication) et l'instance de réplication. Pour tester la connexion, choisissez Run Test, puis créez le point de terminaison. Vous pouvez également configurer les paramètres avancés suivants : maxFileSize et numberDataTypeScale.	AWS SysAdmin, DBA
Créez la tâche de réplication AWS DMS.	Spécifiez le nom de la tâche, l'instance de réplication, les points de terminaison source et cible, ainsi que l'instance de réplication. Pour le type de migration, choisissez Migrer les données existantes et répliquer les modifications en cours. Décochez la case Démarrer la tâche lors de la création.	AWS SysAdmin, DBA

Tâche	Description	Compétences requises
Configurez les paramètres des tâches de réplication AWS DMS.	Pour le mode de préparation de la table cible, choisissez Ne rien faire. Arrêtez la tâche une fois le chargement complet terminé (pour créer des clés primaires). Spécifiez le mode LOB limité ou complet et activez les tables de contrôle. Vous pouvez éventuell ement configurer le réglage CommitRateavancé.	DBA
Configurez les mappages de tables.	Dans la section Mappages de tables, créez une règle d'inclusion pour toutes les tables de tous les schémas inclus dans la migration, puis créez une règle d'exclusion . Ajoutez trois règles de transformation pour convertir les noms de schéma, de table et de colonne en minuscule s, et ajoutez toutes les autres règles nécessaires à cette migration spécifique.	DBA
Lancez la tâche.	Lancez la tâche de réplicati on. Assurez-vous que le chargement complet est en cours. Exécutez ALTER SYSTEM SWITCH LOGFILE sur la base de données Oracle principale pour démarrer la tâche.	DBA

Tâche	Description	Compétences requises
Exécutez les scripts de mi-migration depuis AWS SCT.	Dans Amazon RDS for PostgreSQL, exécutez les scripts suivants générés par AWS SCT : • create_index.sql • create_constraint.sql	DBA
Redémarrez la tâche pour continuer la capture des données de modification (CDC).	Exécutez VACUUM sur l'instance de base de données Amazon RDS for PostgreSQ L et redémarrez la tâche AWS DMS pour appliquer les modifications CDC mises en cache.	DBA

Passez à la base de données PostgreSQL

Tâche	Description	Compétences requises
Consultez les journaux et les tables de validation d'AWS DMS pour détecter toute erreur.	Vérifiez et corrigez les erreurs de réplication ou de validation.	DBA
Arrêtez toutes les dépendanc es Oracle.	Arrêtez toutes les dépendanc es Oracle, arrêtez les écouteurs de la base de données Oracle et exécutez ALTER SYSTEM SWITCH LOGFILE. Arrêtez la tâche AWS DMS lorsqu'elle ne montre aucune activité.	DBA

Tâche	Description	Compétences requises
Exécutez les scripts de post-migration depuis AWS SCT.	Dans Amazon RDS for PostgreSQL, exécutez les scripts suivants générés par AWS SCT : • create_foreign_key_constraint.sql • create_triggers.sql	DBA
Effectuez les étapes supplémentaires relatives à Amazon RDS for PostgreSQL.	Incrémentez les séquences pour qu'elles correspondent à Oracle si nécessaire, exécutez VACUUM et ANALYZE, puis prenez un instantané pour vérifier la conformité.	DBA
Ouvrez les connexions à Amazon RDS for PostgreSQL.	Supprimez les groupes de sécurité AWS DMS d'Amazon RDS for PostgreSQL, ajoutez des groupes de sécurité de production et dirigez vos applications vers la nouvelle base de données.	DBA
Nettoyez les objets AWS DMS.	Supprimez les points de terminaison, les tâches de réplication, les instances de réplication et l' EC2 instance.	SysAdmin, DBA

Ressources connexes

- Documentation AWS DMS
- Documentation AWS SCT
- Tarification d'Amazon RDS for PostgreSQL

Migrer d'une base de données Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle GoldenGate

Créée par Dhairya Jindani (AWS), Rajeshkumar Sabankar (AWS) et Sindhusha Paturu (AWS)

Récapitulatif

Ce modèle montre comment migrer une base de données Oracle vers Amazon Relational Database Service (Amazon RDS) pour PostgreSQL à l'aide d'Oracle Cloud Infrastructure (OCI). GoldenGate

Oracle GoldenGate vous permet de répliquer les données entre votre base de données source et une ou plusieurs bases de données de destination avec un temps d'arrêt minimal.

> **Note**
>
> La base de données Oracle source peut se trouver sur site ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez utiliser une procédure similaire lorsque vous utilisez des outils de réplication locaux.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une GoldenGate licence Oracle
- pilote Java Database Connectivity (JDBC) pour se connecter à la base de données PostgreSQL
- Schéma et tables créés avec l'outil AWS Schema Conversion Tool (AWS SCT) sur la base de données Amazon RDS for PostgreSQL cible

Limites

- Oracle GoldenGate peut uniquement répliquer les données de table existantes (chargement initial) et les modifications en cours (capture des données de modification)

Versions du produit

- Oracle Database Enterprise Edition 10g ou versions plus récentes

- Oracle GoldenGate 12.2.0.1.1 pour Oracle ou versions plus récentes
- Oracle GoldenGate 12.2.0.1.1 pour PostgreSQL ou versions plus récentes

Architecture

Le schéma suivant montre un exemple de flux de travail pour la migration d'une base de données Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle : GoldenGate

Le schéma suivant illustre le flux de travail suivant :

1. Le processus Oracle GoldenGate Extract s'exécute sur la base de données source pour extraire les données.
2. Le processus Oracle GoldenGate Replicat fournit les données extraites à la base de données Amazon RDS for PostgreSQL cible.

Outils

- Oracle vous GoldenGate aide à concevoir, exécuter, orchestrer et surveiller vos solutions de réplication et de traitement des données en continu dans l'infrastructure cloud Oracle.
- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.

Épopées

Téléchargez et installez Oracle GoldenGate

Tâche	Description	Compétences requises
Téléchargez Oracle GoldenGate.	Téléchargez les versions suivantes d'Oracle GoldenGate : • Oracle GoldenGate 12.2.0.1.1 pour Oracle ou une version plus récente	DBA

Tâche	Description	Compétences requises
	• Oracle GoldenGate 12.2.0.1.1 pour PostgreSQL ou une version plus récente Pour télécharger le logiciel, consultez Oracle GoldenGate Downloads sur le site Web d'Oracle.	
Installez Oracle GoldenGate pour Oracle sur le serveur de base de données Oracle source.	Pour obtenir des instructions, consultez la GoldenGate documentation Oracle.	DBA
Installez la base de données Oracle GoldenGate pour PostgreSQL sur l'instance Amazon. EC2	Pour obtenir des instructions, consultez la GoldenGate documentation Oracle.	DBA

Configuration d'Oracle GoldenGate sur les bases de données source et cible

Tâche	Description	Compétences requises
Configurez la base de données Oracle GoldenGate pour Oracle sur la base de données source.	Pour obtenir des instructions, consultez la GoldenGate documentation Oracle. Assurez-vous de configurer les éléments suivants : • Journalisation supplémentaire • GoldenGate Utilisateurs d'Oracle	DBA

Tâche	Description	Compétences requises
	• Toutes les subventions et autorisations requises • Fichiers de paramètres • Processus de gestion • Annuaire • Fichiers GLOBALS • Portefeuille Oracle	
Configurez Oracle GoldenGate pour PostgreSQL sur la base de données cible.	Pour obtenir des instructions, reportez-vous à la partie VI Utilisation d'Oracle GoldenGate pour PostgreSQL sur le site Web d'Oracle. Assurez-vous de configurer les éléments suivants : • Processus de gestion • Fichiers GLOBALS • Portefeuille Oracle	DBA

Configuration de la capture de données

Tâche	Description	Compétences requises
Configurez le processus d'extraction dans la base de données source.	Dans la base de données Oracle source, créez un fichier d'extraction pour extraire les données. Pour obtenir des instructions, voir AJOUTER UN EXTRAIT dans la documentation Oracle.	DBA

Tâche	Description	Compétences requises
	Note Le fichier d'extrait inclut la création du fichier de paramètre s d'extraction et du répertoire du fichier de suivi.	
Configurez une pompe de données pour transférer le fichier de suivi de la base de données source vers la base de données cible.	Créez un fichier de paramètre s EXTRACT et un répertoir e de fichiers de suivi en suivant les instructions de la section PARFILE dans Database Utilities sur le site Web d'Oracle. Pour plus d'informations, voir Qu'est-ce qu'un sentier ? dans Fusion Middleware Understan ding Oracle GoldenGate sur le site Web d'Oracle.	DBA

Tâche	Description	Compétences requises
Configurez la réplication sur l'EC2 instance Amazon.	Créez un fichier de paramètres de réplication et un répertoire de fichiers de suivi. Pour plus d'informations sur la création de fichiers de paramètres de réplication, reportez-vous à la section 3.5 Validation d'un fichier de paramètres dans la documentation de la base de données Oracle. Pour plus d'informations sur la création d'un répertoire de fichiers de suivi, consultez la section Création d'un journal dans la documentation d'Oracle Cloud. ⚠ Important Assurez-vous d'ajouter une entrée de table de points de contrôle dans le fichier GLOBALS sur la cible. Pour plus d'informations, voir Qu'est-ce qu'un réplicat ? dans Fusion Middlewar e Understanding Oracle GoldenGate sur le site Web d'Oracle.	DBA

Configuration de la réplication des données

Tâche	Description	Compétences requises
Dans la base de données source, créez un fichier de paramètres pour extraire les données pour le chargement initial.	Suivez les instructions de la section Création d'un fichier de paramètres dans GGSCI dans la documentation Oracle Cloud. ⚠ Important Assurez-vous que le gestionnaire est en cours d'exécution sur la cible.	DBA
Dans la base de données cible, créez un fichier de paramètres pour répliquer les données pour le chargement initial.	Suivez les instructions de la section Création d'un fichier de paramètres dans GGSCI dans la documentation Oracle Cloud. ⚠ Important Assurez-vous d'ajouter et de démarrer le processus Replicat.	DBA

Passez à la base de données Amazon RDS for PostgreSQL

Tâche	Description	Compétences requises
Arrêtez le processus Replicat et assurez-vous que les bases	Comparez le nombre de lignes entre les bases de données source et cible pour vous	DBA

Tâche	Description	Compétences requises
de données source et cible sont synchronisées.	assurer que la réplication des données a été réussie.	
Configurez la prise en charge du langage de définition des données (DDL).	Exécutez le script DDL pour créer des déclencheurs, des séquences, des synonymes et des clés de référence sur PostgreSQL. **Note** Vous pouvez utiliser n'importe quelle application client SQL standard pour vous connecter à une base de données de votre cluster de bases de données. Par exemple, vous pouvez utiliser pgAdmin pour vous connecter à votre instance de base de données.	DBA

Ressources connexes

- Amazon RDS pour PostgreSQL (Guide de l'utilisateur Amazon RDS)
- EC2 Documentation Amazon
- Méthodes de traitement et bases de données prises en GoldenGate charge par Oracle (documentation Oracle)

Migrer une base de données Oracle vers Amazon Redshift à l'aide d'AWS DMS et d'AWS SCT

Créée par Piyush Goyal (AWS) et Brian Motzer (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration de bases de données Oracle vers un entrepôt de données cloud Amazon Redshift dans le cloud Amazon Web Services (AWS) à l'aide d'AWS Database Migration Service (AWS DMS) et d'AWS Schema Conversion Tool (AWS SCT). Le modèle couvre les bases de données Oracle sources qui sont sur site ou installées sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Il couvre également Amazon Relational Database Service (Amazon RDS) pour les bases de données Oracle.

Conditions préalables et limitations

Prérequis

- Une base de données Oracle exécutée dans un centre de données sur site ou dans le cloud AWS
- Un compte AWS actif
- Connaissance de l'utilisation d'une base de données Oracle comme source pour AWS DMS
- Connaissance de l'utilisation d'une base de données Amazon Redshift comme cible pour AWS DMS
- Connaissance d'Amazon RDS, d'Amazon Redshift, des technologies de base de données applicables et de SQL
- Pilotes de connectivité de base de données Java (JDBC) pour les connecteurs AWS SCT, sur lesquels AWS SCT est installé

Versions du produit

- Pour les bases de données Oracle autogérées, AWS DMS prend en charge toutes les éditions de base de données Oracle pour les versions 10.2 et ultérieures (pour les versions 10). x), 11 g et jusqu'à 12,2, 18 °C et 19 °C. Pour les bases de données Amazon RDS for Oracle gérées par AWS, AWS DMS prend en charge toutes les éditions des bases de données Oracle pour les versions 11g (versions 11.2.0.4 et ultérieures) et jusqu'à 12.2, 18c et 19c. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.

Architecture

Pile technologique source

L'un des éléments suivants :

- Une base de données Oracle sur site
- Une base de données Oracle sur une EC2 instance
- Une instance de base de données Amazon RDS pour Oracle

Pile technologique cible

- Amazon Redshift

Architecture cible

D'une base de données Oracle exécutée dans le cloud AWS à Amazon Redshift :

D'une base de données Oracle exécutée dans un centre de données sur site à Amazon Redshift :

Outils

- AWS DMS - AWS Data Migration Service (AWS DMS) vous aide à migrer des bases de données vers AWS rapidement et en toute sécurité. La base de données source reste pleinement opérationnelle pendant la migration, minimisant ainsi les interruptions de service pour les applications qui dépendent de la base de données. AWS DMS peut migrer vos données vers et depuis les bases de données commerciales et open source les plus utilisées.
- AWS SCT - AWS Schema Conversion Tool (AWS SCT) peut être utilisé pour convertir votre schéma de base de données existant d'un moteur de base de données à un autre. Il prend en charge divers moteurs de base de données, notamment Oracle, SQL Server et PostgressQL, en tant que sources.

Épopées

Préparez-vous à la migration

Tâche	Description	Compétences requises
Validez les versions de base de données.	Validez les versions de base de données source et cible et assurez-vous qu'elles sont prises en charge par AWS DMS. Pour plus d'informations sur les versions de base de données Oracle prises en charge, consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS. Pour plus d'informations sur l'utilisation d'Amazon Redshift comme cible, consultez la section Utilisation d'une base de données Amazon Redshift comme cible pour AWS DMS.	DBA
Créez un VPC et un groupe de sécurité.	Dans votre compte AWS, créez un cloud privé virtuel (VPC), s'il n'existe pas. Créez un groupe de sécurité pour le trafic sortant vers les bases de données source et cible. Pour plus d'informations, consultez la documentation Amazon Virtual Private Cloud (Amazon VPC).	Administrateur de systèmes
Installer AWS SCT.	Téléchargez et installez la dernière version d'AWS SCT et les pilotes correspondants.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez Installation, vérification et mise à jour de l'AWS SCT.	
Créez un utilisateur pour la tâche AWS DMS.	Créez un utilisateur AWS DMS dans la base de données source et accordez-lui les privilèges READ. Cet utilisateur sera utilisé à la fois par AWS SCT et AWS DMS.	DBA
Testez la connectivité à la base de données.	Testez la connectivité à l'instance de base de données Oracle.	DBA
Créez un projet dans AWS SCT.	Ouvrez l'outil AWS SCT et créez un nouveau projet.	DBA
Analysez le schéma Oracle à migrer.	Utilisez AWS SCT pour analyser le schéma à migrer et générer un rapport d'évaluation de la migration de base de données. Pour plus d'informations, consultez la section Création d'un rapport d'évaluation de la migration de base de données dans la documentation AWS SCT.	DBA

Tâche	Description	Compétences requises
Consultez le rapport d'évaluation.	Consultez le rapport pour connaître la faisabilité de la migration. Certains objets de base de données peuvent nécessiter une conversion manuelle. Pour plus d'informations sur le rapport, consultez la section Affichage du rapport d'évaluation dans la documentation AWS SCT.	DBA

Préparer la base de données cible

Tâche	Description	Compétences requises
Créez un cluster Amazon Redshift.	Créez un cluster Amazon Redshift au sein du VPC que vous avez créé précédemment. Pour plus d'informations, consultez les clusters Amazon Redshift dans la documentation Amazon Redshift.	DBA
Créez des utilisateurs de base de données.	Extrayez la liste des utilisateurs, des rôles et des autorisations de la base de données source Oracle. Créez des utilisateurs dans la base de données Amazon Redshift cible et appliquez les rôles définis à l'étape précédente.	DBA
Évaluez les paramètres de base de données.	Passez en revue les options de base de données, les paramètres, les fichiers	DBA

Tâche	Description	Compétences requises
	réseau et les liens de base de données de la base de données source Oracle, et évaluez leur applicabilité à la cible.	
Appliquez tous les paramètres pertinents à la cible.	Pour plus d'informations sur cette étape, consultez la référence de configuration dans la documentation Amazon Redshift.	DBA

Création d'objets dans la base de données cible

Tâche	Description	Compétences requises
Créez un utilisateur AWS DMS dans la base de données cible.	Créez un utilisateur AWS DMS dans la base de données cible et accordez-lui des privilèges de lecture et d'écriture. Validez la connectivité depuis AWS SCT.	DBA
Convertissez le schéma, consultez le rapport SQL et enregistrez les erreurs ou les avertissements éventuels.	Pour plus d'informations, consultez la section Conversion de schémas de base de données à l'aide d'AWS SCT dans la documentation AWS SCT.	DBA
Appliquez les modifications de schéma à la base de données cible ou enregistrez-les sous forme de fichier .sql.	Pour obtenir des instructions, consultez la section Enregistrer et appliquer votre schéma converti dans l'AWS SCT dans la documentation AWS SCT.	DBA

Tâche	Description	Compétences requises
Validez les objets de la base de données cible.	Validez les objets créés à l'étape précédente dans la base de données cible. Réécrivez ou redessinez les objets qui n'ont pas été correctement convertis.	DBA
Désactivez les clés étrangères et les déclencheurs.	Désactivez les clés étrangère s et les déclencheurs. Cela peut entraîner des problèmes de chargement des données pendant le processus de chargement complet lors de l'exécution d'AWS DMS.	DBA

Migrer des données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication AWS DMS.	Connectez-vous à l'AWS Management Console, puis ouvrez la console AWS DMS. Dans le volet de navigatio n, choisissez Instances de réplication, puis Créer une instance de réplication. Pour obtenir des instructions détaillées, consultez l'étape 1 de la section Mise en route avec AWS DMS dans la documentation AWS DMS.	DBA
Créez des points de terminais on source et cible.	Créez des points de terminais on source et cible, testez la connexion entre l'instance de	DBA

Tâche	Description	Compétences requises
	réplication et les points de terminaison source et cible. Pour obtenir des instructions détaillées, consultez l'étape 2 de la section Mise en route avec AWS DMS dans la documentation AWS DMS.	
Créez une tâche de réplicati on.	Créez une tâche de réplicati on et sélectionnez la méthode de migration appropriée. Pour obtenir des instructions détaillées, consultez l'étape 3 de la section Mise en route avec AWS DMS dans la documentation AWS DMS.	DBA
Démarrez la réplication des données.	Lancez la tâche de réplication et surveillez les journaux pour détecter toute erreur.	DBA

Migrez votre application

Tâche	Description	Compétences requises
Créez des serveurs d'applica tions.	Créez les nouveaux serveurs d'applications sur AWS.	Propriétaire de l'application
Migrez le code de l'application.	Migrez le code de l'application vers les nouveaux serveurs.	Propriétaire de l'application
Configurez le serveur d'applica tions.	Configurez le serveur d'applica tions pour la base de données cible et les pilotes.	Propriétaire de l'application

Tâche	Description	Compétences requises
Optimisez le code de l'application.	Optimisez le code de l'application pour le moteur cible.	Propriétaire de l'application

Passez à la base de données cible

Tâche	Description	Compétences requises
Validez les utilisateurs.	Dans la base de données Amazon Redshift cible, validez les utilisateurs et accordez-leur des rôles et des privilèges.	DBA
Vérifiez que l'application est verrouillée.	Assurez-vous que l'application est verrouillée afin d'empêcher toute modification ultérieure.	Propriétaire de l'application
Validez les données.	Validez les données de la base de données Amazon Redshift cible.	DBA
Activez les clés étrangères et les déclencheurs.	Activez les clés étrangères et les déclencheurs dans la base de données Amazon Redshift cible.	DBA
Connectez-vous à la nouvelle base de données.	Configurez l'application pour qu'elle se connecte à la nouvelle base de données Amazon Redshift.	Propriétaire de l'application
Effectuez les dernières vérifications.	Effectuez une dernière vérification complète du système avant la mise en ligne.	DBA, propriétaire de l'application

Tâche	Description	Compétences requises
Passez en direct.	Passez en ligne avec la base de données Amazon Redshift cible.	DBA

Clôturer le projet de migration

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.	Arrêtez les ressources AWS temporaires telles que l'instance de réplication AWS DMS et l' EC2 instance utilisée pour AWS SCT.	DBA, administrateur système
Passez en revue les documents.	Passez en revue et validez les documents du projet de migration.	DBA, administrateur système
Collectez des statistiques.	Collectez des informations sur le projet de migration, telles que le délai de migration, le pourcentage de tâches manuelles par rapport aux tâches liées aux outils et les économies totales.	DBA, administrateur système
Clôturez le projet.	Clôturez le projet et faites part de vos commentaires.	DBA, administrateur système

Ressources connexes

Références

- Guide de l'utilisateur d'AWS DMS
- Guide de l'utilisateur d'AWS SCT

- Guide de démarrage d'Amazon Redshift

Tutoriels et vidéos

- Découvrez AWS SCT et AWS DMS en profondeur (présentation tirée d'AWS re:Invent 2019)
- Commencer à utiliser AWS Database Migration Service

Migrer une base de données Oracle vers Aurora PostgreSQL à l'aide d'AWS DMS et d'AWS SCT

Créée par Senthil Ramasamy (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Oracle vers Amazon Aurora PostgreSQL Compatible Edition à l'aide d'AWS Data Migration Service (AWS DMS) et d'AWS Schema Conversion Tool (AWS SCT).

Le modèle couvre les bases de données Oracle sources qui se trouvent sur site, les bases de données Oracle installées sur les instances Amazon Elastic Compute Cloud (Amazon EC2) et Amazon Relational Database Service (Amazon RDS) pour les bases de données Oracle. Le modèle convertit ces bases de données en bases de données compatibles avec Aurora PostgreSQL.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une base de données Oracle dans un centre de données sur site ou dans le cloud AWS.
- Clients SQL installés sur une machine locale ou sur une EC2 instance.
- Pilotes Java Database Connectivity (JDBC) pour les connecteurs AWS SCT, installés soit sur une machine locale, soit sur une instance sur EC2 laquelle AWS SCT est installé.

Limites

- Limite de taille de base de données : 128 To
- Si la base de données source prend en charge une application commerciale off-the-shelf (COTS) ou est spécifique à un fournisseur, vous ne pourrez peut-être pas la convertir vers un autre moteur de base de données. Avant d'utiliser ce modèle, vérifiez que l'application est compatible avec Aurora PostgreSQL.

Versions du produit

- Pour les bases de données Oracle autogérées, AWS DMS prend en charge toutes les éditions de base de données Oracle pour les versions 10.2 et ultérieures (pour les versions 10.x), 11g et

jusqu'à 12.2, 18c et 19c. Pour obtenir la dernière liste des versions de base de données Oracle prises en charge (autogérée et Amazon RDS for Oracle), consultez les sections Utilisation d'une base de données Oracle comme source pour AWS DMS et Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS.

- Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités. Pour plus d'informations sur les versions de base de données Oracle prises en charge par AWS SCT, consultez la documentation AWS SCT.
- Aurora prend en charge les versions de PostgreSQL répertoriées dans les versions et versions du moteur d'Amazon Aurora PostgreSQL.

Architecture

Pile technologique source

L'un des éléments suivants :

- Une base de données Oracle sur site
- Une base de données Oracle sur une EC2 instance
- Une instance de base de données Amazon RDS pour Oracle

Pile technologique cible

- Compatible avec Aurora avec PostgreSQL

Architecture cible

Architecture de migration des données

- À partir d'une base de données Oracle exécutée dans le cloud AWS

- À partir d'une base de données Oracle exécutée dans un centre de données sur site

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Épopées

Préparer la migration

Tâche	Description	Compétences requises
Préparez la base de données source.	Pour préparer la base de données source, consultez la section Utilisation d'Oracle Database comme source pour AWS SCT dans la documentation AWS SCT.	DBA
Créez une EC2 instance pour AWS SCT.	Créez et configurez une EC2 instance pour AWS SCT, si nécessaire.	DBA
Téléchargez AWS SCT.	Téléchargez la dernière version d'AWS SCT et des pilotes associés. Pour plus d'informations, consultez la section Installation, vérification et mise à jour d'AWS SCT dans la documentation AWS SCT.	DBA
Ajoutez des utilisateurs et des autorisations.	Ajoutez et validez les utilisateurs et autorisations requis	DBA

Tâche	Description	Compétences requises
	dans la base de données source.	
Créez un projet AWS SCT.	Créez un projet AWS SCT pour la charge de travail et connectez-vous à la base de données source. Pour obtenir des instructions, consultez les sections Création d'un projet AWS SCT et Ajout de serveurs de base de données dans la documentation AWS SCT.	DBA
Évaluez la faisabilité.	Générez un rapport d'évaluation qui résume les mesures à prendre pour les schémas qui ne peuvent pas être convertis automatiquement et fournit des estimations pour les efforts de conversion manuels. Pour plus d'informations, consultez la section Création et révision du rapport d'évaluation de la migration de base de données dans la documentation AWS SCT.	DBA

Préparer la base de données cible

Tâche	Description	Compétences requises
Créez une instance de base de données Amazon RDS cible.	Créez une instance de base de données Amazon RDS cible en utilisant Amazon	DBA

Tâche	Description	Compétences requises
	Aurora comme moteur de base de données. Pour obtenir des instructions, consultez la section Création d'une instance de base de données Amazon RDS dans la documentation Amazon RDS.	
Extrayez les utilisateurs, les rôles et les autorisations.	Extrayez la liste des utilisateurs, des rôles et des autorisations de la base de données source.	DBA
Cartographier les utilisateurs.	Mappez les utilisateurs de base de données existants aux nouveaux utilisateurs de base de données.	Propriétaire de l'application
Créez des utilisateurs.	Créez des utilisateurs dans la base de données cible.	DBA, propriétaire de l'application
Appliquez des rôles.	Appliquez les rôles de l'étape précédente à la base de données cible.	DBA
Vérifiez les options, les paramètres, les fichiers réseau et les liens de base de données.	Passez en revue les options, les paramètres, les fichiers réseau et les liens de base de données dans la base de données source, puis évaluez leur applicabilité à la base de données cible.	DBA
Appliquez les paramètres.	Appliquez tous les paramètres pertinents à la base de données cible.	DBA

Transférer des objets

Tâche	Description	Compétences requises
Configurez la connectivité AWS SCT.	Configurez la connectiv ité AWS SCT à la base de données cible.	DBA
Convertissez le schéma à l'aide d'AWS SCT.	AWS SCT convertit automatiq uement le schéma de base de données source et la majeure partie du code personnalisé dans un format compatibl e avec la base de données cible. Tout code que l'outil ne peut pas convertir automatiq uement est clairement marqué afin que vous puissiez le convertir manuellement.	DBA
Passez en revue le rapport.	Passez en revue le rapport SQL généré et enregistrez les erreurs et les avertissements éventuels.	DBA
Appliquez des modifications de schéma automatisées.	Appliquez des modifications de schéma automatisées à la base de données cible ou enregistrez-les sous forme de fichier .sql.	DBA
Validez les objets.	Vérifiez qu'AWS SCT a créé les objets sur la cible.	DBA
Gérez les éléments qui n'ont pas été convertis.	Réécrivez, rejetez ou redessinez manuellement les éléments qui n'ont pas pu être convertis automatiquement.	DBA, propriétaire de l'applica tion

Tâche	Description	Compétences requises
Appliquez les autorisations des rôles et des utilisateurs.	Appliquez le rôle et les autorisations utilisateur générés et passez en revue les exceptions.	DBA

Migrer les données

Tâche	Description	Compétences requises
Déterminez la méthode.	Déterminez la méthode de migration des données.	DBA
Créez une instance de réplication.	Créez une instance de réplication depuis la console AWS DMS. Pour plus d'informations, consultez la section Utilisation d'une instance de réplication AWS DMS dans la documentation AWS DMS.	DBA
Créez les points de terminaison source et cible.	Pour créer des points de terminaison, suivez les instructions de la section Création de points de terminaison source et cible dans la documentation AWS DMS.	DBA
Créez une tâche de réplication.	Pour créer une tâche, consultez la section Utilisation des tâches AWS DMS dans la documentation AWS DMS.	DBA

Tâche	Description	Compétences requises
Lancez la tâche de réplication et surveillez les journaux.	Pour plus d'informations sur cette étape, consultez la section Surveillance des tâches AWS DMS dans la documentation AWS DMS.	DBA

Migrer l'application

Tâche	Description	Compétences requises
Analysez et convertissez les éléments SQL dans le code de l'application.	Utilisez AWS SCT pour analyser et convertir les éléments SQL du code de l'application. Lorsque vous convertissez votre schéma de base de données à partir d'un moteur à un autre, vous devez également mettre à jour le code SQL dans vos applications pour interagir avec le nouveau moteur de base de données au lieu de l'ancien. Vous pouvez afficher, analyser, modifier et enregistr er le code SQL converti.	Propriétaire de l'application
Créez des serveurs d'applica tions.	Créez les nouveaux serveurs d'applications sur AWS.	Propriétaire de l'application
Migrez le code de l'application.	Migrez le code de l'application vers les nouveaux serveurs.	Propriétaire de l'application

Tâche	Description	Compétences requises
Configurez les serveurs d'applications.	Configurez les serveurs d'applications pour la base de données cible et les pilotes.	Propriétaire de l'application
Corrigez le code.	Corrigez tout code spécifiqu e au moteur de base de données source de votre application.	Propriétaire de l'application
Optimisez le code.	Optimisez le code de votre application pour le moteur de base de données cible.	Propriétaire de l'application

Découper

Tâche	Description	Compétences requises
Passez à la base de données cible.	Effectuez le transfert vers la nouvelle base de données.	DBA
Verrouillez l'application.	Empêchez toute autre modification de l'application.	Propriétaire de l'application
Validez les modifications.	Vérifiez que toutes les modifications ont été propagées à la base de données cible.	DBA
Redirige vers la base de données cible.	Dirigez les nouveaux serveurs d'applications vers la base de données cible.	Propriétaire de l'application
Vérifiez tout.	Effectuez une dernière vérification complète du système.	Propriétaire de l'application

Tâche	Description	Compétences requises
Passez en direct.	Effectuez les dernières tâches de transition.	Propriétaire de l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources temporaires.	Arrêtez les ressources AWS temporaires telles que l'instance de réplication AWS DMS et l' EC2 instance utilisée pour AWS SCT.	DBA, propriétaire de l'application
Mettez à jour les commentaires.	Mettez à jour les commentaires sur le processus AWS DMS destinés aux équipes internes.	DBA, propriétaire de l'application
Réviser le processus et les modèles.	Révisez le processus AWS DMS et améliorez le modèle si nécessaire.	DBA, propriétaire de l'application
Validez les documents.	Passez en revue et validez les documents du projet.	DBA, propriétaire de l'application
Collectez des statistiques.	Collectez des indicateurs pour évaluer le temps nécessaire à la migration, le pourcentage d'économies réalisées manuellement par rapport aux coûts liés aux outils, etc.	DBA, propriétaire de l'application
Fermez le projet.	Clôturez le projet de migration et faites part de vos	DBA, propriétaire de l'application

Tâche	Description	Compétences requises
	commentaires aux parties prenantes.	

Ressources connexes

Références

- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Utilisation d'une base de données PostgreSQL comme cible pour AWS Database Migration Service
- Manuel de migration d'une base de données Oracle 11g/12c vers Amazon Aurora compatible avec PostgreSQL (9.6.x)
- Manuel de migration d'Oracle Database 19c vers Amazon Aurora avec compatibilité avec PostgreSQL (12.4)
- Migration d'une base de données Amazon RDS for Oracle vers une édition compatible avec Amazon Aurora PostgreSQL
- Service de migration de données AWS
- Outil de conversion de schéma AWS
- Migrer d'Oracle vers Amazon Aurora
- Tarification d’Amazon RDS

Tutoriels et vidéos

- Tutoriels de migration de base de Step-by-Step données
- Commencer à utiliser AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)
- Service de migration de données AWS (vidéo)
- Migration d'une base de données Oracle vers PostgreSQL (vidéo)

Informations supplémentaires

.

Migrer les données d'une base de données Oracle sur site vers Aurora PostgreSQL

Créée par Michelle Deng (AWS) et Shunan Xiang (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration des données d'une base de données Oracle sur site vers une édition compatible avec Amazon Aurora PostgreSQL. Il cible une stratégie de migration des données en ligne avec un minimum de temps d'arrêt pour les bases de données Oracle de plusieurs téraoctets contenant de grandes tables impliquant des activités de langage de manipulation de données (DML) élevées. Une base de données de secours Oracle Active Data Guard est utilisée comme source pour décharger la migration des données depuis la base de données principale. La réplication de la base de données principale Oracle vers la base de données de secours peut être suspendue pendant le chargement complet afin d'éviter les erreurs ORA-01555.

Les colonnes de table contenant des clés primaires (PKs) ou des clés étrangères (FKs), avec le type de données NUMBER, sont couramment utilisées pour stocker des entiers dans Oracle. Nous vous recommandons de les convertir en INT ou BIGINT dans PostgreSQL pour de meilleures performances. Vous pouvez utiliser l'AWS Schema Conversion Tool (AWS SCT) pour modifier le mappage des types de données par défaut pour les colonnes PK et FK. (Pour plus d'informations, consultez le billet de blog AWS Convert the NUMBER type de données Oracle to PostgreSQL.) La migration des données selon ce modèle utilise AWS Database Migration Service (AWS DMS) à la fois pour le chargement complet et la capture des données modifiées (CDC).

Vous pouvez également utiliser ce modèle pour migrer une base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour PostgreSQL, ou une base de données Oracle hébergée sur Amazon Elastic Compute Cloud (Amazon) vers EC2 Amazon RDS for PostgreSQL ou Aurora PostgreSQL compatible.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source Oracle dans un centre de données sur site avec Active Data Guard en mode veille configuré
- AWS Direct Connect configuré entre le centre de données sur site et le cloud AWS
- Connaissance de l'utilisation d'une base de données Oracle comme source pour AWS DMS
- Connaissance de l'utilisation d'une base de données PostgreSQL comme cible pour AWS DMS

Limites

- Les clusters de base de données Amazon Aurora peuvent être créés avec jusqu'à 128 TiB de stockage. Les instances de base de données Amazon RDS for PostgreSQL peuvent être créées avec jusqu'à 64 TiB de stockage. Pour obtenir les dernières informations sur le stockage, consultez les sections Stockage et fiabilité Amazon Aurora et Amazon RDS DB instance Storage dans la documentation AWS.

Versions du produit

- AWS DMS prend en charge toutes les éditions de base de données Oracle pour les versions 10.2 et ultérieures (pour les versions 10.x), 11g et versions supérieures à 12.2, 18c et 19c. Pour obtenir la dernière liste des versions prises en charge, consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS dans la documentation AWS.

Architecture

Pile technologique source

- Bases de données Oracle sur site avec configuration de secours Oracle Active Data Guard

Pile technologique cible

- Compatible avec Aurora avec PostgreSQL

Architecture de migration des données

Outils

- AWS DMS - AWS Database Migration Service (AWS DMS) prend en charge plusieurs bases de données sources et cibles. Consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS dans la documentation AWS DMS pour obtenir la liste des versions et éditions de base de données source et cible Oracle prises en charge. Si la base de données source n'est pas prise en charge par AWS DMS, vous devez sélectionner une autre méthode pour migrer les données dans la phase 6 (dans la section Epics). Remarque importante : comme il s'agit d'une migration hétérogène, vous devez d'abord vérifier si la base de données prend en charge une application commerciale off-the-shelf (COTS). Si l'application est COTS, consultez le

fournisseur pour vérifier que la compatibilité avec Aurora PostgreSQL est prise en charge avant de continuer. Pour plus d'informations, consultez les procédures pas à pas de Step-by-Step migration vers AWS DMS dans la documentation AWS.

- AWS SCT - L'AWS Schema Conversion Tool (AWS SCT) facilite les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible. Le code personnalisé converti par l'outil inclut les vues, les procédures stockées et les fonctions. Tout code que l'outil ne peut pas convertir automatiquement est clairement indiqué afin que vous puissiez le convertir vous-même.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.		DBA
Installez AWS SCT et ses pilotes.		DBA
Ajoutez et validez les utilisateurs prérequis d'AWS SCT et la base de données des sources de subventions.		DBA
Créez un projet AWS SCT pour la charge de travail et connectez-vous à la base de données source.		DBA
Générez un rapport d'évaluation et évaluez la faisabilité.		DBA, propriétaire de l'application

Préparation de la base de données cible

Tâche	Description	Compétences requises
Créez une base de données cible compatible avec Aurora PostgreSQL.		DBA
Extrayez la liste des utilisateurs, des rôles et des autorisations de la base de données source.		DBA
Mappez les utilisateurs de base de données existants aux nouveaux utilisateurs de base de données.		Propriétaire de l'application
Créez des utilisateurs dans la base de données cible.		DBA
Appliquez les rôles de l'étape précédente à la base de données cible compatible Aurora PostgreSQL.		DBA
Passez en revue les options de base de données, les paramètres, les fichiers réseau et les liens de base de données depuis la base de données source, et évaluez leur applicabilité à la base de données cible.		DBA, propriétaire de l'application
Appliquez tous les paramètres pertinents à la base de données cible.		DBA

Préparation à la conversion du code objet de la base de données

Tâche	Description	Compétences requises
Configurez la connectivité AWS SCT à la base de données cible.		DBA
Convertissez le schéma dans AWS SCT et enregistrez le code converti dans un fichier .sql.		DBA, propriétaire de l'application
Convertissez manuellement tous les objets de base de données qui n'ont pas pu être convertis automatiquement.		DBA, propriétaire de l'application
Optimisez la conversion du code de base de données.		DBA, propriétaire de l'application
Séparez le fichier .sql en plusieurs fichiers .sql en fonction du type d'objet.		DBA, propriétaire de l'application
Validez les scripts SQL dans la base de données cible.		DBA, propriétaire de l'application

Préparation à la migration des données

Tâche	Description	Compétences requises
Créez une instance de réplication AWS DMS.		DBA
Créez les points de terminaison source et cible.	Si le type de données du PKs et FKs est converti de NUMBER dans Oracle en	DBA

Tâche	Description	Compétences requises
	BIGINT dans PostgreSQL, pensez à spécifier l'`numberDataTypeScale=-2` attribut de connexion lorsque vous créez le point de terminaison source.	

Migrer les données — chargement complet

Tâche	Description	Compétences requises
Créez le schéma et les tables dans la base de données cible.		DBA
Créez des tâches à chargement complet AWS DMS en regroupant les tables ou en divisant une grande table en fonction de la taille de la table.		DBA
Arrêtez les applications sur les bases de données Oracle sources pendant une courte période.		Propriétaire de l'application
Vérifiez que la base de données de secours Oracle est synchrone avec la base de données principale et arrêtez la réplication de la base de données principale vers la base de données de secours.		DBA, propriétaire de l'application

Tâche	Description	Compétences requises
Démarrez les applications sur la base de données Oracle source.		Propriétaire de l'application
Démarrez les tâches de chargement complet d'AWS DMS en parallèle depuis la base de données de secours Oracle vers la base de données compatible Aurora PostgreSQL.		DBA
Créez PKs des index secondaires une fois le chargement complet terminé.		DBA
Validez les données.		DBA

Migrer les données — CDC

Tâche	Description	Compétences requises
Créez des tâches de réplication continues AWS DMS en spécifiant une heure de début CDC ou un numéro de modification du système (SCN) personnalisé lorsque le serveur de secours Oracle a été synchronisé avec la base de données principale et avant le redémarrage des applications lors de la tâche précédente.		DBA

Tâche	Description	Compétences requises
Démarrez des tâches AWS DMS en parallèle pour répliquer les modifications en cours depuis la base de données de secours Oracle vers la base de données compatible Aurora PostgreSQL.		DBA
Rétablissez la réplication de la base de données principale Oracle vers la base de données de secours.		DBA
Surveillez les journaux et arrêtez les applications sur la base de données Oracle lorsque la base de données cible compatible Aurora PostgreSQL est presque synchrone avec la base de données Oracle source.		DBA, propriétaire de l'application
Arrêtez les tâches AWS DMS lorsque la cible est entièrement synchronisée avec la base de données Oracle source.		DBA
Créez FKs et validez les données dans la base de données cible.		DBA

Tâche	Description	Compétences requises
Créez des fonctions, des vues, des déclencheurs, des séquences et d'autres types d'objets dans la base de données cible.		DBA
Appliquez des attributions de rôles dans la base de données cible.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Utilisez AWS SCT pour analyser et convertir les instructions SQL contenues dans le code de l'application.		Propriétaire de l'application
Créez de nouveaux serveurs d'applications sur AWS.		Propriétaire de l'application
Migrez le code de l'application vers les nouveaux serveurs.		Propriétaire de l'application
Configurez le serveur d'applications pour la base de données cible et les pilotes.		Propriétaire de l'application
Corrigez tout code spécifique au moteur de base de données source de l'application.		Propriétaire de l'application

Tâche	Description	Compétences requises
Optimisez le code de l'application pour la base de données cible.		Propriétaire de l'application

Découper

Tâche	Description	Compétences requises
Pointez le nouveau serveur d'applications vers la base de données cible.		DBA, propriétaire de l'application
Effectuez des contrôles de santé mentale.		DBA, propriétaire de l'application
Passez en direct.		DBA, propriétaire de l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, administrateur système
Passez en revue et validez les documents du projet.		DBA, propriétaire de l'application
Collectez des indicateurs concernant le temps de migration, le pourcentage d'utilisation manuelle par rapport à l'utilisation d'outils,		DBA, propriétaire de l'application

Tâche	Description	Compétences requises
les économies de coûts et les données similaires.		
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de l'application

Ressources connexes

Références

- Compatible avec Oracle Database vers Aurora PostgreSQL : manuel de migration
- Migration d'une base de données Amazon RDS for Oracle vers Amazon Aurora MySQL
- Site Web AWS DMS
- Documentation AWS DMS
- Site Web AWS SCT
- Documentation AWS SCT
- Migrer d'Oracle vers Amazon Aurora

Didacticiels

- Commencer à utiliser AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)
- Procédures Step-by-Step pas à pas du service de migration de base de données AWS

Migrez de SAP ASE vers Amazon RDS for SQL Server à l'aide d'AWS DMS

Créée par Amit Kumar (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données SAP Adaptive Server Enterprise (ASE) vers une instance de base de données Amazon Relational Database Service (Amazon RDS) exécutant Microsoft SQL Server. La base de données source peut être située dans un centre de données sur site ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Le modèle utilise AWS Database Migration Service (AWS DMS) pour migrer les données et (éventuellement) des outils d'ingénierie logicielle assistée par ordinateur (CASE) pour convertir le schéma de base de données.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données SAP ASE dans un centre de données sur site ou sur une instance EC2
- Une base de données Amazon RDS for SQL Server cible qui est opérationnelle

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- SAP ASE version 15.7 ou 16.x uniquement. Pour obtenir les dernières informations, consultez la section Utilisation d'une base de données SAP comme source pour AWS DMS.
- Pour les bases de données cibles Amazon RDS, AWS DMS prend en charge les versions de Microsoft SQL Server sur Amazon RDS pour les éditions Enterprise, Standard, Web et Express. Pour obtenir les dernières informations sur les versions prises en charge, consultez la documentation AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.

Architecture

Pile technologique source

- Une base de données SAP ASE sur site ou sur une EC2 instance Amazon

Pile technologique cible

- Une instance de base de données Amazon RDS pour SQL Server

Architecture source et cible

D'une base de données SAP ASE sur Amazon EC2 à une instance de base de données Amazon RDS for SQL Server :

D'une base de données SAP ASE sur site à une instance de base de données Amazon RDS for SQL Server :

Outils

- AWS Database Migration Service (AWS DMS) est un service Web que vous pouvez utiliser pour migrer les données de votre base de données sur site, sur une instance de base de données Amazon RDS ou d'une base de données sur une EC2 instance, vers une base de données sur un service AWS tel qu'Amazon RDS for SQL Server ou une instance. EC2 Vous pouvez également migrer une base de données d'un service AWS vers une base de données sur site. Vous pouvez migrer des données entre des moteurs de base de données hétérogènes ou homogènes.
- Pour les conversions de schéma, vous pouvez éventuellement utiliser Erwin Data Modeler ou SAP. PowerDesigner

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.		DBA

Tâche	Description	Compétences requises
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d'instanc e approprié en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin
Identifiez la stratégie de migration des applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		SysAdmin
Créez des groupes de sécurité et des listes de contrôle d'accès au réseau (ACLs).		SysAdmin
Configurez et démarrez une instance de base de données Amazon RDS.		SysAdmin

Migrer les données - option 1

Tâche	Description	Compétences requises
Migrez le schéma de base de données manuellement ou utilisez un outil CASE tel que Erwin Data Modeler ou SAP. PowerDesigner		DBA

Migrer les données - option 2

Tâche	Description	Compétences requises
Migrez les données à l'aide d'AWS DMS.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.		DBA, propriétaire de SysAdmin l'application

Découper

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, SysAdmin
Passez en revue et validez les documents du projet.		DBA, propriétaire de SysAdmin l'application
Collectez des indicateurs tels que le temps de migration , le pourcentage de tâches manuelles par rapport aux tâches automatisées et les économies de coûts.		DBA, propriétaire de SysAdmin l'application
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de SysAdmin l'application

Ressources connexes

Références

- Site Web AWS DMS
- Tarification d'Amazon RDS
- Utilisation d'une base de données SAP ASE comme source pour AWS DMS
- Limitations de RDS Custom pour SQL Server

Tutoriels et vidéos

- Commencer à utiliser AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)
- AWS DMS (vidéo)
- Amazon RDS (vidéo)

Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide d'AWS DMS

Créée par Marcelo Fernandes (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide d'AWS Data Migration Service (AWS DMS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Microsoft SQL Server source dans un centre de données sur site
- Conditions préalables remplies pour utiliser une base de données Amazon Redshift comme cible pour AWS DMS, comme indiqué dans la documentation AWS DMS

Versions du produit

- SQL Server 2005-2019, éditions Enterprise, Standard, Workgroup, Developer et Web. Pour obtenir la dernière liste des versions prises en charge, consultez la section Utilisation d'une base de données Microsoft SQL Server comme source pour AWS DMS dans la documentation AWS.

Architecture

Pile technologique source

- Une base de données Microsoft SQL Server sur site

Pile technologique cible

- Amazon Redshift

Architecture de migration des données

Outils

- AWS DMS est un service de migration de données qui prend en charge plusieurs types de bases de données source et cible. Pour plus d'informations sur les versions et éditions de base de données Microsoft SQL Server prises en charge pour une utilisation avec AWS DMS, consultez la section Utilisation d'une base de données Microsoft SQL Server comme source pour AWS DMS dans la documentation AWS DMS. Si AWS DMS ne prend pas en charge votre base de données source, vous devez sélectionner une autre méthode pour la migration des données.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez la version et le moteur de la base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, administrateur système
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, administrateur système
Choisissez le type d'instanc e approprié en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		DBA, administrateur système
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, administrateur système

Tâche	Description	Compétences requises
Identifiez la stratégie de migration des applications.		DBA, propriétaire de l'application, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)	Pour plus d'informations, consultez la section Travailler avec une instance de base de données dans un VPC dans la documentation AWS.	Administrateur de systèmes
Créez des groupes de sécurité.		Administrateur de systèmes
Configurez et démarrez un cluster Amazon Redshift.	Pour plus d'informations, consultez la section Créer un exemple de cluster Amazon Redshift dans la documentation Amazon Redshift.	DBA, administrateur système

Migrer les données

Tâche	Description	Compétences requises
Migrez les données de la base de données Microsoft SQL Server à l'aide d'AWS DMS.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.		DBA, propriétaire de l'application, administrateur système

Découper

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources temporaires.		DBA, administrateur système
Passez en revue et validez les documents du projet.		DBA, propriétaire de l'application, administrateur système
Collectez des indicateurs tels que le temps de migration , le pourcentage de tâches manuelles par rapport aux tâches automatisées et les économies de coûts.		DBA, propriétaire de l'application, administrateur système
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de l'application, administrateur système

Ressources connexes

Références

- Documentation AWS DMS
- Documentation Amazon Redshift
- Tarification d'Amazon Redshift

Tutoriels et vidéos

- Commencer à utiliser AWS DMS
- Commencer à utiliser Amazon Redshift
- Utilisation d'une base de données Amazon Redshift comme cible pour AWS Database Migration Service
- AWS DMS (vidéo)

Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT

Créée par Neha Thakur (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'une base de données source Microsoft SQL Server sur site vers une base de données cible Amazon Redshift à l'aide des agents d'extraction de données AWS Schema Conversion Tool (AWS SCT). Un agent est un programme externe intégré à AWS SCT mais qui effectue la transformation des données ailleurs et qui interagit avec d'autres services AWS en votre nom.

Conditions préalables et limitations

Prérequis

- Base de données source Microsoft SQL Server utilisée pour la charge de travail de l'entrepôt de données dans un centre de données sur site
- Un compte AWS actif

Versions du produit

- Microsoft SQL Server version 2008 ou ultérieure. Pour obtenir la dernière liste des versions prises en charge, consultez la documentation AWS SCT.

Architecture

pile technologique Source

- Une base de données Microsoft SQL Server sur site

pile technologique Target

- Amazon Redshift

Architecture de migration des données

Outils

- AWS Schema Conversion Tool (AWS SCT) gère les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible. Lorsque les bases de données source et cible sont très différentes, vous pouvez utiliser un agent AWS SCT pour effectuer une transformation de données supplémentaire. Pour plus d'informations, consultez la section Migration de données d'un entrepôt de données sur site vers Amazon Redshift dans la documentation AWS.

Bonnes pratiques

- Bonnes pratiques pour AWS SCT
- Bonnes pratiques pour Amazon Redshift

Épopées

Préparation à la migration

Tâche	Description	Compétences requises
Validez les versions et les moteurs de base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, SysAdmin
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d'instance approprié (capacité, fonctionn alités de stockage, fonctionn alités réseau).		DBA, SysAdmin

Tâche	Description	Compétences requises
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin
Choisissez une stratégie de migration d'applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		SysAdmin
Créez des groupes de sécurité.		SysAdmin
Configurez et démarrez le cluster Amazon Redshift.		SysAdmin

Migrer les données

Tâche	Description	Compétences requises
Migrez les données à l'aide des agents d'extraction de données AWS SCT.		DBA

Migrer des applications

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications choisie.		DBA, propriétaire de SysAdmin l'application

Passez à la base de données cible

Tâche	Description	Compétences requises
Faites passer les clients de l'application à la nouvelle infrastructure.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, SysAdmin
Passez en revue et validez les documents du projet.		DBA, propriétaire de SysAdmin l'application
Collectez des indicateurs tels que le temps de migration , le pourcentage de tâches manuelles par rapport aux tâches automatisées et les économies de coûts.		DBA, propriétaire de SysAdmin l'application
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de SysAdmin l'application

Ressources connexes

Références

- Guide de l'utilisateur d'AWS SCT
- Utilisation d'agents d'extraction de données
- Tarification d'Amazon Redshift

Tutoriels et vidéos

- Commencer à utiliser l'outil AWS Schema Conversion Tool
- Commencer à utiliser Amazon Redshift

Migrer une base de données Teradata vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT

Créée par Sergey Dmitriev (AWS)

Récapitulatif

Ce modèle explique les étapes de migration d'une base de données Teradata, utilisée comme entrepôt de données dans un centre de données sur site, vers une base de données Amazon Redshift. Le modèle utilise les agents d'extraction de données AWS Schema Conversion Tool (AWS SCT). Un agent est un programme externe intégré à AWS SCT mais qui effectue la transformation des données ailleurs et qui interagit avec d'autres services AWS en votre nom.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source Teradata dans un centre de données sur site

Versions du produit

- Teradata version 13 et versions ultérieures. Pour obtenir la dernière liste des versions prises en charge, consultez la documentation AWS SCT.

Architecture

Pile technologique source

- Base de données Teradata sur site

Pile technologique cible

- Cluster Amazon Redshift

Architecture de migration des données

Outils

- AWS SCT — AWS Schema Conversion Tool (AWS SCT) gère les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible. Lorsque les bases de données source et cible sont très différentes l'une de l'autre, vous pouvez utiliser un agent AWS SCT pour effectuer une transformation de données supplémentaire. Pour plus d'informations, consultez la section Migration de données d'un entrepôt de données sur site vers Amazon Redshift dans la documentation AWS.

Épopées

Préparation à la migration

Tâche	Description	Compétences requises
Validez les versions et les moteurs de base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, SysAdmin
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d'instance approprié (capacité, fonctionn alités de stockage, fonctionn alités réseau).		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin

Tâche	Description	Compétences requises
Choisissez une stratégie de migration d'applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		SysAdmin
Créez des groupes de sécurité.		SysAdmin
Configurez et démarrez le cluster Amazon Redshift.		SysAdmin

Migrer les données

Tâche	Description	Compétences requises
Migrez les données à l'aide des agents d'extraction de données AWS SCT.	Pour obtenir des informati ons détaillées sur l'utilisation des agents d'extraction de données AWS SCT, consultez les liens dans la section Références et aide.	DBA

Migrer des applications

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications choisie.		DBA, propriétaire de SysAdmin l'application

Passez à la base de données Amazon Redshift cible

Tâche	Description	Compétences requises
Passez des clients d'applica tions à la nouvelle infrastru cture.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, SysAdmin
Passez en revue et validez les documents du projet.		DBA, propriétaire de SysAdmin l'application
Collectez des indicateurs concernant le temps de migration, le pourcentage de tâches manuelles par rapport aux tâches liées aux outils, les économies de coûts, etc.		DBA, propriétaire de SysAdmin l'application
Clôturez le projet et faites part de vos commentaires.		

Ressources connexes

Références

- Guide de l'utilisateur AWS SCT
- Utilisation d'agents d'extraction de données
- Tarification d'Amazon Redshift
- Convertir la fonctionnalité Teradata RESET WHEN en Amazon Redshift SQL (AWS Prescriptive Guidance)
- Convertir la fonctionnalité temporelle Teradata NORMALIZE en Amazon Redshift SQL (AWS Prescriptive Guidance)

Didacticiels

- Commencer à utiliser l'outil AWS Schema Conversion Tool
- Commencer à utiliser Amazon Redshift

Migrer une base de données Vertica sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT

Créée par Sergey Dmitriev (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données Vertica sur site vers un cluster Amazon Redshift à l'aide des agents d'extraction de données AWS Schema Conversion Tool (AWS SCT). Un agent est un programme externe intégré à AWS SCT mais qui effectue la transformation des données ailleurs et qui interagit avec d'autres services AWS en votre nom.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source Vertica utilisée pour la charge de travail de l'entrepôt de données dans un centre de données sur site
- Un cluster cible Amazon Redshift

Versions du produit

- Vertica version 7.2.2 et versions ultérieures. Pour obtenir la dernière liste des versions prises en charge, consultez la documentation AWS SCT.

Architecture

Pile technologique source

- Une base de données Vertica sur site

Pile technologique cible

- Un cluster Amazon Redshift

Architecture de migration des données

Outils

- AWS Schema Conversion Tool (AWS SCT) gère les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible. Lorsque les bases de données source et cible sont très différentes l'une de l'autre, vous pouvez utiliser un agent AWS SCT pour effectuer une transformation de données supplémentaire. Pour plus d'informations, consultez la section Migration de données d'un entrepôt de données sur site vers Amazon Redshift dans la documentation AWS.

Épopées

Préparation à la migration

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.		DBA
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d'instance approprié (capacité, fonctionn alités de stockage, fonctionn alités réseau).		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin
Choisissez une stratégie de migration d'applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		SysAdmin
Créez des groupes de sécurité.		SysAdmin
Configurez et démarrez un cluster Amazon Redshift.		SysAdmin

Migrer les données

Tâche	Description	Compétences requises
Migrez les données à l'aide des agents d'extraction de données AWS SCT.	Pour obtenir des informati ons détaillées sur l'utilisation des agents d'extraction de données AWS SCT, consultez les liens dans la section Références et aide.	DBA

Migrer des applications

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications choisie.		DBA, propriétaire de SysAdmin l'application

Passez à la base de données cible

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, SysAdmin
Passez en revue et validez les documents du projet.		DBA, propriétaire de SysAdmin l'application
Collectez des indicateurs sur le temps de migration , le pourcentage de tâches manuelles par rapport aux tâches liées aux outils, les économies de coûts, etc.		DBA, propriétaire de SysAdmin l'application
Clôturez le projet et faites part de vos commentaires.		

Ressources connexes

Références

- Guide de l'utilisateur d'AWS SCT
- Utilisation d'agents d'extraction de données
- Tarification d'Amazon Redshift

Tutoriels et vidéos

- Commencer à utiliser l'outil AWS Schema Conversion Tool
- Commencer à utiliser Amazon Redshift

Migrer les applications existantes d'Oracle Pro*C vers ECPG

Créée par Sai Parthasaradhi (AWS) et Mahesh Balumuri (AWS)

Récapitulatif

La plupart des applications existantes qui intègrent du code SQL utilisent le précompilateur Oracle Pro*C pour accéder à la base de données. Lorsque vous migrez ces bases de données Oracle vers Amazon Relational Database Service (Amazon RDS) pour PostgreSQL ou Amazon Aurora PostgreSQL Compatible Edition, vous devez convertir le code de votre application dans un format compatible avec le précompilateur de PostgreSQL, appelé ECPG. Ce modèle décrit comment convertir le code Oracle Pro*C en son équivalent dans PostgreSQL ECPG.

Pour plus d'informations sur Pro*C, consultez la documentation Oracle. Pour une brève introduction à l'ECPG, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL
- Une base de données Oracle exécutée sur site

Outils

- Les packages PostgreSQL répertoriés dans la section suivante.
- AWS CLI — L'interface de ligne de commande AWS (AWS CLI) est un outil open source permettant d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande. Avec une configuration minimale, vous pouvez exécuter des commandes de l'interface de ligne de commande AWS qui mettent en œuvre des fonctionnalités équivalentes à celles fournies par la console de gestion AWS basée sur un navigateur à partir d'une invite de commande.

Épopées

Définissez l'environnement de génération sur CentOS ou RHEL

Tâche	Description	Compétences requises

Installez les packages PostgreSQL.	Installez les packages PostgreSQL requis à l'aide des commandes suivantes.
	`yum update -y`
	`yum install -y yum-utils`
	`rpm -ivh https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm`
	`dnf -qy module disable postgresql`
		Développeur d'applications, DevOps ingénieur

Installez les fichiers d'en-tête et les bibliothèques.	Installez le `postgresql12-devel` package, qui contient les fichiers d'en-tête et les bibliothèques, à l'aide des commandes suivantes. Installez le package dans les environnements de développement et d'exécution pour éviter les erreurs dans l'environnement d'exécution.
	`dnf -y install postgresql12-devel`
	`yum install ncompress zip ghostscript jq unzip wget git -y`
		Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises

	Pour l'environnement de développement uniquement, exécutez également les commandes suivantes.
	`yum install zlib-devel make -y`
	`ln -s /usr/pgsql-12/bin/ecpg /usr/bin/`	

Configurez la variable de chemin d'environnement.	Définissez le chemin d'environnement pour les bibliothèques clientes PostgreSQL. `export PATH=$PATH:/usr/pgsql-12/bin`	Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises

Installez des logiciels supplémentaires si nécessaire.	Si nécessaire, installez pgLoader en remplacement de SQL*Loader dans Oracle.
	`wget -O /etc/yum.repos.d/pgloader-ccl.repo https://dl.packager.io/srv/opf/pgloader-ccl/master/installer/el/7.repo`
	`yum install pgloader-ccl -y`
	`ln -s /opt/pgloader-ccl/bin/pgloader /usr/bin/`
	Si vous appelez des applications Java à partir de modules Pro*C, installez Java.
	`yum install java -y`
	Installez ant pour compiler le code Java.
	`yum install ant -y`
		Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises

Installez l'AWS CLI.	Installez l'interface de ligne de commande AWS pour exécuter des commandes afin d'interagir avec les services AWS tels qu'AWS Secrets Manager et Amazon Simple Storage Service (Amazon S3) depuis vos applications.
	`cd /tmp/`
	`curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`./aws/install -i /usr/local/aws-cli -b /usr/local/bin --update`
		Développeur d'applications, DevOps ingénieur

Identifiez les programmes à convertir.	Identifiez les applications que vous souhaitez convertir de Pro*C en ECPG.	Développeur d'applications, propriétaire de l'application

Convertir le code Pro*C en ECPG

Tâche	Description	Compétences requises
Supprimez les en-têtes indésirables.	Supprimez `include` les en-têtes qui ne sont pas obligatoires dans PostgreSQL, tels que`oci.h`, et. `oratypes` `sqlda`	Propriétaire de l'application, développeur de l'application
Mettez à jour les déclarations de variables.	Ajoutez `EXEC SQL` des instructions pour toutes les	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	déclarations de variables utilisées comme variables hôtes. Supprimez les `EXEC SQL VAR` déclarations telles que les suivantes de votre application. `EXEC SQL VAR query IS STRING(2048);`	

Tâche	Description	Compétences requises

Mettez à jour la fonctionnalité ROWNUM.	La `ROWNUM` fonction n'est pas disponible dans PostgreSQL. Remplacez-la par la fonction de `ROW_NUMBER` fenêtre dans les requêtes SQL.
	
	Code Pro*C :
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME FROM DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2 WHERE ROWNUM <=1 ORDER BY ROWNUM;`
	
	Code ECPG :
	
	`SELECT SUBSTR(RT RIM(FILE_NAME,'.tx t'),12) INTO :gcpclFil eseq FROM (SELECT FILE_NAME , ROW_NUMBE R() OVER (ORDER BY FILE_NAME DESC) AS ROWNUM FROM demo_sche ma.DEMO_FILES_TABLE WHERE FILE_NAME LIKE '%POC%' ORDER BY FILE_NAME DESC) FL2`
		Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	`WHERE ROWNUM <=1 ORDER BY ROWNUM;`	

Mettez à jour les paramètres de la fonction pour utiliser des variables d'alias.	Dans PostgreSQL, les paramètres des fonctions ne peuvent pas être utilisés comme variables hôtes. Remplacez-les en utilisant une variable d'alias.
	
	Code Pro*C :
	
	`int processData(int referenceId){ EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
	
	Code ECPG :
	
	`int processData(int referenceIdParam){ EXEC SQL int referenceId = referenceIdParam; EXEC SQL char col_val[100]; EXEC SQL select column_name INTO :col_val from table_name where col=:referenceId; }`
		Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
Mettez à jour les types de structure.	Définissez les `struct` types `EXEC SQL BEGIN` et les `END` blocs avec `typedef` si les variables `struct` de type sont utilisées comme variables hôtes. Si les `struct` types sont définis dans des fichiers d'en-tête (`.h`), incluez les fichiers avec des instructions `EXEC SQL include`. Code Pro*C : Fichier d'en-tête (`demo.h`) `struct s_partiti on_ranges { char sc_table_ group[31]; char sc_table_ name[31]; char sc_range_ value[10]; }; struct s_partiti on_ranges_ind { short ss_table_ group; short ss_table_ name; short ss_range_ value; };` Code ECPG : Fichier d'en-tête (`demo.h`)	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises

```
EXEC SQL BEGIN DECLARE
 SECTION;
typedef struct
{
  char   sc_table_
group[31];
  char   sc_table_
name[31];
  char   sc_range_
value[10];
} s_partition_ranges;
typedef struct
{
  short    ss_table_
group;
  short    ss_table_
name;
  short    ss_range_
value;
} s_partition_ranges
_ind;
EXEC SQL END DECLARE
 SECTION;
```

Fichier Pro*C () `demo.pc`

```
#include "demo.h"
struct s_partiti
on_ranges gc_partit
ion_data[MAX_PART_
TABLE] ;
struct s_partiti
on_ranges_ind
 gc_partition_data_
ind[MAX_PART_TABLE] ;
```

Fichier ECPG () `demo.pc`

```
exec sql include
 "demo.h"
```

Tâche	Description	Compétences requises
	`EXEC SQL BEGIN DECLARE SECTION; s_partition_ranges gc_partition_data[ MAX_PART_TABLE] ; s_partition_ranges_ind gc_partition_data_ ind[MAX_PART_TABLE] ; EXEC SQL END DECLARE SECTION;`	

Modifiez la logique à récupérer à partir des curseurs.	Pour récupérer plusieurs lignes à partir de curseurs à l'aide de variables de tableau, modifiez le code à utiliser. `FETCH FORWARD`
	
	Code Pro*C :
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL FETCH filename_ cursor into :aPoeFile s;`
	
	Code ECPG :
	
	`EXEC SQL char aPoeFiles [MAX_FILES][FILENA ME_LENGTH]; EXEC SQL int fetchSize = MAX_FILES; EXEC SQL FETCH FORWARD :fetchSiz e filename_cursor into :aPoeFiles;`
		Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises

Modifiez les appels de packages qui n'ont pas de valeur de retour.	Les fonctions de package Oracle qui n'ont pas de valeurs de retour doivent être appelées avec une variable indicatrice. Si votre application inclut plusieurs fonctions portant le même nom ou si les fonctions de type inconnu génèrent des erreurs d'exécution, transformez les valeurs en types de données.
	
	Code Pro*C :
	
	`void ProcessData (char *data , int id) { EXEC SQL EXECUTE BEGIN pkg_demo. process_data (:data, :id); END; END-EXEC; }`
	
	Code ECPG :
	
	`void ProcessData (char *dataParam, int idParam ) { EXEC SQL char *data = dataParam;`
		Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises

	`EXEC SQL int id = idParam;`
	`EXEC SQL short rowInd;`
	`EXEC SQL short rowInd = 0;`
	`EXEC SQL SELECT pkg_demo.process_data (`
	`inp_data => :data::text,`
	`inp_id => :id )`
	`INTO :rowInd;`
	`}`	

Tâche	Description	Compétences requises

Réécrivez les variables SQL_CURSOR.	Réécrivez la SQL_CURSOR variable et son implément ation.
	
	Code Pro*C :
	
	`/* SQL Cursor */ SQL_CU RSOR demo_cursor; EXEC SQL ALLOCATE :demo_cursor; EXEC SQL EXECUTE BEGIN pkg_demo. get_cursor( demo_cur= >:demo_cursor ); END; END-EXEC;`
	
	Code ECPG :
	
	`EXEC SQL DECLARE demo_cursor CURSOR FOR SELECT * from pkg_demo.open_file name_rc( demo_cur= >refcursor ) ; EXEC SQL char open_file name_rcInd[100]; # As the below function returns cursor_name as # return we need to use char[] type as indicator.`
		Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	`EXEC SQL SELECT pkg_demo.get_cursor ( demo_cur=>'demo_cursor' ) INTO :open_filename_rcInd;`	

Tâche	Description	Compétences requises
Appliquez des modèles de migration courants.	• Modifiez les requêtes SQL afin qu'elles soient compatibles avec PostgreSQL. • Déplacez les blocs anonymes, lorsqu'ils ne sont pas pris en charge dans ECPG, vers la base de données. • Supprimez `dbms_application_info` la logique, qui n'est pas prise en charge par PostgreSQL. • Déplace `EXEC SQL COMMIT` les instructions après la fermeture du curseur. Si vous validez des requêtes alors que vous êtes dans la boucle pour récupérer les enregistrements à partir du curseur, le curseur est fermé et un message d'erreur indiquant que le curseur n'existe pas s'affiche. • Pour plus d'informations sur la gestion des exceptions dans ECPG et des codes d'erreur, consultez la section Gestion des erreurs dans la documentation de PostgreSQL.	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
Activez le débogage, si nécessaire.	Pour exécuter le programme ECPG en mode debug, ajoutez la commande suivante dans le bloc fonctionnel principal. `ECPGdebug(1, stderr);`	Développeur d'applications, propriétaire de l'application

Compiler des programmes ECPG

Tâche	Description	Compétences requises

Créez un fichier exécutable pour ECPG.	Si vous avez nommé un fichier source Embedded SQL C`prog1.pgc` , vous pouvez créer un programme exécutable à l'aide de la séquence de commandes suivante.
	`ecpg prog1.pgc`
	`cc -I/usr/local/pgsql/include -c prog1.c`
	`cc -o prog1 prog1.o -L/usr/local/pgsql/lib -lecpg`
		Développeur d'applications, propriétaire de l'application

Créez un fichier make pour la compilation.	Créez un fichier make pour compiler le programme ECPG, comme indiqué dans l'exemple de fichier suivant. `CFLAGS ::= $(CFLAGS) -I/usr/pgsql-12/include -g -Wall`	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises

	`LDFLAGS ::= $(LDFLAGS) -L/usr/pgsql-12/lib -Wl,-rpath,/usr/pgsql-12/lib`
	`LDLIBS ::= $(LDLIBS) -lecpg`
	`PROGRAMS = test`
	`.PHONY: all clean`
	`%.c: %.pgc`
	`ecpg $<`
	`all: $(PROGRAMS)`
	`clean:`
	`rm -f $(PROGRAMS) $(PROGRAMS:%=%.c) $(PROGRAMS:%=%.o)`	

Tester l'application

Tâche	Description	Compétences requises
Testez le code.	Testez le code d'application converti pour vous assurer qu'il fonctionne correctement.	Développeur d'applications, propriétaire de l'application, ingénieur de test

Ressources connexes

- ECPG - SQL intégré en C (documentation PostgreSQL)
- Gestion des erreurs (documentation PostgreSQL)
- Pourquoi utiliser le précompilateur Oracle Pro*C/C++ (documentation Oracle)

Informations supplémentaires

PostgreSQL possède un précompilateur SQL intégré, ECPG, équivalent au précompilateur Oracle Pro*C. ECPG convertit les programmes C contenant des instructions SQL intégrées en code C standard en remplaçant les appels SQL par des appels de fonction spéciaux. Les fichiers de sortie peuvent ensuite être traités avec n'importe quelle chaîne d'outils de compilation C.

Fichiers d'entrée et de sortie

ECPG convertit chaque fichier d'entrée que vous spécifiez sur la ligne de commande en fichier de sortie C correspondant. Si le nom d'un fichier d'entrée n'a pas d'extension de fichier, .pgc est supposé. L'extension du fichier est remplacée par `.c` pour construire le nom du fichier de sortie. Cependant, vous pouvez remplacer le nom du fichier de sortie par défaut en utilisant l'`-o`option.

Si vous utilisez un tiret (`-`) comme nom de fichier d'entrée, ECPG lit le programme depuis l'entrée standard et écrit sur la sortie standard, sauf si vous le remplacez en utilisant l'`-o`option.

Fichiers d'en-tête

Lorsque le compilateur PostgreSQL compile les fichiers de code C prétraités, il recherche les fichiers d'en-tête ECPG dans le répertoire PostgreSQL. `include` Par conséquent, vous devrez peut-être utiliser l'`-I`option pour pointer le compilateur vers le bon répertoire (par exemple,`-I/usr/local/pgsql/include`).

Bibliothèques

Les programmes qui utilisent le code C avec Embedded SQL doivent être liés à la `libecpg` bibliothèque. Par exemple, vous pouvez utiliser les options `-L/usr/local/pgsql/lib -lecpg` de l'éditeur de liens.

Les applications ECPG converties appellent des fonctions de la `libpq` bibliothèque via la bibliothèque Embedded SQL (`ecpglib`) et communiquent avec le serveur PostgreSQL en utilisant le protocole frontend/backend standard.

Migrer les colonnes générées virtuellement d'Oracle vers PostgreSQL

Créée par Veeranjaneyulu Grandhi (AWS), Rajesh Madiwale (AWS) et Ramesh Pathuri (AWS)

Récapitulatif

Dans les versions 11 et antérieures, PostgreSQL ne fournit aucune fonctionnalité directement équivalente à une colonne virtuelle Oracle. La gestion des colonnes générées virtuelles lors de la migration d'Oracle Database vers PostgreSQL version 11 ou antérieure est difficile pour deux raisons :

- Les colonnes virtuelles ne sont pas visibles pendant la migration.
- PostgreSQL ne prend pas en charge l'expression avant `generate` la version 12.

Cependant, il existe des solutions pour émuler des fonctionnalités similaires. Lorsque vous utilisez AWS Database Migration Service (AWS DMS) pour migrer des données d'Oracle Database vers PostgreSQL version 11 ou antérieure, vous pouvez utiliser des fonctions de déclenchement pour renseigner les valeurs dans les colonnes générées virtuellement. Ce modèle fournit des exemples de code Oracle Database et PostgreSQL que vous pouvez utiliser à cette fin. Sur AWS, vous pouvez utiliser Amazon Relational Database Service (Amazon RDS) pour PostgreSQL ou Amazon Aurora PostgreSQL Compatible Edition pour votre base de données PostgreSQL.

À partir de la version 12 de PostgreSQL, les colonnes générées sont prises en charge. Les colonnes générées peuvent être calculées à partir d'autres valeurs de colonne à la volée ou calculées et stockées. Les colonnes générées par PostgreSQL sont similaires aux colonnes virtuelles Oracle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle source
- Bases de données PostgreSQL cibles (sur Amazon RDS for PostgreSQL ou compatible avec Aurora PostgreSQL)
- Expertise en codage PL/pgSQL

Limites

- S'applique uniquement aux versions de PostgreSQL antérieures à la version 12.
- S'applique à la version 11g ou ultérieure d'Oracle Database.
- Les colonnes virtuelles ne sont pas prises en charge dans les outils de migration de données.
- S'applique uniquement aux colonnes définies dans le même tableau.
- Si une colonne générée virtuelle fait référence à une fonction déterministe définie par l'utilisateur, elle ne peut pas être utilisée comme colonne clé de partitionnement.
- La sortie de l'expression doit être une valeur scalaire. Il ne peut pas renvoyer un type de données fourni par Oracle, un type défini par l'utilisateur, `LOB` ou. `LONG RAW`
- Les index définis par rapport à des colonnes virtuelles sont équivalents aux index basés sur des fonctions dans PostgreSQL.
- Les statistiques du tableau doivent être collectées.

Outils

- pgAdmin 4 est un outil de gestion open source pour PostgreSQL. Cet outil fournit une interface graphique qui simplifie la création, la maintenance et l'utilisation des objets de base de données.
- Oracle SQL Developer est un environnement de développement intégré gratuit permettant de travailler avec SQL dans les bases de données Oracle dans le cadre de déploiements traditionnels et dans le cloud.

Épopées

Création de tables de base de données source et cible

Tâche	Description	Compétences requises
Créez une table de base de données Oracle source.	Dans Oracle Database, créez une table avec des colonnes générées virtuellement à l'aide de l'instruction suivante. `CREATE TABLE test.generated_column ( CODE NUMBER, STATUS VARCHAR2(12) DEFAULT 'PreOpen',`	DBA, développeur d'applications

Tâche	Description	Compétences requises

	<pre>FLAG CHAR(1) GENERATED
	ALWAYS AS (CASE
	UPPER(STATUS) WHEN
	'OPEN' THEN 'N' ELSE
	'Y' END) VIRTUAL
	VISIBLE
	);</pre>
	Dans ce tableau source, les données de la `STATUS` colonne sont migrées via AWS DMS vers la base de données cible. La `FLAG` colonne est toutefois remplie à l'aide de `generate by` fonctionnalités. Elle n'est donc pas visible par AWS DMS pendant la migration. Pour implémenter la fonctionnalité de`generated by`, vous devez utiliser des déclencheurs et des fonctions dans la base de données cible pour renseigner les valeurs de la `FLAG` colonne, comme indiqué dans l'épopée suivante.	

Tâche	Description	Compétences requises
Créez une table PostgreSQL cible sur AWS.	Créez une table PostgreSQL sur AWS à l'aide de l'instruction suivante. `CREATE TABLE test.generated_column ( code integer not null, status character varying(12) not null , flag character(1) );` Dans ce tableau, la `status` colonne est une colonne standard. La `flag` colonne sera une colonne générée en fonction des données qu'elle `status` contient.	DBA, développeur d'applications

Créez une fonction de déclenchement pour gérer la colonne virtuelle dans PostgreSQL

Tâche	Description	Compétences requises
Créez un déclencheur PostgreSQL.	Dans PostgreSQL, créez un déclencheur. `CREATE TRIGGER tgr_gen_column AFTER INSERT OR UPDATE OF status ON test.generated_column FOR EACH ROW`	DBA, développeur d'applications

Tâche	Description	Compétences requises
	`EXECUTE FUNCTION test.tgf_gen_column();`	

Tâche	Description	Compétences requises
Créez une fonction de déclenchement PostgreSQL.	Dans PostgreSQL, créez une fonction pour le déclencheur. Cette fonction remplit une colonne virtuelle insérée ou mise à jour par l'application ou AWS DMS, et valide les données. `CREATE OR REPLACE FUNCTION test.tgf_gen_column() RETURNS trigger AS $VIRTUAL_COL$ BEGIN IF (TG_OP = 'INSERT') THEN IF (NEW.flag IS NOT NULL) THEN RAISE EXCEPTION 'ERROR: cannot insert into column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF (TG_OP = 'UPDATE') THEN IF (NEW.flag::VARCHAR != OLD.flag::varchar) THEN RAISE EXCEPTION 'ERROR: cannot update column "flag"' USING DETAIL = 'Column "flag" is a generated column.'; END IF; END IF; IF TG_OP IN ('INSERT','UPDATE') THEN`	DBA, développeur d'applications

Tâche	Description	Compétences requises
	`IF (old.flag is NULL) OR (coalesce(old.status,'') != coalesce(new.status,'')) THEN UPDATE test.generated_column SET flag = (CASE UPPER(status) WHEN 'OPEN' THEN 'N' ELSE 'Y' END) WHERE code = new.code; END IF; END IF; RETURN NEW; END $VIRTUAL_COL$ LANGUAGE plpgsql;`	

Testez la migration des données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication.	Pour créer une instance de réplication, suivez les instructions de la documentation AWS DMS. L'instance de réplication doit se trouver dans le même cloud privé virtuel (VPC) que vos bases de données source et cible.	DBA, développeur d'applications
Créez des points de terminaison source et cible.	Pour créer les points de terminaison, suivez les instructions de la documentation AWS DMS.	DBA, développeur d'applications

Tâche	Description	Compétences requises
Testez les connexions des terminaux.	Vous pouvez tester les connexions du point de terminaison en spécifiant le VPC et l'instance de réplicati on, puis en choisissant Run test.	DBA, développeur d'applica tions
Créez et lancez une tâche de chargement complet.	Pour obtenir des instructi ons, consultez les sections Création d'une tâche et Chargement complet de la tâche dans la documentation AWS DMS.	DBA, développeur d'applica tions
Validez les données de la colonne virtuelle.	Comparez les données de la colonne virtuelle dans les bases de données source et cible. Vous pouvez valider les données manuellement ou écrire un script pour cette étape.	DBA, développeur d'applica tions

Ressources connexes

- Mise en route avec AWS Database Migration Service (documentation AWS DMS)
- Utilisation d'une base de données Oracle comme source pour AWS DMS (documentation AWS DMS)
- Utilisation d'une base de données PostgreSQL comme cible pour AWS DMS (documentation AWS DMS)
- Colonnes générées dans PostgreSQL (documentation PostgreSQL)
- Fonctions de déclenchement (documentation PostgreSQL)
- Colonnes virtuelles dans la base de données Oracle (documentation Oracle)

Configuration de la fonctionnalité Oracle UTL_FILE sur Aurora compatible avec PostgreSQL

Créée par Rakesh Raghav (AWS) et anuradha chintha (AWS)

Récapitulatif

Dans le cadre de votre migration d'Oracle vers l'édition compatible avec Amazon Aurora PostgreSQL sur le cloud Amazon Web Services (AWS), vous pouvez rencontrer de nombreux défis. Par exemple, la migration de code qui repose sur l'`UTL_FILE`utilitaire Oracle représente toujours un défi. Dans Oracle PL/SQL, le `UTL_FILE` package est utilisé pour les opérations sur les fichiers, telles que la lecture et l'écriture, conjointement avec le système d'exploitation sous-jacent. L'`UTL_FILE`utilitaire fonctionne à la fois pour les serveurs et les ordinateurs clients.

Amazon Aurora PostgreSQL compatible est une offre de base de données gérée. De ce fait, il n'est pas possible d'accéder aux fichiers sur le serveur de base de données. Ce modèle vous explique comment intégrer Amazon Simple Storage Service (Amazon S3) et Amazon Aurora PostgreSQL compatible pour obtenir un sous-ensemble de fonctionnalités. `UTL_FILE` Grâce à cette intégration, nous pouvons créer et consommer des fichiers sans utiliser d'outils ou de services tiers d'extraction, de transformation et de chargement (ETL).

Vous pouvez éventuellement configurer la CloudWatch surveillance Amazon et les notifications Amazon SNS.

Nous vous recommandons de tester minutieusement cette solution avant de l'implémenter dans un environnement de production.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Expertise du service de migration de base de données AWS (AWS DMS)
- Expertise en codage PL/pgSQL
- Un cluster compatible avec Amazon Aurora PostgreSQL
- Compartiment S3

Limites

Ce modèle ne fournit pas les fonctionnalités nécessaires pour remplacer l'`UTL_FILE`utilitaire Oracle. Toutefois, les étapes et les exemples de code peuvent être encore améliorés pour atteindre les objectifs de modernisation de votre base de données.

Versions du produit

- Édition 11.9 compatible avec Amazon Aurora PostgreSQL

Architecture

Pile technologique cible

- Compatible avec Amazon Aurora PostgreSQL
- Amazon CloudWatch
- Amazon Simple Notification Service (Amazon SNS)
- Amazon S3

Architecture cible

Le schéma suivant montre une représentation de haut niveau de la solution.

1. Les fichiers sont chargés depuis l'application dans le compartiment S3.
2. L'`aws_s3`extension accède aux données à l'aide de PL/pgSQL et les télécharge sur Aurora PostgreSQL compatible.

Outils

- Compatible avec Amazon Aurora PostgreSQL — L'édition compatible avec Amazon Aurora PostgreSQL est un moteur de base de données relationnelle entièrement géré, compatible avec PostgreSQL et conforme à l'ACID. Il associe la rapidité et la fiabilité des bases de données commerciales haut de gamme à la rentabilité des bases de données open source.
- AWS CLI — L'interface de ligne de commande AWS (AWS CLI) est un outil unifié permettant de gérer vos services AWS. Avec un seul outil à télécharger et à configurer, vous pouvez contrôler plusieurs services AWS depuis la ligne de commande et les automatiser par le biais de scripts.
- Amazon CloudWatch — Amazon CloudWatch surveille les ressources et l'utilisation d'Amazon S3.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Dans ce modèle, Amazon S3 fournit une couche de stockage pour recevoir et stocker des fichiers destinés à être consommés et transmis vers et depuis le cluster compatible Aurora PostgreSQL.
- aws_s3 — L'`aws_s3`extension intègre la compatibilité avec Amazon S3 et Aurora PostgreSQL.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients. Dans ce modèle, Amazon SNS est utilisé pour envoyer des notifications.
- pgAdmin — pgAdmin est un outil de gestion open source pour Postgres. pgAdmin 4 fournit une interface graphique pour créer, gérer et utiliser des objets de base de données.

Code

Pour obtenir les fonctionnalités requises, le modèle crée plusieurs fonctions avec un nom similaire à`UTL_FILE`. La section Informations supplémentaires contient le code de base de ces fonctions.

Dans le code, remplacez `testaurorabucket` par le nom de votre compartiment S3 de test. `us-east-1`Remplacez-le par la région AWS dans laquelle se trouve votre compartiment S3 de test.

Épopées

Intégrez la compatibilité avec Amazon S3 et Aurora PostgreSQL

Tâche	Description	Compétences requises
Configurez des politiques IAM.	Créez des politiques AWS Identity and Access Management (IAM) qui accordent l'accès au compartiment S3 et aux objets qu'il contient. Pour le code, consultez la section Informati ons supplémentaires.	Administrateur AWS, DBA
Ajoutez des rôles d'accès Amazon S3 à Aurora PostgreSQL.	Créez deux rôles IAM : un rôle pour l'accès en lecture et un rôle pour l'accès en écriture à Amazon S3. Associez	Administrateur AWS, DBA

Tâche	Description	Compétences requises
	les deux rôles au cluster compatible avec Aurora PostgreSQL : • Un rôle pour la fonctionn alité S3Export • Un rôle pour la fonctionn alité S3Import Pour plus d'informations, consultez la documenta tion compatible avec Aurora PostgreSQL sur l'importation et l'exportation de données vers Amazon S3.	

Configurer les extensions dans Aurora PostgreSQL compatible

Tâche	Description	Compétences requises
Créez l'extension aws_commo ns.	L'`aws_commons` extension est une dépendance de l'`aws_s3`extension.	DBA, Développeur
Créez l'extension aws_s3.	L'`aws_s3`extension interagit avec Amazon S3.	DBA, Développeur

Validez l'intégration compatible avec Amazon S3 et Aurora PostgreSQL

Tâche	Description	Compétences requises
Testez l'importation de fichiers depuis Amazon S3 vers Aurora PostgreSQL.	Pour tester l'importation de fichiers dans un environne ment compatible avec Aurora	DBA, Développeur

Tâche	Description	Compétences requises
	PostgreSQL, créez un exemple de fichier CSV et chargez-le dans le compartiment S3. Créez une définition de table basée sur le fichier CSV et chargez le fichier dans le tableau à l'aide de la `aws_s3.table_import_from_s3` fonction.	
Testez l'exportation de fichiers depuis Aurora PostgreSQL vers Amazon S3.	Pour tester l'exportation de fichiers depuis une version compatible avec Aurora PostgreSQL, créez une table de test, remplissez-la de données, puis exportez les données à l'aide de la fonction. `aws_s3.query_export_to_s3`	DBA, Développeur

Pour imiter l'utilitaire UTL_FILE, créez des fonctions wrapper

Tâche	Description	Compétences requises
Créez le schéma utl_file_utility.	Le schéma maintient les fonctions du wrapper ensemble. Pour créer le schéma, exécutez la commande suivante. `CREATE SCHEMA utl_file_utility;`	DBA, Développeur
Créez le type file_type.	Pour créer le `file_type` type, utilisez le code suivant.	DBA/Développeur

Tâche	Description	Compétences requises
	`CREATE TYPE utl_file_utility.file_type AS ( p_path character varying(30), p_file_name character varying );`	
Créez la fonction d'initialisation.	La `init` fonction initialise une variable courante telle que `bucket` ou`region`. Pour le code, consultez la section Informations supplémentaires.	DBA/Développeur
Créez les fonctions du wrapper.	Créez les fonctions du wrapper `fopen`, `put_line`, et. `fclose` Pour le code, consultez la section Informations supplémentaires.	DBA, Développeur

Testez les fonctions du wrapper

Tâche	Description	Compétences requises
Testez les fonctions du wrapper en mode écriture.	Pour tester les fonctions du wrapper en mode écriture, utilisez le code fourni dans la section Informations supplémentaires.	DBA, Développeur
Testez les fonctions du wrapper en mode ajout.	Pour tester les fonctions du wrapper en mode ajout, utilisez le code fourni dans	DBA, Développeur

Tâche	Description	Compétences requises
	la section Informations supplémentaires.	

Ressources connexes

- Intégration avec Amazon S3
- Amazon S3
- Aurora
- Amazon CloudWatch
- Amazon SNS

Informations supplémentaires

Configurer des politiques IAM

Créez les politiques suivantes.

Nom de la politique

S3 IntRead

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
         "arn:aws:s3:::testaurorabuc
ket/*",
         "arn:aws:s3:::testaurorabuc
ket"
            ]
        }
```

```
    ]
}
```

S3 IntWrite

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3integrationtest
",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",

                "s3:ListBucket"
            ],
            "Resource": [
    "arn:aws:s3:::testaurorabucket/
*",                "arn:aws:s3:::test
aurorabucket"
            ]
        }
    ]
}
```

Création de la fonction d'initialisation

Pour initialiser des variables courantes, telles que `bucket` ou`region`, créez la `init` fonction à l'aide du code suivant.

```
CREATE OR REPLACE FUNCTION utl_file_utility.init(
    )
    RETURNS void
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
BEGIN
      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 'region' )
      , 'us-east-1'::text
```

```
      , false );

      perform set_config
      ( format( '%s.%s','UTL_FILE_UTILITY', 's3bucket' )
      , 'testaurorabucket'::text
      , false );
END;
$BODY$;
```

Création des fonctions du wrapper

Créez les fonctions `fopen`, `put_line`, et `fclose` wrapper.

fouvrir

```
CREATE OR REPLACE FUNCTION utl_file_utility.fopen(
    p_file_name character varying,
    p_path character varying,
    p_mode character DEFAULT 'W'::bpchar,
    OUT p_file_type utl_file_utility.file_type)
    RETURNS utl_file_utility.file_type
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
declare
    v_sql character varying;
    v_cnt_stat integer;
    v_cnt integer;
    v_tabname character varying;
    v_filewithpath character varying;
    v_region character varying;
    v_bucket character varying;

BEGIN
    /*initialize common variable */
    PERFORM utl_file_utility.init();
    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    /* set tabname*/
    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
```

```
   v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
concat_ws('/',p_path,p_file_name) end ;
   raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
v_region;

   /* APPEND MODE HANDLING; RETURN EXISTING FILE DETAILS IF PRESENT ELSE CREATE AN
EMPTY FILE */
   IF p_mode = 'A' THEN
       v_sql := concat_ws('','create temp table if not exists ', v_tabname,' (col1
text)');
       execute v_sql;

       begin
       PERFORM aws_s3.table_import_from_s3
           ( v_tabname,
           '',
           'DELIMITER AS ''#''',
           aws_commons.create_s3_uri
           (     v_bucket,
               v_filewithpath ,
               v_region)
           );
       exception
           when others then
            raise notice 'File load issue ,%',sqlerrm;
            raise;
       end;
       execute concat_ws('','select count(*) from ',v_tabname) into v_cnt;

       IF v_cnt > 0
       then
           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       else
           PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
v_region)
                             );

           p_file_type.p_path := p_path;
           p_file_type.p_file_name := p_file_name;
       end if;
       v_sql := concat_ws('','drop table ', v_tabname);
       execute v_sql;
```

```
    ELSEIF p_mode = 'W' THEN
            PERFORM aws_s3.query_export_to_s3('select ''''',
                           aws_commons.create_s3_uri(v_bucket, v_filewithpath,
 v_region)
                             );
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
    END IF;

EXCEPTION
        when others then
            p_file_type.p_path := p_path;
            p_file_type.p_file_name := p_file_name;
            raise notice 'fopenerror,%',sqlerrm;
            raise;
END;
$BODY$;
```

put_line

```
CREATE OR REPLACE FUNCTION utl_file_utility.put_line(
    p_file_name character varying,
    p_path character varying,
    p_line text,
    p_flag character DEFAULT 'W'::bpchar)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
/*****************************************************************
* Write line, p_line in windows format to file, p_fp - with carriage return
* added before new line.
*****************************************************************/
declare
    v_sql varchar;
    v_ins_sql varchar;
    v_cnt INTEGER;
    v_filewithpath character varying;
    v_tabname  character varying;
    v_bucket character varying;
    v_region character varying;
```

```
BEGIN
 PERFORM utl_file_utility.init();

/* check if temp table already exist */

 v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );

 v_sql := concat_ws('','select count(1) FROM pg_catalog.pg_class c LEFT JOIN
 pg_catalog.pg_namespace n ON n.oid = c.relnamespace where n.nspname like ''pg_temp_
%'''
                        ,' AND pg_catalog.pg_table_is_visible(c.oid) AND
 Upper(relname) = Upper( '''
                        ,  v_tabname ,''' ) ');

 execute v_sql into v_cnt;

  IF v_cnt = 0 THEN
         v_sql := concat_ws('','create temp table ',v_tabname,' (col text)');
        execute v_sql;
        /* CHECK IF APPEND MODE */
        IF upper(p_flag) = 'A' THEN
            PERFORM utl_file_utility.init();
            v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 'region' ) );
            v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY',
 's3bucket' ) );

            /* set tabname*/
            v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

            begin
               PERFORM aws_s3.table_import_from_s3
                     ( v_tabname,
                          '',
                       'DELIMITER AS ''#''',
                        aws_commons.create_s3_uri
                           ( v_bucket,
                               v_filewithpath,
                               v_region    )
                    );
            exception
```

```
                when others then
                    raise notice  'Error Message : %',sqlerrm;
                    raise;
            end;
        END IF;
    END IF;
    /* INSERT INTO TEMP TABLE */
    v_ins_sql := concat_ws('','insert into ',v_tabname,' values(''',p_line,''')');
    execute v_ins_sql;
    RETURN TRUE;
    exception
            when others then
                raise notice  'Error Message : %',sqlerrm;
                raise;
END;
$BODY$;
```

fermer

```
CREATE OR REPLACE FUNCTION utl_file_utility.fclose(
    p_file_name character varying,
    p_path character varying)
    RETURNS boolean
    LANGUAGE 'plpgsql'

    COST 100
    VOLATILE
AS $BODY$
DECLARE
    v_filewithpath character varying;
    v_bucket character varying;
    v_region character varying;
    v_tabname character varying;
    v_sql character varying;
BEGIN
      PERFORM utl_file_utility.init();

    v_region := current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 'region' ) );
    v_bucket :=  current_setting( format( '%s.%s', 'UTL_FILE_UTILITY', 's3bucket' ) );

    v_tabname := substring(p_file_name,1,case when strpos(p_file_name,'.') = 0 then
 length(p_file_name) else strpos(p_file_name,'.') - 1 end );
```

```
    v_filewithpath := case when NULLif(p_path,'') is null then p_file_name else
 concat_ws('/',p_path,p_file_name) end ;

    raise notice 'v_bucket %, v_filewithpath % , v_region %', v_bucket,v_filewithpath,
 v_region ;

    /* exporting to s3 */
    perform aws_s3.query_export_to_s3
        (concat_ws('','select * from ',v_tabname,'  order by ctid asc'),
            aws_commons.create_s3_uri(v_bucket, v_filewithpath, v_region)
        );
    v_sql := concat_ws('','drop table ', v_tabname);
    execute v_sql;
    RETURN TRUE;
EXCEPTION
       when others then
     raise notice 'error fclose %',sqlerrm;
     RAISE;
END;
$BODY$;
```

Testez votre configuration et les fonctions du wrapper

Utilisez les blocs de code anonymes suivants pour tester votre configuration.

Tester le mode d'écriture

Le code suivant écrit un fichier nommé `s3inttest` dans le compartiment S3.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'W';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;

select * from
```

```
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Testez le mode d'ajout

Le code suivant ajoute des lignes au `s3inttest` fichier créé lors du test précédent.

```
do $$
declare
l_file_name varchar := 's3inttest' ;
l_path varchar := 'integration_test' ;
l_mode char(1) := 'A';
l_fs utl_file_utility.file_type ;
l_status boolean;

begin
select * from
utl_file_utility.fopen( l_file_name, l_path , l_mode ) into l_fs ;
raise notice 'fopen : l_fs : %', l_fs;


select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket: for
 test purpose : append 1', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from
utl_file_utility.put_line( l_file_name, l_path ,'this is test file:in s3bucket : for
 test purpose : append 2', l_mode ) into l_status ;
raise notice 'put_line : l_status %', l_status;

select * from utl_file_utility.fclose( l_file_name , l_path ) into l_status ;
raise notice 'fclose : l_status %', l_status;

end;
$$
```

Notifications Amazon SNS

Vous pouvez éventuellement configurer la CloudWatch surveillance Amazon et les notifications Amazon SNS sur le compartiment S3. Pour plus d'informations, consultez Surveillance d'Amazon S3 et Configuration des notifications Amazon SNS.

Valider les objets de base de données après la migration d'Oracle vers Amazon Aurora PostgreSQL

Créée par Venkatramana Chintha (AWS) et Eduardo Valentim (AWS)

Récapitulatif

Ce modèle décrit une step-by-step approche permettant de valider des objets après la migration d'une base de données Oracle vers Amazon Aurora PostgreSQL Compatible Edition.

Ce modèle décrit les scénarios d'utilisation et les étapes de validation des objets de base de données ; pour plus d'informations, consultez la section Validation des objets de base de données après la migration à l'aide d'AWS SCT et d'AWS DMS sur le blog de base de données AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Base de données Oracle sur site qui a été migrée vers une base de données compatible Aurora PostgreSQL.
- Identifiants de connexion auxquels s'applique la RDSData FullAccess politique Amazon, pour la base de données compatible Aurora PostgreSQL.
- Ce modèle utilise l'éditeur de requêtes pour les clusters de base de données Aurora Serverless, disponible dans la console Amazon Relational Database Service (Amazon RDS). Toutefois, vous pouvez utiliser ce modèle avec n'importe quel autre éditeur de requêtes.

Limites

- Les objets Oracle SYNONYM ne sont pas disponibles dans PostgreSQL mais peuvent être partiellement validés par le biais de vues ou de requêtes SET search_path.
- L'éditeur de requêtes Amazon RDS n'est disponible que dans certaines régions AWS et pour certaines versions de MySQL et PostgreSQL.

Architecture

Outils

Outils

- Édition compatible avec Amazon Aurora PostgreSQL — Aurora PostgreSQL compatible est un moteur de base de données relationnelle entièrement géré, compatible avec PostgreSQL et compatible ACID qui associe la vitesse et la fiabilité des bases de données commerciales haut de gamme à la simplicité et à la rentabilité des bases de données open source.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud AWS. Il fournit des capacités redimensionnables, à faible coût, pour les bases de données relationnelles classiques, et gère les tâches courantes d'administration de base de données.
- Éditeur de requêtes pour Aurora Severless : l'éditeur de requêtes vous permet d'exécuter des requêtes SQL dans la console Amazon RDS. Vous pouvez exécuter n'importe quelle instruction SQL valide sur le cluster de base de données Aurora Serverless, y compris les instructions de manipulation et de définition des données.

Pour valider les objets, utilisez les scripts complets du fichier « Scripts de validation d'objets » dans la section « Pièces jointes ». Utilisez le tableau suivant à titre de référence.

Objet Oracle	Script à utiliser
Packages	Requête 1
Tables	Requête 3
Vues	Requête 5
Séquences	Requête 7
Déclencheurs	Requête 9
Clés primaires	Requête 11
Index	Requête 13
Contraintes de validation	Requête 15
Clés étrangères	Requête 17

objet PostgreSQL	Script à utiliser
Packages	Requête 2
Tables	Requête 4
Vues	Requête 6
Séquences	Requête 8
Déclencheurs	Requête 10
Clés primaires	Requête 12
Index	Requête 14
Contraintes de validation	Requête 16
Clés étrangères	Requête 18

Épopées

Valider les objets dans la base de données Oracle source

Tâche	Description	Compétences requises
Exécutez la requête de validation « packages » dans la base de données Oracle source.	Téléchargez et ouvrez le fichier « Scripts de validation d'objets » dans la section « Pièces jointes ». Connectez-vous à la base de données Oracle source via votre programme client. Exécutez le script de validation « Requête 1 » depuis le fichier « Scripts de validation d'objets ». Important : Entrez votre nom d'utilisateur Oracle au lieu de « your_schema » dans	Développeur, DBA

Tâche	Description	Compétences requises
	les requêtes. Assurez-vous d'enregistrer les résultats de votre requête.	
Exécutez la requête de validation « tables ».	Exécutez le script « Requête 3 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « views ».	Exécutez le script « Requête 5 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la validation du nombre de « séquences ».	Exécutez le script « Query 7 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « triggers ».	Exécutez le script « Requête 9 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation des « clés primaires ».	Exécutez le script « Requête 11 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA

Tâche	Description	Compétences requises
Exécutez la requête de validation « index ».	Exécutez le script de validation « Requête 13 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « check constraints ».	Exécutez le script « Requête 15 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « clés étrangères ».	Exécutez le script de validation « Requête 17 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA

Valider les objets dans la base de données cible compatible Aurora PostgreSQL

Tâche	Description	Compétences requises
Connectez-vous à la base de données cible compatible Aurora PostgreSQL à l'aide de l'éditeur de requêtes.	Connectez-vous à l'AWS Management Console et ouvrez la console Amazon RDS. Dans le coin supérieur droit, choisissez la région AWS dans laquelle vous avez créé la base de données compatible Aurora PostgreSQL. Dans le volet de navigation, choisissez « Databases », puis choisissez la base de	Développeur, DBA

Tâche	Description	Compétences requises
	données cible compatible Aurora PostgreSQL. Dans « Actions », choisissez « Requête ». Important : Si vous ne vous êtes jamais connecté à la base de données, la page « Connexion à la base de données » s'ouvre. Vous devez ensuite saisir les informations de votre base de données, telles que le nom d'utilisateur et le mot de passe.	
Exécutez la requête de validation « packages ».	Exécutez le script « Requête 2 » depuis le fichier « Scripts de validation d'objets » dans la section « Pièces jointes ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « tables ».	Retournez dans l'éditeur de requêtes pour la base de données compatible Aurora PostgreSQL et exécutez le script « Query 4 » à partir du fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA

Tâche	Description	Compétences requises
Exécutez la requête de validation « views ».	Retournez dans l'éditeur de requêtes pour la base de données compatible Aurora PostgreSQL et exécutez le script « Query 6 » à partir du fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la validation du nombre de « séquences ».	Retournez dans l'éditeur de requêtes pour la base de données compatible Aurora PostgreSQL et exécutez le script « Query 8 » à partir du fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « triggers ».	Retournez dans l'éditeur de requêtes pour la base de données compatible Aurora PostgreSQL et exécutez le script « Query 10 » à partir du fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA

Tâche	Description	Compétences requises
Exécutez la requête de validation des « clés primaires ».	Retournez dans l'éditeur de requêtes pour la base de données compatible Aurora PostgreSQL et exécutez le script « Query 12 » à partir du fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « index ».	Retournez dans l'éditeur de requêtes pour la base de données compatible Aurora PostgreSQL et exécutez le script « Query 14 » à partir du fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « check constraints ».	Exécutez le script « Requête 16 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA
Exécutez la requête de validation « clés étrangères ».	Exécutez le script de validation « Query 18 » depuis le fichier « Scripts de validation d'objets ». Assurez-vous d'enregistrer les résultats de votre requête.	Développeur, DBA

Comparez les enregistrements de validation des bases de données source et cible

Tâche	Description	Compétences requises
Comparez et validez les résultats des deux requêtes.	Comparez les résultats des requêtes des bases de données compatibles Oracle et Aurora PostgreSQL pour valider tous les objets. S'ils correspondent tous, cela signifie que tous les objets ont été validés avec succès.	Développeur, DBA

Ressources connexes

- Validation des objets de base de données après une migration à l'aide d'AWS SCT et d'AWS DMS
- Fonctionnalités d'Amazon Aurora : édition compatible avec PostgreSQL

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Réhéberger

Rubriques

- Accélérez la découverte et la migration des charges de travail Microsoft vers AWS
- Automatisez les activités d'ingestion préalables à la charge de travail pour AWS Managed Services sous Windows
- Créez un processus d'approbation pour les demandes de pare-feu lors d'une migration de réhébergement vers AWS
- Ingérez et migrez des instances EC2 Windows vers un compte AWS Managed Services
- Migrer une base de données Couchbase Server vers Amazon EC2
- Migrez Db2 for LUW vers Amazon EC2 en utilisant l'expédition des journaux pour réduire les temps d'arrêt
- Migrez Db2 for LUW vers Amazon EC2 avec une reprise après sinistre à haute disponibilité
- Migrer une base de données Microsoft SQL Server sur site vers Amazon à EC2 l'aide du service de migration d'applications
- Migrez VMware VMs avec HCX Automation à l'aide de PowerCLI
- Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS
- Migrer une application Web Go sur site vers AWS Elastic Beanstalk à l'aide de la méthode binaire
- Migrer un serveur SFTP sur site vers AWSAWS Transfer for SFTP
- Migrer une machine virtuelle sur site vers Amazon à l'aide EC2 d'AWS Application Migration Service
- Migrez de petits ensembles de données sur site vers Amazon S3 à l'aide d'AWS SFTP
- Migrer d'Oracle GlassFish vers AWS Elastic Beanstalk
- Migrer une base de données Oracle sur site vers Oracle sur Amazon EC2
- Migrer une base de données Oracle sur site vers Amazon à l'aide EC2 d'Oracle Data Pump
- Migrez les systèmes RHEL BYOL vers des instances incluses dans une licence AWS à l'aide d'AWS MGN
- Migrer une base de données SAP ASE sur site vers Amazon EC2
- Migrer une base de données Microsoft SQL Server sur site vers Amazon EC2
- Migrer une base de données MySQL sur site vers Amazon EC2
- Réduisez le temps de migration homogène vers SAP en utilisant le service de migration d'applications

- Réhébergez les charges de travail sur site dans le cloud AWS : liste de contrôle pour la migration
- Configurez une infrastructure multi-AZ pour un SQL Server Always On FCI à l'aide d'Amazon FSx
- Utilisez les requêtes BMC Discovery pour extraire les données de migration afin de planifier la migration

Accélérez la découverte et la migration des charges de travail Microsoft vers AWS

Créée par Ali Alzand

Récapitulatif

Ce modèle vous montre comment utiliser le PowerShell module Migration Validator Toolkit pour découvrir et migrer vos charges de travail Microsoft vers AWS. Le module fonctionne en effectuant plusieurs vérifications et validations pour les tâches courantes associées à n'importe quelle charge de travail Microsoft. Par exemple, le module recherche les instances auxquelles plusieurs disques peuvent être attachés ou les instances qui utilisent de nombreuses adresses IP. Pour une liste complète des contrôles que le module peut effectuer, consultez la section Contrôles sur la GitHub page du module.

Le PowerShell module Migration Validator Toolkit peut aider votre entreprise à réduire le temps et les efforts nécessaires pour découvrir les applications et les services exécutés sur vos charges de travail Microsoft. Le module peut également vous aider à identifier les configurations de vos charges de travail afin de savoir si vos configurations sont prises en charge sur AWS. Le module fournit également des recommandations quant aux prochaines étapes et mesures d'atténuation, afin que vous puissiez éviter toute erreur de configuration avant, pendant ou après votre migration.

Conditions préalables et limitations

Prérequis

- Compte d'administrateur local
- PowerShell 4,0

Limites

- Fonctionne uniquement sur Microsoft Windows Server 2012 R2 ou version ultérieure

Outils

Outils

- PowerShell 4,0

Référentiel de code

Le PowerShell module Migration Validator Toolkit pour ce modèle est disponible dans le référentiel GitHub migration-validator-toolkit-for-microsoft-workloads.

Épopées

Exécutez le PowerShell module Migration Validator Toolkit sur une seule cible

Tâche	Description	Compétences requises

Téléchargez, extrayez, importez et appelez le module.	Choisissez l'une des méthodes suivantes pour télécharger et déployer le module :
	• Exécutez le PowerShell script
	• Téléchargez et extrayez le fichier .zip
	• Cloner le GitHub référentiel
	
	Exécutez le PowerShell script
	
	Dans PowerShell, exécutez l'exemple de code suivant :
	
	`#MigrationValidatorToolkit`
	`$uri = 'https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads/archive/refs/heads/main.zip'`
	`$destination = (Get-Location).Path`
	`if ((Test-Path -Path "$destination\MigrationValidatorToolkit.zip" -PathType`
		Administrateur système

Tâche	Description	Compétences requises

	Leaf) -or (Test-Path -Path "$destination\MigrationValidatorToolkit")) {
	write-host "File $destination\MigrationValidatorToolkit.zip or folder $destination\MigrationValidatorToolkit found, exiting"
	}else {
	Write-host "Enable TLS 1.2 for this PowerShell session only."
	[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
	$webClient = New-Object System.Net.WebClient
	Write-host "Downloading MigrationValidatorToolkit.zip"
	$webClient.DownloadFile($uri, "$destination\MigrationValidatorToolkit.zip")
	Write-host "MigrationValidatorToolkit.zip download successfully"
	Add-Type -Assembly "system.io.compression.filesystem"
	[System.IO.Compression.ZipFile]::ExtractToDirectory("$destination\Migrat	

Tâche	Description	Compétences requises

	<pre>ionValidatorToolki
	t.zip","$destinati
	on\MigrationValida
	torToolkit")
	    Write-host
	 "Extracting Migration
	ValidatorToolkit.zip
	 complete successfully"
	    Import-Module
	 "$destination\Migr
	ationValidatorToolkit
	\migration-validator-
	toolkit-for-microsoft
	-workloads-main\Mi
	grationValidatorTo
	olkit.psm1"; Invoke-
	MigrationValidatorTo
	olkit
	}</pre> Le code télécharge le module à partir d'un fichier .zip. Ensuite, le code extrait, importe et invoque le module.
	
	Téléchargez et extrayez le fichier .zip
	
	1. Téléchargez le fichier .zip (téléchargement).
	2. Extrayez le fichier .zip.
	3. Suivez les étapes décrites dans l'article Invoke the module handly de ce guide.
	
	Cloner le GitHub référentiel	

Tâche	Description	Compétences requises
	1. Pour cloner le dépôt GitHub migration-validator-toolkit-for-microsoft-workloads, exécutez la commande Git suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git` 2. Suivez les étapes décrites dans l'article Invoke the module handly de ce guide.	

Tâche	Description	Compétences requises

Appelez le module manuellement.	1. Accédez au répertoire dans lequel le module téléchargé est stocké.
	2. Pour générer le résultat de votre choix, exécutez l'une des commandes suivantes en tant qu'administrateur dans PowerShell :
	
	Format : Format du tableau :
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit`
	
	Format-Format de liste :
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -List`
	
	GridViewFormat de sortie :
	`Import-Module .\MigrationValidatorToolkit.psm1;Invoke-MigrationValidatorToolkit -GridView`
	
	ConvertTo-Format CSV :
	`Import-Module .\MigrationValidatorToolkit`
		Administrateur système

Tâche	Description	Compétences requises
	`.psm1;Invoke-Migra tionValidatorToolkit -csv`	

Exécutez le PowerShell module Migration Validator Toolkit sur plusieurs cibles

Tâche	Description	Compétences requises
Téléchargez le fichier .zip ou clonez le GitHub dépôt.	Choisissez l'une des options suivantes : • Téléchargez le fichier zip. (téléchargement). • Pour cloner le dépôt GitHub migration-validator-toolkit-for-microsoft-workloads, exécutez la commande Git suivante dans une fenêtre de terminal : `git clone https://github.com/aws-samples/migration-validator-toolkit-for-microsoft-workloads.git`	Administrateur système
Mettez à jour la liste server.csv.	Si vous avez téléchargé le fichier .zip, procédez comme suit : 1. Extrayez le fichier .zip. 2. Accédez au répertoire `MigrationValidatorToolkit\Inputs\` .	Administrateur système

Tâche	Description	Compétences requises
	3. Effectuez la mise à jour `serverlist.csv` avec le nom d'hôte de vos ordinateurs cibles.	
Invoquez le module.	Vous pouvez utiliser n'importe quel ordinateur du domaine qui utilise un utilisateur du domaine disposant d'un accès administrateur aux ordinateurs cibles. 1. Téléchargez le code source sous forme de fichier .zip et extrayez le fichier. 2. En tant qu'administrateur PowerShell, exécutez la commande suivante : `Import-Module .\MigrationValidatorToolkit.psm1;Invoke-DomainComputers` Le fichier .csv de sortie est enregistré `MigrationValidatorToolkit\Outputs\folder` avec le nom du préfixe. `DomainComputers_MigrationAutomations_YYYY-MM-DDTHH-MM-SS`	Administrateur système

Résolution des problèmes

Problème	Solution
`MigrationValidatorToolkit` écrit des informations sur les exécutions, les commandes et les erreurs dans les fichiers journaux de l'hôte en cours d'exécution.	Vous pouvez consulter les fichiers journaux manuellement à l'emplacement suivant : 1. Accédez au répertoire `Migration ValidatorToolkit\logs\` . 2. Localisez le fichier journal. Le format du nom du fichier journal est le suivant : `ComputerName_MigrationValidatorToolkit_YYYY-MM-SSTHH-MM-SS.log`

Ressources connexes

- Options, outils et meilleures pratiques pour la migration des charges de travail Microsoft vers AWS (AWS Prescriptive Guidance)
- Modèles de migration Microsoft (AWS Prescriptive Guidance)
- Services de migration vers le cloud gratuits sur AWS (documentation AWS)
- Actions prédéfinies après le lancement (documentation marketing des applications)

Informations supplémentaires

Questions fréquentes (FAQ)

Où puis-je exécuter le PowerShell module Migration Validator Toolkit ?

Vous pouvez exécuter le module sur Microsoft Windows Server 2012 R2 ou version ultérieure.

Quand dois-je exécuter ce module ?

Nous vous recommandons d'exécuter le module pendant la phase d'évaluation du processus de migration.

Le module modifie-t-il mes serveurs existants ?

Non Toutes les actions de ce module sont en lecture seule.

Combien de temps faut-il pour exécuter le module ?

L'exécution du module prend généralement 1 à 5 minutes, mais cela dépend de l'allocation des ressources de votre serveur.

De quelles autorisations le module a-t-il besoin pour fonctionner ?

Vous devez exécuter le module à partir d'un compte d'administrateur local.

Puis-je exécuter le module sur des serveurs physiques ?

Oui, à condition que le système d'exploitation soit Microsoft Windows Server 2012 R2 ou version ultérieure.

Comment exécuter le module à grande échelle pour plusieurs serveurs ?

Pour exécuter le module sur plusieurs ordinateurs joints à un domaine à grande échelle, suivez les étapes décrites dans le module Run the Migration Validator Toolkit on multiple targets, PowerShell décrit dans l'article détaillé de ce guide. Pour les ordinateurs n'appartenant pas à un domaine, utilisez un appel à distance ou exécutez le module localement en suivant les étapes décrites dans le PowerShell module Run the Migration Validator Toolkit on a single target epic de ce guide.

Automatisez les activités d'ingestion préalables à la charge de travail pour AWS Managed Services sous Windows

Créée par Jacob Zhang (AWS), Calvin Yeh (AWS) et Dwayne Bordelon (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), AWS Managed Services (AMS) utilise AMS workload ingest (WIGS) pour déplacer les charges de travail existantes vers un VPC géré par AMS. Ce modèle décrit une solution pour automatiser les activités courantes de pré-ingestion de charge de travail, telles que la mise à niveau de .NET et de Windows PowerShell et l'exécution de la validation de pré-ingestion Windows WIGS gérée par AMS. Le modèle fournit également une interface utilisateur unifiée pour les résultats d'exécution. Il intègre un document de commande AWS Systems Manager, qui exécute les activités préalables à l'ingestion, dans un CloudFormation modèle AWS. Le modèle peut être déployé à plusieurs reprises sans nécessiter l'accès à Systems Manager lui-même ni entrer en conflit avec les automatisations d'AMS.

Antécédents commerciaux

Les migrations vers AMS nécessitent la mise à disposition de nouvelles instances Amazon Elastic Compute Cloud (Amazon EC2) à l'aide d'Amazon Machine Images (AMIs) gérées par AMS qui incluent des composants AMS. Toutes les charges de travail ou applications exécutées dans les centres de données existants doivent être redéployées vers de nouvelles EC2 instances lancées à partir de ces AMS. AMIs Pour éviter le travail manuel potentiellement énorme au cours du processus, l'équipe AMS a créé le flux de travail AMS (WIGS) pour intégrer vos images personnalisées dans AMS.

Les instances Windows doivent satisfaire à quelques prérequis avant que le processus WIGS ait lieu. Les PowerShell scripts Windows sont généralement utilisés pour effectuer les préparations nécessaires (préparation WIGS) et vérifier si les instances sont prêtes WIGs (validation préalable à l'ingestion par WIGS). Les processus de préparation et de validation nécessitent qu'un ingénieur passe 15 à 30 minutes sur chaque serveur, à se connecter manuellement et à exécuter les scripts un par un.

Moteur commercial

En général, Systems Manager vous permet d'automatiser des tâches opérationnelles telles que l'exécution de PowerShell scripts Windows. Cependant, en raison des risques élevés et des conflits fréquents entre les automatisations d'AMS et celles des utilisateurs, AMS n'accorde généralement pas à ses utilisateurs l'accès à Systems Manager.

Pour les migrations de masse à l'aide d'AWS Application Migration Service (AWS MGN), les PowerShell scripts Windows s'exécutent `C:\Program Files (x86)\AWS Replication Agent\post_launch folder` généralement automatiquement lorsqu'une instance de test ou de transition est lancée. Toutefois, ces scripts, s'ils sont exécutés immédiatement lors du lancement d'une instance, entrent fréquemment en conflit avec les automatisations d'AMS. Par conséquent, le lancement peut échouer sans fournir les résultats d'exécution dont vous avez besoin pour résoudre le problème.

Ce modèle permet de résoudre ces problèmes et fournit une solution automatisée fonctionnelle.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec intégration d'AMS est terminé.
- Un compartiment Amazon Simple Storage Service (Amazon S3) dans le compte AWS. S'il n'existe aucun compartiment S3 sur lequel vous avez le contrôle dans le compte, utilisez une demande de modification (RFC) pour en créer un.
- Le modèle Pre WIGs _CFN.json téléchargé depuis le référentiel. ams-auto-prewigs-windows
- Le serveur auquel vous appliquez ce modèle doit répondre aux exigences suivantes :
  - Exécutez Windows Server 2012 ou version ultérieure.
  - Être lancé ou prêt à être lancé dans le sous-réseau de migration VPC sandbox.
  - Installez un agent AWS Systems Manager (agent SSM).
  - Associez un profil d'instance AWS Identity and Access Management (IAM). Le profil d'instance doit être autorisé à télécharger des fichiers depuis des compartiments S3 dans le même compte AWS. Un profil d'instance répondant aux exigences susmentionnées est généralement déjà établi lors des configurations antérieures d'une migration.
  - Soyez consultable depuis AWS Systems Manager Fleet Manager.

Limites

- Les activités de pré-perruque varient en fonction de votre environnement et des exigences de votre entreprise. Vous devrez peut-être apporter des modifications mineures à ce modèle pour répondre à vos besoins spécifiques.

Versions du produit

- Le modèle est testé avec Windows Server 2012, 2012 R2, 2016 et 2019. Il fonctionne théoriquement avec les versions ultérieures de Windows. Il ne fonctionne pas avec les versions antérieures de Windows.

Architecture

Le schéma d'architecture montre ce qui suit :

1. VPC sandbox doté d'un sous-réseau de migration contenant des serveurs qui n'ont pas été préparés.
2. Le compartiment S3 qui stocke les scripts utilisés par le CloudFormation modèle.
3. Le CloudFormation modèle déploie le document de commande Systems Manager. Le processus se répète jusqu'à ce que les étapes soient terminées.
4. Les instances sont préparées et RFCs pour les WIGS sont créées.
5. Dans le VPC géré par AMS, le sous-réseau géré par AMS contient les serveurs après l'ingestion de la charge de travail.

Fonctionnement

- Ce modèle est intégré dans un CloudFormation modèle AWS qui permet des déploiements répétables de l'infrastructure sous forme de code (IaC). Vous ne devez déployer ce modèle qu'une seule fois pour chaque compte AWS nécessitant cette automatisation.
- L'automatisation est appliquée à toutes les EC2 instances dotées d'une clé de balise AutoPreWIGsdans le compte AWS où ce modèle est déployé. La première fois qu'une instance Amazon EC2 Windows avec la clé tag AutoPreWIGsdémarre, l'automatisation exécute les tâches suivantes.
  1. Met à niveau Windows PowerShell vers la version 5.1 et .NET vers la version 4.5.2. L'instance peut redémarrer plusieurs fois, en fonction de ses versions Windows PowerShell et .NET existantes. Après chaque redémarrage, les mises à niveau se poursuivent jusqu'à ce qu'elles soient terminées. Cette étape utilise du code intégré dans le CloudFormation modèle modifié à partir d'un PowerShell script Windows, ainsi que des instructions spécifiques de Systems Manager concernant le redémarrage du serveur.

2. Télécharge depuis Amazon S3 et exécute un PowerShell script Windows que vous avez personnalisé pour préparer l'instance Amazon EC2 Windows pour WIGS. Pour plus d'informations, consultez la section Epics.
3. Installe le module de validation préalable à l'ingestion de Windows WIGS PowerShell d'AWS.
4. Exécute la validation préalable à l'ingestion de Windows WIGS et affiche les résultats dans Systems Manager State Manager.

Outils

- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos ressources AWS. Vous pouvez utiliser un qui décrit toutes les ressources AWS que vous souhaitez ainsi que leurs dépendances, afin de pouvoir lancer et configurer ces ressources sous forme de pile. Ce modèle utilise un CloudFormation modèle pour automatiser le déploiement des ressources de ce modèle.
- AWS Managed Services — AWS Managed Services (AMS) est un service d'entreprise qui assure la gestion continue de votre infrastructure AWS. Les modifications apportées à l'infrastructure dans un environnement AMS doivent être effectuées par le biais d'un RFC.
- AWS Systems Manager — AWS Systems Manager (anciennement connu sous le nom de SSM) est un service AWS que vous pouvez utiliser pour visualiser et contrôler votre infrastructure sur AWS. À l'aide de la console Systems Manager, vous pouvez consulter les données opérationnelles de plusieurs services AWS et automatiser les tâches opérationnelles sur l'ensemble de vos ressources AWS. Ce modèle utilise Systems Manager pour exécuter et visualiser les résultats d'exécution des activités antérieures à Wigs.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Ce modèle utilise Amazon S3 pour stocker le CloudFormation modèle et un PowerShell script Windows téléchargé.

Épopées

Créez un PowerShell script Windows personnalisé pour automatiser des tâches supplémentaires

Tâche	Description	Compétences requises
Effectuez les modifications nécessaires sur les serveurs	Si vous souhaitez que les modifications soient automatiq	PowerShell écriture de scripts

Tâche	Description	Compétences requises
en fonction des besoins de l'entreprise.	uement appliquées à vos serveurs avant leur ingestion , créez un PowerShell script Windows nommé. `ingestion-prep.ps1` **Important** Le script ne doit pas contenir d'instructions pour redémarrer le serveur et ne doit pas nécessiter de privilèges d'administrateur.	
Supprimez les logiciels qui ne sont pas pris en charge par AMS.	AMS nécessite la suppression de certains logiciels, tels que les applications antivirus et les VMware outils, avant que WIGS ne fonctionne. Incluez la désinstallation dans le `ingestion-prep.ps1` script. Pour plus d'informations sur les logiciels non pris en charge, consultez la documentation AWS.	PowerShell écriture de scripts

Téléchargez le CloudFormation modèle et le PowerShell script Windows facultatif sur Amazon S3

Tâche	Description	Compétences requises
Créez un dossier dans S3.	Dans un compartiment S3 du même compte AWS où vous	AWS général

Tâche	Description	Compétences requises
	déployez ce modèle, créez un dossier.	
Téléchargez les scripts.	Téléchargez le `PreWIGs_CFN.json` CloudFormation modèle et le PowerShell script `ingestion-prep.ps1` Windows, que vous avez créés dans l'épopée précédente, dans le dossier Amazon S3.	AWS général

Déployez la CloudFormation pile

Tâche	Description	Compétences requises
Sélectionnez le type de modification.	Accédez à la console AMS pour créer une RFC. Utilisez le type de modification Create Stack from CloudFormation (CFN) Template.	AMS général
Définissez les paramètres d'exécution pour le chemin d'accès au CloudFormation modèle.	Dans la section Configuration de l'exécution, développez Configuration supplémentaire. Dans la zone CloudFormation de point de terminaison S3 du modèle, collez l'URL du CloudFormation modèle.	AMS général
Spécifiez le chemin d'accès au dossier Amazon S3.	Sous Paramètres, utilisez ScriptSourcecomme nom. Pour Value, entrez le chemin d'accès au dossier S3 contenant les PowerShell scripts Windows. Assurez-	AMS général

Tâche	Description	Compétences requises
	vous d'utiliser l'`https://xxx` URL au lieu de l'`s3://xxx`URI et de l'inclure `/` à la fin.	
Déployez la pile.	Pour déployer la pile, choisissez Create.	AMS général
Transférez le RFC à AMS Ops.	Le RFC doit être implément é manuellement par l'équipe AMS Ops car il utilise Systems Manager pour déployer des ressources et nécessite un examen de sécurité. Dès que vous créez la RFC, elle sera automatiquement rejetée par le système. Choisisse z la RFC et ajoutez une correspondance à la RFC indiquant Veuillez exécuter manuellement. Notez l'ID RFC et augmentez-le avec une demande de service.	AMS général

Appliquez l'automatisation aux instances

Tâche	Description	Compétences requises
Ajoutez le AutoPre WIGs tag aux instances.	Notez IDs toutes les instances auxquelles vous souhaitez appliquer cette automatis ation et attendez au moins 30 minutes pour que l'instanc e termine les automatis ations mises en œuvre par	AMS général

Tâche	Description	Compétences requises
	AMS. Soumettez une RFC automatique pour ajouter la balise avec AutoPreWIGscomme clé et n'importe quelle chaîne, telle que 1, comme valeur. L'automatisation sera appliquée quelques minutes après l'ajout de la balise.	
Vérifiez les résultats de l'automatisation.	Ouvrez la console Systems Manager, puis choisissez State Manager. Choisissez l'ID d'association avec le nom AMS-Prewig-Prep-and-Validation-Association. Dans l'onglet Historique des exécutions, vous pouvez voir les résultats de l'automatisation.	AMS général
Corrigez toutes les erreurs.	Si l'automatisation échoue, choisissez son ID d'exécution. Vous pouvez voir les résultats de l'exécution pour chaque EC2 instance. Pour voir les détails de chaque étape de l'automatisation, choisissez Output. Si une étape donnée échoue, utilisez les informations des sections Sortie et Erreur pour diagnostiquer le problème.	Ingénieur en migration

Tâche	Description	Compétences requises
Retirez l' AutoPreWIGs étiquette.	**⚠ Important** Après avoir corrigé les erreurs, le cas échéant, soumettez une RFC automatiq ue pour supprimer la AutoPreWIGsbalise. WIGS échouera si vous ne retirez pas l'étiquette.	AMS général

Ingérez les instances préparées

Tâche	Description	Compétences requises
Soumettre RFCs pour WIGS.	Maintenant que les instances sont prêtes pour l'ingestion de la charge de travail, soumettez -les RFCs pour WIGS.	AMS général

Ressources connexes

- Ingestion de la charge de travail AMS (WIGS)
- Migration des charges de travail : validation préalable à l'ingestion de Windows
- Guide de démarrage rapide d'AWS Application Migration Service
- Commencer à utiliser AWS CloudFormation
- Configuration d'AWS Systems Manager

Créez un processus d'approbation pour les demandes de pare-feu lors d'une migration de réhébergement vers AWS

Créée par Srikanth Rangavajhala (AWS)

Récapitulatif

Si vous souhaitez utiliser AWS Application Migration Serviceou activer Cloud Migration Factory AWS pour une migration de réhôte vers le AWS Cloud, l'une des conditions préalables est de garder les ports TCP 443 et 1500 ouverts. L'ouverture de ces ports de pare-feu nécessite généralement l'approbation de votre équipe chargée de la sécurité des informations (InfoSec).

Ce modèle décrit le processus permettant d'obtenir l'approbation d'une demande de pare-feu auprès d'une InfoSec équipe lors d'une migration de réhébergement vers le AWS Cloud. Vous pouvez utiliser ce processus pour éviter le rejet de votre demande de pare-feu par l' InfoSec équipe, ce qui peut s'avérer coûteux et chronophage. Le processus de demande de pare-feu comporte deux étapes de révision et d'approbation entre les consultants en AWS migration et les responsables qui travaillent avec votre équipe InfoSec et celle des applications pour ouvrir les ports du pare-feu.

Ce modèle suppose que vous planifiez une migration de réhébergement avec des AWS consultants ou des spécialistes de la migration de votre organisation. Vous pouvez utiliser ce modèle si votre organisation ne dispose pas d'un processus d'approbation du pare-feu ou d'un formulaire d'approbation générale pour les demandes de pare-feu. Pour plus d'informations à ce sujet, consultez la section Limitations de ce modèle. Pour plus d'informations sur la configuration réseau requise pour le service de migration d'applications, consultez la section Configuration réseau requise dans la documentation du service de migration d'applications.

Conditions préalables et limitations

Prérequis

- Une migration de réhébergement planifiée avec des AWS consultants ou des spécialistes de la migration de votre organisation
- Les informations de port et d'IP requises pour migrer la pile
- Schémas d'architecture d'état existants et futurs
- Informations sur le pare-feu concernant l'infrastructure locale et de destination, les ports et le flux de zone-to-zone trafic
- Une liste de vérification des demandes de pare-feu (ci-jointe)
- Un document de demande de pare-feu, configuré selon les exigences de votre organisation

- Une liste de contacts pour les réviseurs et les approbateurs du pare-feu, y compris les rôles suivants :
  - Soumetteur de demandes de pare-feu : spécialiste ou AWS consultant en migration. L'expéditeur de la demande de pare-feu peut également être un spécialiste de la migration de votre organisation.
  - Réviseur des demandes de pare-feu : il s'agit généralement du point de contact unique (SPOC) à partir AWS duquel.
  - Approbateur de demandes de pare-feu : membre de InfoSec l'équipe.

Limites

- Ce modèle décrit un processus générique d'approbation des demandes de pare-feu. Les exigences peuvent varier d'une organisation à l'autre.
- Assurez-vous de suivre les modifications apportées à votre document de demande de pare-feu.

Le tableau suivant présente les cas d'utilisation de ce modèle.

Votre entreprise dispose-t-elle déjà d'un processus d'approbation de pare-feu ?	Votre organisation possède-t-elle déjà un formulaire de demande de pare-feu ?	Action suggérée
Oui	Oui	Collaborez avec AWS des consultants ou vos spécialistes de la migration pour mettre en œuvre le processus de votre organisation.
Non	Oui	Utilisez le processus d'approbation du pare-feu de ce modèle. Faites appel à un AWS consultant ou à un spécialiste de la migration de votre organisation pour soumettre le formulaire d'approbation générale de la demande de pare-feu.

Non	Non	Utilisez le processus d'approbation du pare-feu de ce modèle. Faites appel à un AWS consultant ou à un spécialiste de la migration de votre organisation pour soumettre le formulaire d'approbation générale de la demande de pare-feu.

Architecture

Le schéma suivant montre les étapes du processus d'approbation des demandes de pare-feu.

Outils

Vous pouvez utiliser des outils de numérisation tels que Palo Alto Networks ou SolarWindspour analyser et valider les pare-feux et les adresses IP.

Épopées

Analyser la demande de pare-feu

Tâche	Description	Compétences requises
Analysez les ports et les adresses IP.	L'expéditeur de la demande de pare-feu effectue une analyse initiale pour comprendre les ports de pare-feu et les adresses IP requis. Une fois cette opération terminée, ils demandent à votre InfoSec équipe d'ouvrir les ports requis et de mapper les adresses IP.	Ingénieur cloud AWS, spécialiste de la migration

Validez la demande de pare-feu

Tâche	Description	Compétences requises
Validez les informations du pare-feu.	L' AWS Cloud ingénieur organise une réunion avec votre InfoSec équipe. Au cours de cette réunion, l'ingénieur examine et valide les informations de demande de pare-feu. Généralement, l'expéditeur de la demande de pare-feu est la même personne que le demandeur de pare-feu. Cette phase de validation peut devenir itérative en fonction des commentaires fournis par l'approbateur si quelque chose est observé ou recommandé.	Ingénieur cloud AWS, spécialiste de la migration
Mettez à jour le document de demande de pare-feu.	Une fois que l' InfoSec équipe a partagé ses commentaires, le document de demande de pare-feu est modifié, enregistré et chargé à nouveau. Ce document est mis à jour après chaque itération. Nous vous recommandons de stocker ce document dans un dossier de stockage dont la version est contrôlée. Cela signifie que toutes les modifications sont suivies et correctement appliquées.	Ingénieur cloud AWS, spécialiste de la migration

Soumettre la demande de pare-feu

Tâche	Description	Compétences requises
Soumettez la demande de pare-feu.	Une fois que l'approbateur de demande de pare-feu a approuvé la demande d'approbation globale du pare-feu, l' AWS Cloud ingénieur soumet la demande de pare-feu. La demande indique les ports qui doivent être ouverts et les adresses IP requises pour mapper et mettre à jour le Compte AWS. Vous pouvez faire des suggestions ou fournir des commentaires une fois la demande de pare-feu envoyée. Nous vous recommandons d'automatiser ce processus de feedback et d'envoyer les modifications par le biais d'un mécanisme de flux de travail défini.	Ingénieur cloud AWS, spécialiste de la migration

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Ingérez et migrez des instances EC2 Windows vers un compte AWS Managed Services

Créée par Anil Kunapareddy (AWS) et Venkatramana Chintha (AWS)

Récapitulatif

Ce modèle explique le step-by-step processus de migration et d'ingestion d'instances Windows Amazon Elastic Compute Cloud EC2 (Amazon) vers un compte Amazon Web Services (AWS) Managed Services (AMS). AMS peut vous aider à gérer l'instance de manière plus efficace et plus sûre. AMS fournit une flexibilité opérationnelle, améliore la sécurité et la conformité, et vous aide à optimiser la capacité et à réduire les coûts.

Ce modèle commence par une instance EC2 Windows que vous avez migrée vers un sous-réseau intermédiaire de votre compte AMS. Divers services et outils de migration sont disponibles pour effectuer cette tâche, tels qu'AWS Application Migration Service.

Pour apporter une modification à votre environnement géré par AMS, vous devez créer et soumettre une demande de modification (RFC) pour une opération ou une action particulière. À l'aide d'une RFC d'ingestion de charge de travail AMS (WIGS), vous ingérez l'instance dans le compte AMS et vous créez une Amazon Machine Image (AMI) personnalisée. Vous créez ensuite l' EC2 instance gérée par AMS en soumettant une autre RFC pour créer une pile. EC2 Pour plus d'informations, consultez AMS Workload Ingest dans la documentation AMS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif géré par AMS
- Une zone d'atterrissage existante
- Autorisations permettant d'apporter des modifications dans le VPC géré par AMS
- Une instance Amazon EC2 Windows dans un sous-réseau intermédiaire de votre compte AMS
- Réalisation des prérequis généraux pour la migration des charges de travail à l'aide d'AMS WIGS
- Réalisation des prérequis Windows pour la migration des charges de travail à l'aide d'AMS WIGS

Limites

- Ce modèle est destiné aux EC2 instances exécutant Windows Server. Ce modèle ne s'applique pas aux instances exécutant d'autres systèmes d'exploitation, tels que Linux.

Architecture

Pile technologique source

Instance Amazon EC2 Windows dans un sous-réseau intermédiaire de votre compte AMS

Pile technologique cible

Instance Amazon EC2 Windows gérée par AWS Managed Services (AMS)

Architecture cible

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que vous le souhaitez, et vous pouvez les étendre ou les intégrer.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Managed Services (AMS) vous aide à travailler de manière plus efficace et plus sécurisée en assurant la gestion continue de votre infrastructure AWS, notamment la surveillance, la gestion des incidents, les conseils de sécurité, le support des correctifs et la sauvegarde des charges de travail AWS.

Autres services

- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS.

Épopées

Configurer les paramètres de l'instance

Tâche	Description	Compétences requises
Modifiez les paramètres du client DNS.	1. Sur l' EC2 instance source, ouvrez l'invite	Ingénieur en migration

Tâche	Description	Compétences requises
	de commande en tant qu'administrateur, tapez`gpedit.msc` , puis appuyez sur Entrée. 2. Dans l'éditeur de stratégie de groupe local, accédez à Configuration de l'ordinateur, Modèles d'administration, Réseau, Client DNS. 3. Pour le suffixe DNS principal, choisissez Non configuré. 4. Pour le transfert du suffixe DNS principal, choisissez Non configuré.	

Tâche	Description	Compétences requises
Modifiez les paramètres de Windows Update.	1. Dans l'éditeur de stratégie de groupe local, accédez à Configuration de l'ordinateur, Modèles d'administration, Composants Windows, Windows Update. 2. Pour Spécifier l'emplacement du service Microsoft Update de l'intranet, choisissez Non configuré. 3. Pour Configurer les mises à jour automatiques, choisissez Non configuré. 4. Pour la fréquence de détection des mises à jour automatiques, choisissez Non configuré. 5. Fermez l'éditeur de stratégie de groupe local.	Ingénieur en migration
Activez le pare-feu.	1. Sur l' EC2 instance source, ouvrez l'invite de commande en tant qu'administrateur, tapez`services.msc` , puis appuyez sur Entrée. 2. Dans Windows Services, activez le pare-feu. 3. Fermez les services Windows.	Ingénieur en migration

Préparer l'instance pour AMS WIGS

Tâche	Description	Compétences requises
Nettoyez et préparez l'instance.	1. À l'aide d'un hôte bastion et d'informations d'identification locales, créez une connexion RDP (Remote Desktop Protocol) avec l'EC2 instance dans le sous-réseau intermédiaire. 2. Supprimez tous les anciens logiciels, logiciels antivirus et solutions de sauvegarde qui ne sont pas nécessaires dans AMS.	Ingénieur en migration

Réparez le fichier sppnp.dll.	1. Accédez à `C:\Windows\System32\sppnp.dll` .
	2. Renommer `sppnp.dll` en. `sppnp_old.dll`
	3. À l'aide PowerShell des informations d'identification d'administrateur, entrez les commandes suivantes :
	`dism /online /cleanup-image /restorehealth`
	`sfc /scannnow`
	4. Redémarrez l'instance EC2 Windows.
		Ingénieur en migration

Exécutez le script de validation pré-WIG.	1. Téléchargez le fichier zip de validation préalable à l'ingestion de Windows	Ingénieur en migration

Tâche	Description	Compétences requises
	WIGS (`windows-prewings-valication.zip`) depuis Migration des charges de travail : validation préalable à l'ingestion de Windows dans la documentation AMS. 2. Exécutez le script de validation Windows Pre-WIG et vérifiez les résultats. 3. Si la validation échoue, corrigez le problème et réexécutez le script de validation jusqu'à ce que la validation aboutisse.	

Tâche	Description	Compétences requises
Créez l'AMI à sécurité intégrée.	Une fois la validation préalable au WIG terminée, créez une AMI de pré-ingestion comme suit : 1. Choisissez Deployment, Advanced Stack Components, AMI, Create. 2. Lors de la création, ajoutez un tag `Key=Name, Value=APPLICATION-ID_IngestReady` . 3. Attendez que l'AMI soit créée avant de continuer. Pour plus d'informations, consultez AMI | Create dans la documentation AMS.	Ingénieur en migration

Ingérer et valider l'instance

Tâche	Description	Compétences requises
Soumettez la RFC pour créer la pile d'ingestion de charge de travail.	Soumettez une demande de modification (RFC) pour démarrer l'AMS WIGS. Pour obtenir des instructions, consultez Workload Ingest Stack : Creating dans la documentation AMS. Cela déclenche l'ingestion de la charge de travail et installe tous les logiciels requis par	Ingénieur en migration

Tâche	Description	Compétences requises
	AMS, y compris les outils de sauvegarde, le logiciel EC2 de gestion Amazon et le logiciel antivirus.	
Validez la réussite de la migration.	Une fois l'ingestion de la charge de travail terminée, vous pouvez voir l'instanc e gérée par AMS et l'AMI ingérée par AMS. 1. Connectez-vous à l'instance gérée par AMS à l'aide des informations d'identification du domaine. 2. Validez la jonction de domaine comme suit : a. Dans l'Explorateur Windows, cliquez avec le bouton droit sur Ce PC, puis sélectionnez Propriétés. b. Dans la section Spécifica tion du périphérique, vérifiez que le domaine apparaît dans le nom complet de l'appareil. 3. Validez les unités de disque source et cible.	Ingénieur en migration

Lancez l'instance dans le compte AMS cible

Tâche	Description	Compétences requises
Soumettez le RFC pour créer une EC2 pile.	1. À l'aide de l'AMI ingérée par AMS de l'instance Windows, préparez une RFC pour EC2 une pile conformément aux instructions de la section EC2 Créer une instance de pile dans la documentation AMS. Dans la EC2 pile RFC, indiquez tous les paramètres, y compris le nom du serveur, les balises, le VPC cible, le sous-réseau cible, le type d'instance, les groupes de sécurité cibles, l'AMI d'ingestion et le rôle. 2. Soumettez la RFC pour la EC2 pile, puis attendez que l'instance soit correctement créée.	Ingénieur en migration

Ressources connexes

Recommandations AWS

- Automatisez les activités d'ingestion préalables à la charge de travail pour AWS Managed Services sous Windows
- Créez automatiquement une RFC dans AMS à l'aide de Python

Documentation AMS

- Ingestion de la charge de travail AMS
- Comment la migration modifie vos ressources
- Migration des charges de travail : processus standard

Ressources marketing

- AWS Managed Services
- AWS Managed Services FAQs
- Ressources AWS Managed Services
- Fonctionnalités d'AWS Managed Services

Migrer une base de données Couchbase Server vers Amazon EC2

Créée par Subhani Shaik (AWS)

Récapitulatif

Ce modèle décrit comment vous pouvez migrer le serveur Couchbase d'un environnement sur site vers Amazon Elastic Compute Cloud (Amazon EC2) on. AWS

Couchbase Server est une base de données NoSQL (document JSON) distribuée qui fournit des fonctionnalités de base de données relationnelle. La migration d'une base de données Couchbase Server AWS peut apporter une évolutivité accrue, des performances améliorées, une rentabilité accrue, une sécurité renforcée, une gestion simplifiée et une portée mondiale, ce qui peut profiter aux applications nécessitant un accès aux données à haute disponibilité et à faible latence. Vous avez également accès à des fonctionnalités avancées par le biais de services AWS gérés.

Couchbase Server on AWS fournit les fonctionnalités clés suivantes :

- Architecture axée sur la mémoire
- Haute disponibilité, reprise après sinistre et équilibrage de charge
- Déploiement multi-maîtres et multirégions pour des performances optimales

Pour plus d'informations sur les principaux avantages, consultez la section Informations supplémentaires et le site Web de Couchbase.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS doté d'un cloud privé virtuel (VPC), de deux zones de disponibilité, de sous-réseaux privés et d'un groupe de sécurité. Pour obtenir des instructions, consultez la section Créer un VPC dans la documentation Amazon Virtual Private Cloud (Amazon VPC).
- Connectivité activée entre les environnements source et cible. Pour plus d'informations sur les ports TCX utilisés par Couchbase Server, consultez la documentation de Couchbase.

Architecture

Le schéma suivant montre l'architecture de haut niveau pour la migration de Couchbase Server vers. AWS

À partir du cluster Couchbase sur site, les données passent par une passerelle client en utilisant. AWS Direct Connect Les données passent par un routeur et une AWS Direct Connect route et atteignent le VPC via une passerelle AWS Virtual Private Network (AWS VPN). Le VPC contient une EC2 instance qui exécute Couchbase Server. L' AWS infrastructure inclut également AWS Identity and Access Management (IAM) pour le contrôle d'accès, AWS Key Management Service (AWS KMS) pour le chiffrement des données, Amazon Elastic Block Store (Amazon EBS) pour le stockage par blocs et Amazon Simple Storage Service (Amazon S3) pour le stockage des données.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Direct Connectrelie votre réseau interne à un AWS Direct Connect emplacement via un câble à fibre optique Ethernet standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement destinées au public Services AWS tout en contournant les fournisseurs de services Internet sur votre chemin réseau.

Bonnes pratiques

- Installation et configuration de Couchbase sur différentes plateformes d'exploitation
- Meilleures pratiques pour déployer Couchbase Server sur AWS
- Création d'un cluster Couchbase
- Meilleures pratiques en matière de performances pour les applications Couchbase
- Bonnes pratiques de sécurité pour Couchbase Server
- Meilleures pratiques de stockage pour les bases de données Couchbase Server

Épopées

Déployer une EC2 instance Amazon pour Couchbase Server

Tâche	Description	Compétences requises
Ouvrez la EC2 console Amazon.	Connectez-vous à la EC2 console Amazon AWS Management Consoleet ouvrez-la.	DevOps ingénieur, administrateur Couchbase
Déployez une EC2 instance Amazon.	Lancez une EC2 instance qui correspond aux configurations du serveur Couchbase sur site. Pour plus d'informations sur le déploiement d'une EC2 instance, consultez Lancer une EC2 instance Amazon dans la EC2 documentation Amazon.	DevOps ingénieur, administrateur Couchbase

Installation et configuration du serveur Couchbase sur Amazon EC2

Tâche	Description	Compétences requises
Installez un cluster Couchbase .	Consultez les directives de déploiement de Couchbase Server avant d'installer Couchbase Server sur Amazon. EC2 Pour installer Couchbase Server, consultez la documentation du serveur Couchbase	Administrateur Couchbase
Configurez le cluster.	Pour configurer le cluster, consultez la section Options	Administrateur Couchbase

Tâche	Description	Compétences requises
	de configuration du cluster dans la documentation de Couchbase.	

Ajoutez un nouveau nœud et rééquilibrez le cluster Couchbase

Tâche	Description	Compétences requises
Ajoutez un nœud pour l' EC2 instance.	Ajoutez l' EC2 instance récemment déployée sur laquelle Couchbase est installé au cluster sur site existant. Pour obtenir des instructions, consultez la section Ajouter un nœud et rééquilibrer dans la documentation du serveur Couchbase.	Administrateur Couchbase
Rééquilibrez le cluster.	Le processus de rééquilibrage fait du nœud nouvellement ajouté avec l' EC2 instance un membre actif du cluster Couchbase. Pour obtenir des instructions, consultez la section Ajouter un nœud et rééquilibrer dans la documentation du serveur Couchbase	Administrateur Couchbase

Reconfigurer les connexions

Tâche	Description	Compétences requises
Supprimez les nœuds locaux et rééquilibrez.	Vous pouvez désormais supprimer les nœuds locaux du cluster. Après avoir supprimé les nœuds, suivez le processus de rééquilibrage pour redistribuer les données, les index, le traitement des événements et le traitement des requêtes entre les nœuds disponibles du cluster. Pour obtenir des instructions, consultez Supprimer un nœud et rééquilibrer dans la documentation du serveur Couchbase.	Administrateur Couchbase
Mettez à jour les paramètres de connexion.	Mettez à jour les paramètres de connexion de votre application pour utiliser la nouvelle adresse EC2 IP Amazon, afin que votre application puisse se connecter au nouveau nœud.	Développeur d'applications Couchbase

Ressources connexes

- Services de serveur Couchbase
- Déployez le serveur Couchbase à l'aide de AWS Marketplace
- Connectez-vous au serveur Couchbase
- Gérer les buckets
- Réplication entre centres de données (XDCR)
- Contrat de licence de Couchbase Inc.

Informations supplémentaires

Principaux avantages

La migration de votre base de données Couchbase AWS offre les avantages suivants :

Scalabilité. Vous pouvez faire évoluer votre cluster Couchbase à la hausse ou à la baisse en fonction de la demande sans avoir à gérer de matériel physique. Vous pouvez ainsi facilement vous adapter aux fluctuations des volumes de données et de l'utilisation des applications. AWS fournit :

- Options de mise à l'échelle verticale et horizontale
- Capacités de déploiement mondiales
- Équilibrage de charge entre Régions AWS
- Solutions de dimensionnement des bases de données
- Optimisation de la diffusion de contenu

Optimisation des performances. AWS fournit une infrastructure réseau performante et des types d'instances optimisés pour garantir un accès rapide aux données et une faible latence pour votre base de données Couchbase.

- Options de calcul haute performance (HPC)
- Diffusion de contenu dans le monde entier via Amazon CloudFront
- Plusieurs options de stockage
- Services de base de données avancés, notamment Amazon Relational Database Service (Amazon RDS) et Amazon DynamoDB
- Connexions à faible latence avec AWS Direct Connect

Optimisation des coûts. Sélectionnez le type d'instance et la configuration appropriés pour équilibrer les performances et les coûts en fonction de votre charge de travail. Payez uniquement pour les ressources que vous utilisez. Cela peut potentiellement réduire vos coûts d'exploitation en éliminant le besoin de gérer le matériel sur site et en tirant parti des AWS Cloud économies d'échelle.

- Les instances réservées peuvent vous aider à planifier à l'avance et à réduire considérablement vos coûts lorsque vous utilisez Couchbase sur. AWS
- La mise à l'échelle automatique empêche le surprovisionnement et vous aide à optimiser votre utilisation et votre rentabilité.

Sécurité renforcée. Profitez des fonctionnalités de sécurité robustes AWS, telles que le chiffrement des données, les contrôles d'accès et les groupes de sécurité, pour protéger les données sensibles que vous stockez dans Couchbase. Avantages supplémentaires :

- Le modèle de responsabilitéAWS partagée fait clairement la différence entre la sécurité du cloud (AWS responsabilité) et la sécurité dans le cloud (responsabilité du client).
- AWS la conformité prend en charge les principales normes de sécurité.
- AWS fournit des options de chiffrement avancées.
- AWS Identity and Access Management (IAM) vous aide à gérer l'accès sécurisé à vos ressources.

Gestion simplifiée. AWS fournit des services gérés pour Couchbase, afin que vous puissiez vous concentrer sur le développement d'applications plutôt que sur la gestion de l'infrastructure sous-jacente.

Portée mondiale. Vous pouvez déployer votre cluster Couchbase sur plusieurs clusters Régions AWS afin de réduire le temps de latence pour les utilisateurs du monde entier. Vous pouvez déployer vos bases de données entièrement dans le cloud ou dans un environnement hybride. Vous pouvez protéger vos données grâce à une sécurité intégrée de niveau entreprise et à une synchronisation bidirectionnelle rapide et efficace des données entre la périphérie et le cloud. Dans le même temps, vous pouvez simplifier le développement grâce à un modèle de programmation cohérent pour créer des applications Web et mobiles.

Continuité des activités :

- Sauvegarde et restauration des données. En cas de problème, vous pouvez l'utiliser AWS Backuppour garantir la résilience des données et une restauration facile. Pour les options de reprise après sinistre, consultez la documentation AWS Well-Architected Framework.
- Déploiement multirégional de Couchbase : pour déployer une base de données Couchbase dans un AWS environnement multirégional, vous pouvez vous abonner à Couchbase Server dans, utiliser des AWS CloudFormationmodèles pour créer des clusters Couchbase distincts dans chaque région AWS Marketplace, puis configurer la réplication entre régions pour synchroniser les données entre les régions. Cette configuration garantit une haute disponibilité et une redondance géographique dans plusieurs régions. Pour plus d'informations, consultez la section Déployer le serveur Couchbase AWS Marketplaceà l'aide de la documentation Couchbase.

Agilité de l'infrastructure :

- Provisionnement et déprovisionnement rapides des ressources
- Portée mondiale de l'infrastructure
- Mise à l'échelle automatique en fonction de la demande
- Infrastructure en tant que code (IaC) pour des déploiements cohérents
- Plusieurs types d'instances optimisés pour différentes charges de travail

Facilitation de l'innovation :

- Accès aux dernières technologies, notamment l'IA/ML, l'IoT et l'analytique
- Services gérés, qui réduisent les frais d'exploitation
- Pratiques modernes de développement d'applications
- Options informatiques sans serveur

Excellence opérationnelle :

- Surveillance et journalisation centralisées
- Gestion automatisée des ressources
- Capacités de maintenance prédictive
- Visibilité améliorée sur l'utilisation des ressources
- Processus de déploiement rationalisés

Opportunités de modernisation :

- Architecture des microservices
- DevOpsmise en œuvre des pratiques
- Développement d'applications cloud natives
- Modernisation des applications existantes

Avantages compétitifs :

- Délai de mise sur le marché plus court
- Expérience client améliorée
- Prise de décision basée sur les données

- Intelligence d'affaires améliorée

Migrez Db2 for LUW vers Amazon EC2 en utilisant l'expédition des journaux pour réduire les temps d'arrêt

Créée par Feng Cai (AWS), Ambarish Satarkar (AWS) et Saurabh Sharma (AWS)

Récapitulatif

Lorsque les clients migrent leurs charges de travail IBM Db2 for LUW (Linux, UNIX et Windows) vers Amazon Web Services (AWS), l'utilisation d'Amazon Elastic Compute Cloud (Amazon EC2) avec le modèle Bring Your Own License (BYOL) est le moyen le plus rapide. Cependant, la migration de grandes quantités de données de Db2 sur site vers AWS peut s'avérer difficile, en particulier lorsque la période de panne est courte. De nombreux clients essaient de fixer la fenêtre d'interruption à moins de 30 minutes, ce qui laisse peu de temps à la base de données elle-même.

Ce modèle explique comment effectuer une migration DB2 avec une courte période de panne en utilisant l'expédition du journal des transactions. Cette approche s'applique à Db2 sur une plate-forme Linux de type Little-Endian.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance DB2 exécutée sur une EC2 instance qui correspond aux dispositions du système de fichiers sur site
- Un compartiment Amazon Simple Storage Service (Amazon S3) accessible à l'instance EC2
- Une politique et un rôle AWS Identity and Access Management (IAM) pour effectuer des appels programmatiques vers Amazon S3
- Fuseau horaire et horloges système synchronisés sur Amazon EC2 et sur le serveur local
- Le réseau sur site connecté à AWS via le Site-to-SiteVPN AWS ou AWS Direct Connect

Limites

- L'instance Db2 sur site et Amazon EC2 doivent appartenir à la même famille de plateformes.
- La charge de travail locale DB2 doit être enregistrée. Pour bloquer toute transaction non enregistrée, définissez la configuration de `blocknonlogged=yes` la base de données.

Versions du produit

- Db2 pour LUW version 11.5.9 et versions ultérieures

Architecture

Pile technologique source

- Db2 sous Linux x86_64

Pile technologique cible

- Amazon EBS
- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- Site-to-SiteVPN AWS ou Direct Connect

Architecture cible

Le schéma suivant montre une instance Db2 exécutée sur site avec une connexion de réseau privé virtuel (VPN) à DB2 sur Amazon. EC2 Les lignes en pointillés représentent le tunnel VPN entre votre centre de données et le cloud AWS.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Direct Connect relie votre réseau interne à un emplacement Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les services AWS publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Site-to-SiteLe VPN AWS vous aide à faire passer le trafic entre les instances que vous lancez sur AWS et votre propre réseau distant.

Autres outils

- db2cli est la commande CLI interactive DB2.

Bonnes pratiques

- Sur la base de données cible, utilisez les points de terminaison de passerelle pour Amazon S3 afin d'accéder à l'image de sauvegarde de la base de données et aux fichiers journaux dans Amazon S3.
- Sur la base de données source, utilisez AWS PrivateLink pour Amazon S3 pour envoyer l'image de sauvegarde de la base de données et les fichiers journaux à Amazon S3.

Épopées

Définir les variables d'environnement

Tâche	Description	Compétences requises
Définissez les variables d'environnement.	Ce modèle utilise les noms suivants : • Nom de l’instance : `db2inst1` • Nom de la base de données : `SAMPLE`	DBA

Tâche	Description	Compétences requises
	Vous pouvez les adapter à votre environnement.	

Configuration du serveur DB2 sur site

Tâche	Description	Compétences requises

Configurez l'interface de ligne de commande AWS.	Pour télécharger et installer la dernière version de l'AWS CLI, exécutez les commandes suivantes :
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Administrateur Linux

Configurez une destination locale pour les journaux d'archive DB2.	Pour que la base de données cible sur Amazon EC2 reste synchronisée avec la base de données source sur site, les derniers journaux de transactions doivent être extraits de la source. Dans cette configuration, `/db2logs` est définie par `LOGARCHMETH2` la source en tant que zone intermédiaire. Les journaux archivés de ce répertoire seront synchronisés dans Amazon S3 et Db2 sur Amazon y accédera.	DBA

Tâche	Description	Compétences requises

	EC2 Le modèle est utilisé `LOGARCHMETH2` parce qu'il a `LOGARCHMETH1` peut-être été configuré pour utiliser un outil d'un fournisseur tiers auquel la commande de la CLI AWS ne peut pas accéder. Pour récupérer les journaux, exécutez la commande suivante :
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 disk:/db2logs`	

Exécutez une sauvegarde de base de données en ligne.	Exécutez une sauvegarde de base de données en ligne et enregistrez-la dans le système de fichiers de sauvegarde local : `db2 backup db sample online to /backup`	DBA

Configuration du compartiment S3 et de la politique IAM

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment S3 pour que le serveur sur site envoie les images DB2 de sauvegarde et les fichiers journaux vers AWS. Amazon	Administrateur système AWS

Tâche	Description	Compétences requises
	pourra également accéder au bucket EC2 : `aws s3api create-bucket --bucket logshipmig-db2 --region us-east-1`	

Tâche	Description	Compétences requises
Créez une politique IAM.	Le `db2bucket.json` fichier contient la politique IAM permettant d'accéder au compartiment Amazon S3 : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload", "s3:ListBucket", "s3:DeleteObject", "s3:GetObjectVersion", "s3:ListMultipartUploadParts" ], "Resource": [`	Administrateur AWS, administrateur système AWS

Tâche	Description	Compétences requises

	<pre>"arn:aws:s3:::logshipmig-db2/*",
	
	"arn:aws:s3:::logshipmig-db2"
	]
	}
	]
	}</pre>
	Pour créer la politique, utilisez la commande de l'AWS CLI suivante :
	<pre>aws iam create-policy \
	--policy-name db2s3policy \
	--policy-document file://db2bucket.json</pre>
	La sortie JSON indique le nom de ressource Amazon (ARN) pour la politique, où `aws_account_id` représente l'ID de votre compte :
	<pre>"Arn": "arn:aws:iam::aws_account_id:policy/db2s3policy"</pre>	

Tâche	Description	Compétences requises
Attachez la politique IAM au rôle IAM utilisé par l' EC2 instance.	Dans la plupart des environnements AWS, une EC2 instance en cours d'exécution possède un rôle IAM défini par votre administrateur système. Si le rôle IAM n'est pas défini, créez-le et choisissez Modifier le rôle IAM sur la EC2 console pour associer le rôle à l' EC2 instance qui héberge la base de données Db2. Associez la stratégie IAM au rôle IAM avec l'ARN de la stratégie : `aws iam attach-role-policy \ --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3policy" \ --role-name db2s3role` Une fois la politique attachée, toute EC2 instance associée au rôle IAM peut accéder au compartiment S3.	Administrateur AWS, administrateur système AWS

Envoyez l'image de sauvegarde et les fichiers journaux de la base de données source à Amazon S3

Tâche	Description	Compétences requises
Configurez l'AWS CLI sur le serveur Db2 sur site.	Configurez l'AWS CLI avec le `Access Key ID` et `Secret`	Administrateur AWS, administrateur système AWS

Tâche	Description	Compétences requises

	`Access Key` généré à l'étape précédente :
	
	`$ aws configure`
	`AWS Access Key ID`
	` [None]: **********`
	`AWS Secret Access Key`
	` [None]: ********`
	`**********`
	`Default region name`
	` [None]: us-east-1`
	`Default output format`
	` [None]: json`	

Envoyez l'image de sauvegarde à Amazon S3.	Auparavant, une sauvegarde de base de données en ligne était enregistrée dans le répertoire `/backup` local. Pour envoyer cette image de sauvegarde vers le compartiment S3, exécutez la commande suivante :
	
	`aws s3 sync /backup`
	` s3://logshipmig-db2/`
	`SAMPLE_backup`
		Administrateur AWS, ingénieur en migration

Tâche	Description	Compétences requises
Envoyez les journaux d'archive DB2 à Amazon S3.	Synchronisez les journaux d'archive Db2 sur site avec le compartiment S3 auquel l'instance Db2 cible peut accéder sur Amazon : EC2 `aws s3 sync /db2logs s3://logshipmig-db2/SAMPLE_LOG` Exécutez cette commande régulièrement à l'aide de cron ou d'autres outils de planification. La fréquence dépend de la fréquence à laquelle la base de données source archive les journaux de transactions.	Administrateur AWS, ingénieur en migration

Connectez Db2 sur Amazon EC2 à Amazon S3 et lancez la synchronisation de la base de données

Tâche	Description	Compétences requises
Créez un PKCS12 keystore.	Db2 utilise un magasin de clés de chiffrement PKCS (Public-Key Cryptography Standards) pour sécuriser la clé d'accès AWS. Créez un keystore et configurez l'instance Db2 source pour l'utiliser : `gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<passwor`	DBA

Tâche	Description	Compétences requises
	d>" -type pkcs12 -stash db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"	
Créez l'alias d'accès au stockage DB2.	Pour créer l'alias d'accès au stockage, utilisez la syntaxe de script suivante : db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'" Par exemple, votre script peut ressembler à ce qui suit : db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'logshipmig-db2'"	DBA

Tâche	Description	Compétences requises
Définissez la zone de transit.	Par défaut, Db2 l'utilise `DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH` comme zone intermédiaire pour charger et télécharger des fichiers depuis et vers Amazon S3. Le chemin par défaut se trouve `sqllib/tmp/RemoteStorage.xxxx` sous le répertoire d'accueil de l'instance, en `xxxx` référence au numéro de partition DB2. Notez que la zone de stockage doit avoir une capacité suffisante pour contenir les images de sauvegarde et les fichiers journaux. Vous pouvez utiliser le registre pour faire pointer la zone de transit vers un autre répertoire. Nous vous recommandons également d'utiliser `DB2_ENABLE_COS_SDK=ON DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , et le lien vers la `awssdk` bibliothèque pour contourner la zone intermédiaire Amazon S3 pour la sauvegarde et la restauration de bases de données :	DBA

Tâche	Description	Compétences requises

	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`Db2set DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore`
	`db2stop`
	`db2start`	

Restaurez la base de données à partir de l'image de sauvegarde.	Restaurez la base de données cible sur Amazon EC2 à partir de l'image de sauvegarde dans le compartiment S3 : `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshipmig-db2/SAMPLE_backup replace existing`	DBA

Tâche	Description	Compétences requises

Procédez à la progression de la base de données.	Une fois la restauration terminée, la base de données cible sera placée dans l'état d'attente du rollforward. Configurez `LOGARCHMETH1` et faites en `LOGARCHMETH2` sorte que Db2 sache où obtenir les fichiers du journal des transactions :
	`db2 update db cfg for SAMPLE using LOGARCHMETH1 'DB2REMOTE://DB2AWSS3//SAMPLE_LOGS/'`
	`db2 update db cfg for SAMPLE using LOGARCHMETH2 OFF`
	Lancer le rollforward de la base de données :
	`db2 ROLLFORWARD DATABASE sample to END OF LOGS`
	Cette commande traite tous les fichiers journaux qui ont été transférés vers le compartiment S3. Exécutez-le régulièrement en fonction de la fréquence de la `s3 sync` commande sur les serveurs Db2 locaux. Par exemple, si elle `s3 sync` s'exécute toutes les heures et que la synchronisation de tous les fichiers
		DBA

Tâche	Description	Compétences requises
	journaux prend 10 minutes, définissez la commande pour qu'elle s'exécute 10 minutes après chaque heure.	

Mettez Db2 EC2 en ligne sur Amazon pendant la période de transition

Tâche	Description	Compétences requises

Mettez la base de données cible en ligne.	Pendant la fenêtre de basculement, effectuez l'une des opérations suivantes :
	• Insérez la base de données locale et exécutez la `s3 sync` commande pour forcer l'archivage du dernier journal de transactions. `ADMIN MODE`
	• Arrêtez la base de données.
	
	Une fois le dernier journal de transactions synchronisé avec Amazon S3, exécutez la `ROLLFORWARD` commande pour la dernière fois :
	
	`db2 rollforward DB sample to END OF LOGS`
	`db2 rollforward DB sample complete`
	
	`Rollforward Status`
		DBA

Tâche	Description	Compétences requises

	`....`
	` Rollforward status`
	`                  = not`
	` pending`
	`....`
	`DB20000I  The ROLLFORWA`
	`RD command completed`
	` successfully.`
	
	`db2 activate db sample`
	`DB20000I  The ACTIVATE`
	` DATABASE command`
	` completed successfu`
	`lly.`
	
	Mettez la base de données cible en ligne et dirigez les connexions de l'application vers Db2 sur Amazon EC2.	

Résolution des problèmes

Problème	Solution
Si plusieurs bases de données ont le même nom d'instance et le même nom de base de données sur différents hôtes (DEV, QA, PROD), les sauvegardes et les journaux peuvent être placés dans le même sous-répe rtoire.	Utilisez différents compartiments S3 pour DEV, QA et PROD, et ajoutez le nom d'hôte comme préfixe de sous-répertoire pour éviter toute confusion.
Si plusieurs images de sauvegarde se trouvent au même emplacement, le message d'erreur suivant s'affichera lors de la restauration : `SQL2522N More than one backup file matches the time stamp value`	Dans la `restore` commande, ajoutez l'horodat age de la sauvegarde : `db2 restore db sample from DB2REMOTE://DB2AWSS3/logshi`

Problème	Solution
`provided for the backed up database image.`	`pmig-db2/SAMPLE_backup taken at 20230628164042 replace existing`

Ressources connexes

- Opérations de sauvegarde et de restauration DB2 entre différents systèmes d'exploitation et plateformes matérielles
- Configurer Db2 STORAGE ACCESS ALIAS et REMOTE DB2
- Commande DB2 ROLLFORWARD
- Méthode d'archivage du journal secondaire DB2

Migrez Db2 for LUW vers Amazon EC2 avec une reprise après sinistre à haute disponibilité

Créée par Feng Cai (AWS), Aruna Gangireddy (AWS) et Venkatesan Govindan (AWS)

Récapitulatif

Lorsque les clients migrent leur charge de travail IBM Db2 LUW (Linux, UNIX et Windows) vers Amazon Web Services (AWS), l'utilisation d'Amazon Elastic Compute Cloud (Amazon EC2) avec le modèle Bring Your Own License (BYOL) est le moyen le plus rapide. Cependant, la migration de grandes quantités de données de Db2 sur site vers AWS peut s'avérer difficile, en particulier lorsque la période de panne est courte. De nombreux clients essaient de fixer la fenêtre d'interruption à moins de 30 minutes, ce qui laisse peu de temps à la base de données elle-même.

Ce modèle explique comment effectuer une migration vers DB2 avec une courte période de panne en utilisant la reprise après sinistre à haute disponibilité (HADR) de DB2. Cette approche s'applique aux bases de données DB2 qui se trouvent sur la plate-forme Linux Little-endian et n'utilisent pas la fonctionnalité de partitionnement des données (DPF).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance Db2 exécutée sur une EC2 instance Amazon qui correspond aux configurations du système de fichiers sur site
- Un compartiment Amazon Simple Storage Service (Amazon S3) accessible à l'instance EC2
- Politique et rôle d'AWS Identity and Access Management (IAM) pour effectuer des appels programmatiques vers Amazon S3
- Fuseau horaire et horloges système synchronisés sur Amazon EC2 et sur le serveur local
- Le réseau sur site connecté à AWS via le Site-to-SiteVPN AWS ou AWS Direct Connect
- Communication entre le serveur sur site et Amazon EC2 sur les ports HADR

Limites

- L'instance Db2 sur site et Amazon EC2 doivent appartenir à la même famille de plateformes.
- Le HADR n'est pas pris en charge dans un environnement de base de données partitionné.

- Le HADR ne prend pas en charge l'utilisation d'E/S brutes (accès direct au disque) pour les fichiers journaux de base de données.
- Le HADR ne prend pas en charge la journalisation infinie.
- `LOGINDEXBUILD`doit être défini sur`YES`, ce qui augmentera l'utilisation du journal pour la reconstruction de l'index.
- La charge de travail locale DB2 doit être enregistrée. Définissez `blocknonlogged=yes` dans la configuration de la base de données pour bloquer toutes les transactions non enregistrées.

Versions du produit

- Db2 pour LUW version 11.5.9 et versions ultérieures

Architecture

Pile technologique source

- Db2 sous Linux x86_64

Pile technologique cible

- Amazon EC2
- AWS Identity and Access Management (IAM)
- Amazon S3
- Site-to-SiteVPN AWS

Architecture cible

Dans le schéma suivant, Db2 on premises est exécuté en `db2-server1` tant que serveur principal. Il dispose de deux cibles de réserve HADR. Une cible de réserve se trouve sur site et est facultative. L'autre cible de réserve `db2-ec2` se trouve sur Amazon EC2. Une fois la base de données transférée vers AWS, `db2-ec2` elle devient la base de données principale.

1. Les journaux sont transmis de la base de données locale principale vers la base de données locale de secours.

2. À l'aide de Db2 HADR, les journaux sont transmis depuis la base de données principale sur site via un Site-to-Site VPN vers Db2 sur Amazon. EC2
3. Les journaux de sauvegarde et d'archivage DB2 sont envoyés depuis la base de données principale sur site vers le compartiment S3 sur AWS.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Direct Connect relie votre réseau interne à un emplacement Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les services AWS publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Site-to-SiteLe VPN AWS vous aide à faire passer le trafic entre les instances que vous lancez sur AWS et votre propre réseau distant.

Autres outils

- db2cli est la commande CLI interactive DB2.

Bonnes pratiques

- Sur la base de données cible, utilisez les points de terminaison de passerelle pour Amazon S3 afin d'accéder à l'image de sauvegarde de la base de données et aux fichiers journaux dans Amazon S3.

- Sur la base de données source, utilisez AWS PrivateLink pour Amazon S3 pour envoyer l'image de sauvegarde de la base de données et les fichiers journaux à Amazon S3.

Épopées

Définir les variables d'environnement

Tâche	Description	Compétences requises
Définissez les variables d'environnement.	Ce modèle utilise les noms et ports suivants : 1. Nom d'hôte local DB2 : `db2-server1` 2. Nom d'hôte de secours du HADR : `db2-server2` (si le HADR est actuellement exécuté sur site) 3. EC2 Nom d'hôte Amazon : `db2-ec2` 4. Nom de l'instance : `db2inst1` 5. Nom de la base de données : `SAMPLE` 6. Ports HARD : • `db2-server1: 50010` • `db2-server2: 50011` • `db2-ec2: 50012` Vous pouvez les adapter à votre environnement.	DBA

Configuration du serveur DB2 sur site

Tâche	Description	Compétences requises

Configurez l'AWS CLI.	Pour télécharger et installer la dernière version de l'AWS CLI, exécutez les commandes suivantes :
	`$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"`
	`unzip awscliv2.zip`
	`sudo ./aws/install`
		Administrateur Linux

Configurez une destination locale pour les journaux d'archive DB2.	Des conditions telles que les tâches de mise à jour par lots importantes et les ralentissements du réseau peuvent entraîner un décalage du serveur de secours HADR. Pour rattraper son retard, le serveur de secours a besoin des journaux de transactions du serveur principal. La séquence des emplacements pour demander les journaux est la suivante : • Le répertoire des journaux actifs sur le serveur principal • L'`LOGARCHMETH2` emplacement `LOGARCHMETH1` ou sur le serveur de secours	DBA

Tâche	Description	Compétences requises

	• L'LOGARCHME TH2 emplacement LOGARCHMETH1 ou sur le serveur principal
	
	Dans cette configuration, /db2logs est définie par LOGARCHMETH2 la source en tant que zone intermédiaire. Les journaux archivés de ce répertoire seront synchroni sés dans Amazon S3 et Db2 sur Amazon y accédera. EC2 Le modèle est utilisé LOGARCHMETH2 parce qu'il a LOGARCHMETH1 peut-être été configuré pour utiliser un outil d'un fournisseur tiers auquel la commande de la CLI AWS ne peut pas accéder :
	
	`db2 connect to sample`
	`db2 update db cfg for SAMPLE using LOGARCHME TH2 disk:/db2logs`	

Exécutez une sauvegarde de base de données en ligne.	Exécutez une sauvegarde de base de données en ligne et enregistrez-la dans le système de fichiers de sauvegarde local : `db2 backup db sample online to /backup`	DBA

Configuration du compartiment S3 et de la politique IAM

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment S3 pour que le serveur sur site envoie les images DB2 de sauvegarde et les fichiers journaux vers AWS. Le bucket sera accessible par Amazon EC2 : `aws s3api create-bucket --bucket hadrmig-db2 --region us-east-1`	Administrateur AWS
Créez une politique IAM.	Le `db2bucket.json` fichier contient la politique IAM pour accéder au compartiment S3 : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "kms:GenerateDataKey", "kms:Decrypt", "s3:PutObject", "s3:GetObject", "s3:AbortMultipartUpload",`	Administrateur AWS, administrateur système AWS

Tâche	Description	Compétences requises

	<pre>"s3:ListBucket",
	
	"s3:DeleteObject",
	
	"s3:GetObjectVersion",
	
	"s3:ListMultipartUploadParts"
	],
	"Resource":
	[
	
	"arn:aws:s3:::hadrmig-db2/*",
	
	"arn:aws:s3:::hadrmig-db2"
	]
	}
	]
	}</pre>
	Pour créer la politique, utilisez la commande de l'interface de ligne de commande AWS suivante :
	<pre>aws iam create-policy \
	--policy-name
	db2s3hapolicy \
	--policy-document
	file://db2bucket.json</pre>
	La sortie JSON indique le nom de ressource Amazon (ARN) pour la politique, où	

Tâche	Description	Compétences requises
	`aws_account_id` représente l'ID de votre compte : `"Arn": "arn:aws:iam::aws_account_id:policy/db2s3hapolicy"`	
Attachez la politique IAM au rôle IAM.	Généralement, l' EC2 instance sur laquelle Db2 est en cours d'exécution possède un rôle IAM attribué par l'administrateur système. Si aucun rôle IAM n'est attribué, vous pouvez choisir Modifier le rôle IAM sur la console Amazon EC2 . Attachez la politique IAM au rôle IAM associé à l' EC2 instance. Une fois la politique attachée, l' EC2 instance peut accéder au compartiment S3 : `aws iam attach-role-policy --policy-arn "arn:aws:iam::aws_account_id:policy/db2s3hapolicy" --role-name db2s3harole`	

Envoyez l'image de sauvegarde et les fichiers journaux de la base de données source à Amazon S3

Tâche	Description	Compétences requises

Configurez l'AWS CLI sur le serveur Db2 sur site.	Configurez l'AWS CLI avec le `Access Key ID` et `Secret Access Key` que vous avez généré précédemment :
	`$ aws configure`
	`AWS Access Key ID [None]: **********`
	`AWS Secret Access Key [None]: ********** **********`
	`Default region name [None]: us-east-1`
	`Default output format [None]: json`
		Administrateur AWS, administrateur système AWS

Envoyez l'image de sauvegarde à Amazon S3.	Auparavant, une sauvegarde de base de données en ligne était enregistrée dans le répertoire `/backup` local. Pour envoyer cette image de sauvegarde vers le compartiment S3, exécutez la commande suivante : `aws s3 sync /backup s3://hadrmig-db2/SAMPLE_backup`	Administrateur AWS, administrateur système AWS
Envoyez les journaux d'archive DB2 à Amazon S3.	Synchronisez les journaux d'archive Db2 sur site avec le compartiment Amazon S3 auquel l'instance Db2 cible	

Tâche	Description	Compétences requises
	peut accéder sur Amazon : EC2 `aws s3 sync /db2logs s3://hadrmig-db2/SAMPLE_LOGS` Exécutez cette commande régulièrement à l'aide de cron ou d'autres outils de planification. La fréquence dépend de la fréquence à laquelle la base de données source archive les journaux de transactions.	

Connectez Db2 sur Amazon EC2 à Amazon S3 et lancez la synchronisation initiale de la base de données

Tâche	Description	Compétences requises
Créez un PKCS12 keystore.	Db2 utilise un magasin de clés de chiffrement PKCS (Public-Key Cryptography Standards) pour sécuriser la clé d'accès AWS. Créez un keystore et configurez le Db2 source pour l'utiliser : `gsk8capicmd_64 -keydb -create -db "/home/db2inst1/.keystore/db2s3.p12" -pw "<password>" -type pkcs12 -stash`	DBA

Tâche	Description	Compétences requises
	`db2 "update dbm cfg using keystore_location /home/db2inst1/.keystore/db2s3.p12 keystore_type pkcs12"`	

Tâche	Description	Compétences requises

Créez l'alias d'accès au stockage DB2.	Db2 utilise un alias d'accès au stockage pour accéder directement à Amazon S3 à l'aide des `RESTORE DATABASE` commandes `INGEST LOADBACKUP DATABASE`,, ou.
	
	Parce que vous avez attribué un rôle IAM à l' EC2 instance `USER` et que vous n'`PASSWORD`êtes pas obligé de :
	
	`db2 "catalog storage access alias <alias_name> vendor S3 server <S3 endpoint> container '<bucket_name>'"`
	
	Par exemple, votre script peut ressembler à ce qui suit :
	
	`db2 "catalog storage access alias DB2AWSS3 vendor S3 server s3.us-east-1.amazonaws.com container 'hadrmig-db2'"`
		DBA

Tâche	Description	Compétences requises

Définissez la zone de transit.	Nous vous recommandons d'utiliser `DB2_ENABLE_COS_SDK=ON DB2_OBJECT_STORAGE_SETTINGS=EnableStreamingRestore` , et le lien vers la `awssdk` bibliothèque pour contourner la zone intermédiaire Amazon S3 pour la sauvegarde et la restauration de bases de données :
	`#By root:`
	`cp -rp /home/db2inst1/sqllib/lib64/awssdk/RHEL/7.6/* /home/db2inst1/sqllib/lib64/`
	
	`#By db2 instance owner:`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2set DB2_ENABLE_COS_SDK=ON`
	`db2set DB2_OBJECT_STORAGE_LOCAL_STAGING_PATH=/db2stage`
	`db2stop`
	`db2start`
		DBA

Tâche	Description	Compétences requises

Restaurez la base de données à partir de l'image de sauvegarde.	Restaurez la base de données cible sur Amazon EC2 à partir de l'image de sauvegarde dans le compartiment S3 :
	`db2 create db sample on /data1`
	`db2 restore db sample from DB2REMOTE://DB2AWSS3/hadrmig-db2/SAMPLE_backup replace existing`
		DBA

Configurer le HADR sans le HADR sur site

Tâche	Description	Compétences requises
Configurez le serveur DB2 local en tant que serveur principal.	Mettez à jour les paramètres de configuration de base de données pour HADR on `db2-server1` (la source locale) en tant que base principale. Réglez `HADR_SYNCMODE` sur `SUPERASYNC` le mode, qui présente le temps de réponse le plus court pour les transacti ons : `db2 update db cfg for sample using HADR_LOCAL_HOST db2-server1 HADR_LOCAL_SVC 50010 HADR_REMOTE_HOST db2-ec2 HADR_REMOTE_SVC 50012 HADR_REMO`	DBA

Tâche	Description	Compétences requises
	`TE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000 I The UPDATE DATABASE CONFIGURATION command completed successfu lly` Certains retards sur le réseau entre le centre de données sur site et AWS sont attendus. (Vous pouvez définir une `HADR_SYNCMODE` valeur différente en fonction de la fiabilité du réseau. Pour plus d'informations, consultez la section Ressources connexes).	
Modifiez la destination d'archivage des journaux de la base de données cible.	Modifiez la destination d'archivage des journaux de la base de données cible pour qu'elle corresponde à EC2 l'environnement Amazon : `db2 update db cfg for SAMPLE using LOGARCHME TH1 'DB2REMOTE://DB2AW SS3//SAMPLE_LOGS/' LOGARCHMETH2 OFF DB20000I The UPDATE DATABASE CONFIGURA TION command completed successfully`	DBA

Tâche	Description	Compétences requises
Configurez HADR pour Db2 sur le serveur Amazon EC2 .	Mettre à jour la configuration de la base de données pour HADR `db2-ec2` en mode veille : `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNC MODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully`	DBA

Tâche	Description	Compétences requises

Vérifiez la configuration du HADR.	Vérifiez les paramètres HADR sur les serveurs Db2 source et cible.
	
	Pour vérifier l'installation`db2-server1` , exécutez la commande suivante :
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-ec2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50012`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) =`
	`HADR log write synchronization mode`
		DBA

Tâche	Description	Compétences requises
	(HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Pour vérifier l'installation`db2-ec2`, exécutez la commande suivante : `db2 get db cfg for sample|grep HADR` HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-ec2 HADR local service name (HADR_LOCAL_SVC) = 50012 HADR remote host name (HADR_REMOTE_HOST) = db2-server1	

Tâche	Description	Compétences requises
	HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF Les HADR_REMOTE_SVC paramètres HADR_LOCAL_HOST HADR_LOCAL_SVC ,HADR_REMO	

Tâche	Description	Compétences requises
	TE_H0ST , et indiquent la configuration principale et l'autre de secours du HADR.	

Démarrez l'instance Db2 HADR.	Démarrez d'abord l'instanc e Db2 HADR sur le serveur db2-ec2 de secours :
	`db2 start hadr on db sample as standby`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	Démarrez Db2 HADR sur le serveur principal (source) : db2-server1
	`db2 start hadr on db sample as primary`
	`DB20000I The START HADR ON DATABASE command completed successfully.`
	La connexion HADR entre Db2 sur site et sur Amazon EC2 a maintenant été établie avec succès. Le serveur principal Db2 db2-serve r1 commence à diffuser les enregistrements du journal des transactions db2-ec2 en temps réel.
		DBA

Configurer le HADR lorsque le HADR existe sur site

Tâche	Description	Compétences requises
Ajoutez Db2 sur Amazon EC2 en tant que support auxiliaire.	Si le HADR est exécuté sur l'instance Db2 locale, vous pouvez ajouter Db2 sur EC2 Amazon en tant que serveur de secours auxiliaire en HADR_TARGET_LIST exécutant les commandes suivantes sur : db2-ec2 `db2 update db cfg for sample using HADR_LOCAL_HOST db2-ec2 HADR_LOCAL_SVC 50012 HADR_REMOTE_HOST db2-server1 HADR_REMOTE_SVC 50010 HADR_REMOTE_INST db2inst1 HADR_SYNCMODE SUPERASYNC DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. db2 update db cfg for sample using HADR_TARGET_LIST "db2-server1:50010|db2-server2:50011" DB20000I The UPDATE DATABASE CONFIGURATION command`	DBA

Tâche	Description	Compétences requises
	`completed successfully.`	

Tâche	Description	Compétences requises
Ajoutez les informations de veille auxiliaire aux serveurs locaux.	Mise à jour `HADR_TARGET_LIST` sur les deux serveurs locaux (principal et de secours). `db2-server1` Activé, exécutez le code suivant : `db2 update db cfg for sample using HADR_TARGET_LIST "db2-server2:50011|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`  `db2-server2` Activé, exécutez le code suivant :  `db2 update db cfg for sample using HADR_TARG`	DBA

Tâche	Description	Compétences requises
	`ET_LIST "db2-server1:50010|db2-ec2:50012" DB20000I The UPDATE DATABASE CONFIGURATION command completed successfully. SQL1363W One or more of the parameters submitted for immediate modification were not changed dynamically. For these configuration parameters, the database must be shutdown and reactivated before the configuration parameter changes become effective.`	

Tâche	Description	Compétences requises

Vérifiez la configuration du HADR.	Vérifiez les paramètres HADR sur les serveurs Db2 source et cible.
	
	`db2-server1` Activé, exécutez le code suivant :
	
	`db2 get db cfg for sample|grep HADR`
	`HADR database role = PRIMARY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-server1`
	`HADR local service name (HADR_LOCAL_SVC) = 50010`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server2`
	`HADR remote service name (HADR_REMOTE_SVC) = 50011`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server2:50011|db2-ec2:50012`	

Tâche	Description	Compétences requises
	HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF `db2-server2` Activé, exécutez le code suivant : `db2 get db cfg for sample|grep HADR` HADR database role = STANDBY HADR local host name (HADR_LOCAL_HOST) = db2-server2 HADR local service name (HADR_LOCAL_SVC) = 50011 HADR remote host name (HADR_REMOTE_HOST) = db2-server1	

Tâche	Description	Compétences requises
	HADR remote service name (HADR_REMOTE_SVC) = 50010 HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1 HADR timeout value (HADR_TIMEOUT) = 120 HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-ec2:50012 HADR log write synchronization mode (HADR_SYNCMODE) = NEARSYNC HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000) HADR log replay delay (seconds) (HADR_REPLAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certificate label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF `db2-ec2`Activé, exécutez le code suivant :	

Tâche	Description	Compétences requises

	`db2 get db cfg for sample|grep HADR`
	`HADR database role = STANDBY`
	`HADR local host name (HADR_LOCAL_HOST) = db2-ec2`
	`HADR local service name (HADR_LOCAL_SVC) = 50012`
	`HADR remote host name (HADR_REMOTE_HOST) = db2-server1`
	`HADR remote service name (HADR_REMOTE_SVC) = 50010`
	`HADR instance name of remote server (HADR_REMOTE_INST) = db2inst1`
	`HADR timeout value (HADR_TIMEOUT) = 120`
	`HADR target list (HADR_TARGET_LIST) = db2-server1:50010|db2-server2:50011`
	`HADR log write synchronization mode (HADR_SYNCMODE) = SUPERASYNC`
	`HADR spool log data limit (4KB) (HADR_SPOOL_LIMIT) = AUTOMATIC(52000)`	

Tâche	Description	Compétences requises
	``` HADR log replay delay (seconds) (HADR_REP LAY_DELAY) = 0 HADR peer window duration (seconds) (HADR_PEER_WINDOW) = 0 HADR SSL certifica te label (HADR_SSL_LABEL) = HADR SSL Hostname Validation (HADR_SSL_HOST_VAL) = OFF ``` Les `HADR_TARGET_LIST` paramètres`HADR_LOCA L_HOST` ,`HADR_LOCA L_SVC` , `HADR_REMO TE_HOST` `HADR_REMO TE_SVC` , et indiquent la configuration d'un HADR principal et de deux HADR de secours.	

Tâche	Description	Compétences requises

Arrêtez et démarrez Db2 HADR.	`HADR_TARGET_LIST` est désormais configuré sur les trois serveurs. Chaque serveur DB2 connaît les deux autres. Arrêtez et redémarrez le HADR (brève interruption) pour tirer parti de la nouvelle configuration.
	
	`db2-server1` Activé, exécutez les commandes suivantes :
	
	`db2 stop hadr on db sample`
	`db2 deactivate db sample`
	`db2 activate db sample`
	
	`db2-server2` Activé, exécutez les commandes suivantes :
	
	`db2 deactivate db sample`
	`db2 start hadr on db sample as standby`
	`SQL1766W The command completed successfully`
	
	`db2-ec2`Activé, exécutez les commandes suivantes :
	
	`db2 start hadr on db sample as standby`
		DBA

Tâche	Description	Compétences requises

	`SQL1766W The command completed successfully`
	
	`db2-server1` Activé, exécutez les commandes suivantes :
	
	`db2 start hadr on db sample as primary`
	`SQL1766W The command completed successfully`
	
	La connexion HADR entre Db2 on premises et Amazon EC2 est désormais établie avec succès. Le serveur principal DB2 `db2-server1` commence à diffuser les enregistrements du journal des transactions à la fois `db2-server2` et `db2-ec2` en temps réel.	

Définir Db2 sur Amazon EC2 comme principal pendant la période de transition

Tâche	Description	Compétences requises
Assurez-vous qu'il n'y a aucun décalage HADR sur le serveur de secours.	Vérifiez l'état du HADR sur le serveur `db2-server1` principal. Ne vous inquiétez pas lorsque le `REMOTE_CATCHUP` statut `HADR_STATE` est activé, ce qui est normal lorsqu'il `HADR_SYNCMODE` est réglé sur. `SUPERASYNC`	DBA

Tâche	Description	Compétences requises

	Le PRIMARY_LOG_TIME et STANDBY_REPLAY_LOG _TIME montrent qu'ils sont synchronisés :
	
	`db2pd -hadr -db sample`
	
	`HADR_ROLE = PRIMARY`
	
	`REPLAY_TYPE = PHYSICAL`
	
	`HADR_SYNCMODE = SUPERASYNC`
	
	`STANDBY_ID = 2`
	
	`LOG_STREAM_ID = 0`
	
	`HADR_STATE = REMOTE_CATCHUP`
	`.....`
	
	`PRIMARY_LOG_TIME = 10/26/2022 02:11:32. 000000 (1666750292)`
	
	`STANDBY_LOG_TIME = 10/26/2022 02:11:32. 000000 (1666750292)`
	`STANDBY_R EPLAY_LOG_TIME = 10/26/2022 02:11:32. 000000 (1666750292)`	

Tâche	Description	Compétences requises

Lancez HADR Takeover.	Pour terminer la migration , créez `db2-ec2` la base de données principale en exécutant la commande HADR takeover. Utilisez la commande db2pd pour vérifier la `HADR_ROLE` valeur :
	
	`db2 TAKEOVER HADR ON DATABASE sample`
	`DB20000I The TAKEOVER HADR ON DATABASE command completed successfully.`
	
	`db2pd -hadr -db sample`
	`Database Member 0 -- Database SAMPLE -- Active -- Up 0 days 00:03:25 -- Date 2022-10-26-02.46.45.048988`
	
	`HADR_ROLE = PRIMARY`
	`REPLAY_TYPE = PHYSICAL`
	
	Pour terminer la migration vers AWS, dirigez les connexions de l'application vers Db2 sur Amazon EC2.	

Résolution des problèmes

Problème	Solution
Si vous utilisez le NAT pour des raisons de pare-feu et de sécurité, l'hôte peut avoir deux adresses IP (une interne et une externe), ce qui peut entraîner un échec de la vérification de l'adresse IP HADR. La `START HADR ON DATABASE` commande renverra le message suivant : `HADR_LOCAL_HOST:HADR_LOCAL_SVC (-xx-xx-xx-xx.:50011 (xx.xx.xx .xx:50011)) on remote database is different from HADR_REMOTE_HOST:H ADR_REMOTE_SVC (xx-xx-xx- xx.:50011 (x.x.x.x:50011)) on local database.`	Pour prendre en charge le HADR dans un environnement NAT, vous pouvez configurer le `HADR_LOCAL_HOST` avec l'adresse interne et externe. Par exemple, si le serveur DB2 possède le nom interne `host1` et le nom externe`host1E`, cela `HADR_LOCAL_HOST` peut être `HADR_LOCAL_HOST: "host1 | host1E"` le cas.

Ressources connexes

- Opérations de sauvegarde et de restauration DB2 entre différents systèmes d'exploitation et plateformes matérielles
- Configurer Db2 STORAGE ACCESS ALIAS et REMOTE DB2
- Reprise après sinistre à haute disponibilité Db2
- hadr_syncmode - Mode de synchronisation HADR pour les écritures de journal dans le paramètre de configuration de l'état homologue

Migrer une base de données Microsoft SQL Server sur site vers Amazon à EC2 l'aide du service de migration d'applications

Créée par Senthil Ramasamy (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'une base de données Microsoft SQL Server d'un centre de données sur site vers une instance Amazon Elastic Compute Cloud EC2 (Amazon). Il utilise le AWS Application Migration Service (AWS MGN) pour réhéberger votre base de données à l'aide d'une migration automatique lift-and-shift. AWS MGN effectue une réplication au niveau des blocs de votre serveur de base de données source.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une base de données Microsoft SQL Server source dans un centre de données sur site

Limites

- La bande passante de votre réseau peut être limitée entre le centre de données sur site et AWS.
- AWS MGN est limité aux bases de données hébergées sur des serveurs autonomes dotés d'un stockage dédié. Il ne prend pas en charge la migration de systèmes de base de données en cluster ni de systèmes de base de données dont le taux de modification dépasse le débit du réseau.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Versions du produit

- Toutes les versions de la base de données Microsoft SQL Server
- Systèmes d'exploitation Windows et Linux compatibles avec AWS MGN

Architecture

Pile technologique source

Une base de données Microsoft SQL Server sur site

Pile technologique cible

Une base de données Microsoft SQL Server sur une EC2 instance Amazon

Architecture cible

Cette architecture utilise AWS MGN pour répliquer les données d'un centre de données d'entreprise sur site vers. AWS Le schéma montre le processus de réplication des données, les communications avec les API, ainsi que les phases de test et de transition.

1. Réplication des données :
   - AWS MGN réplique les données du centre de données d'entreprise sur site vers le centre de données de l'entreprise AWS et lance une réplication continue des modifications.
   - Les serveurs de réplication du sous-réseau intermédiaire reçoivent et traitent les données.
2. Communication avec l'API :
   - Les serveurs de réplication se connectent aux points de terminaison d'API AWS MGN EC2, Amazon et Amazon Simple Storage Service (Amazon S3) via le port TCP 443.
   - AWS MGN gère la migration.
   - Amazon EC2 gère les opérations des instances.
3. Test et découpage :
   - Les instances de test sont lancées dans le sous-réseau opérationnel à l'aide de données répliquées.
   - Une fois les tests réussis, AWS MGN crée des instances de transition pour la migration finale.

Outils

- AWS Application Migration Service (AWS MGN) vous aide à réhéberger (transférer et déplacer) des applications AWS Cloud sans modification et avec un minimum de temps d'arrêt.
- AWS Direct Connectrelie votre réseau interne à un point Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les AWS services publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Bonnes pratiques

- Configurez des points de terminaison régionaux d'API pour AWS MGN EC2, Amazon et Amazon S3 dans le cloud privé virtuel (VPC) afin d'interdire l'accès public depuis Internet.
- Configurez les paramètres de lancement AWS MGN pour lancer les serveurs de base de données cibles dans un sous-réseau privé.
- N'autorisez que les ports requis dans les groupes de sécurité de base de données.
- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Configuration d'AWS MGN

Tâche	Description	Compétences requises
Configurez AWS MGN.	Recherchez le AWS Application Migration Service dans le AWS Management Console et lancez le processus de configuration. Cela créera un modèle de réplication et vous redirigera vers la page des serveurs source de la console MGN. Lorsque vous configurez le service MGN, choisissez un rôle de service dans la liste générée.	DBA, ingénieur en migration

Tâche	Description	Compétences requises
Ajoutez un serveur source.	Ajoutez les détails de votre serveur de base de données source sur site, puis ajoutez le serveur.	DBA, ingénieur en migration
Installez l'agent AWS MGN sur le serveur source.	Téléchargez le programme d'installation de l'agent AWS MGN sur votre système local et transférez-le sur votre serveur de base de données source. Pour valider le hachage du programme d'installation, voir Validation du programme d'installation de l'agent de AWS réplication téléchargé pour Windows 2012.	DBA, ingénieur en migration

Installation de l'agent AWS MGN sur les machines sources

Tâche	Description	Compétences requises
Générez les informations d'identification IAM du client.	Avant d'installer l'agent AWS MGN, générez des AWS informations d'identification en créant un nouvel utilisateur IAM doté des autorisations appropriées. Pour plus d'informations, consultez les politiques gérées par AWS AWS Application Migration Service et la	DBA, ingénieur en migration

Tâche	Description	Compétences requises
	génération des AWS informations d'identification requises.	
Installez l'agent sur le serveur source.	Installez l'agent sur la machine source qui héberge la base de données Microsoft SQL Server. Pour plus d'informations, consultez la section Installation de l'agent de AWS réplication sur les serveurs Windows. Fournissez les informations d'identification AWS suivantes : • Région AWS • AWS ID de clé d'accès • AWS clé d'accès secrète Vos AWS informations d'identification uniques permettent à l'agent AWS MGN de s'authentifier et d'effectuer des tâches de migration.	Propriétaire de l'application, DBA, ingénieur en migration

Tâche	Description	Compétences requises
Choisissez les disques à répliquer.	Après avoir saisi vos AWS informations d'identification, le programme d'installation vérifie que votre serveur répond aux exigences minimales pour l'installation de l'agent (par exemple, si le serveur dispose de suffisamment d'espace disque pour installer l'agent AWS MGN). Le programme d'installation affiche les étiquettes des volumes et les informations relatives au stockage. Pour répliquer votre base de données à l'aide du service AWS MGN, sélectionnez les disques appropriés sur votre serveur source. Entrez le chemin de chaque disque, séparé par des virgules. Si vous souhaitez répliquer tous les disques, laissez le chemin vide. Après avoir confirmé les disques sélectionnés, l'installation se poursuit.	DBA, ingénieur en migration

Tâche	Description	Compétences requises
Surveillez la progression de la synchronisation.	AWS L'agent de réplicati on lance le processus de synchronisation en prenant d'abord un instantané des disques sélectionnés, puis en répliquant les données. Vous pouvez suivre la progression de la synchroni sation depuis la page Serveur source de la console AWS MGN. Pour plus d'informa tions, voir Surveiller le serveur pendant le cycle de vie de la migration.	DBA, ingénieur en migration

Réplication à l'aide d'AWS MGN

Tâche	Description	Compétences requises
Gérez la progression de la réplication.	Une fois la synchronisation initiale lancée, votre serveur source apparaît dans la console AWS MGN, où vous pouvez gérer et surveiller la migration. La console affiche une estimation de la durée de réplication complète, basée sur la taille totale des disques sélectionnés et la bande passante réseau disponible.	DBA, ingénieur en migration
Vérifiez la synchronisation.	Une fois les disques du serveur source entièrement synchronisés, vérifiez que	Propriétaire de l'application, DBA, ingénieur en migration

Tâche	Description	Compétences requises
	tous les disques sélection nés sont répertoriés comme étant entièrement synchroni sés et qu'aucune erreur n'est signalée dans la console. La console AWS MGN fera ensuite passer automatiq uement l'état du cycle de vie de migration à Prêt pour les tests, ce qui indique que l'environnement répliqué AWS est prêt pour les tests de performances et de fonctionn alités.	

Testez et découpez

Tâche	Description	Compétences requises
Configurez les paramètres de lancement.	Choisissez le serveur source dans la console AWS MGN et mettez à jour les paramètre s de lancement de l'instanc e de test cible. Sur la page de détails du serveur source, accédez à l'onglet Paramètres de lancement pour configurer l'instance de test. Choisissez un type d'instance rentable et un type de volume Amazon Elastic Block Store (Amazon EBS), puis configure z les groupes de sécurité et	DBA, ingénieur en migration

Tâche	Description	Compétences requises
	les exigences du réseau. Pour plus d'informations, consultez la section Paramètres de lancement.	
Lancez l'instance de test cible.	Accédez à la console AWS MGN de votre machine source synchronisée et lancez une instance de test cible en choisissant Test and cut over, puis Launch test instances. Cela crée une tâche de lancement qui déploie l'instance de test en utilisant les paramètres que vous avez configurés. L'instance est lancée dans l'environnement de votre serveur de base de données source AWS Cloud et le réplique. Surveillez la progression du lancement depuis la page Historique des lancements, où vous pouvez suivre la création de l'instance et résoudre les éventuels problèmes.	DBA, ingénieur en migration

Tâche	Description	Compétences requises
Validez l'instance de test cible.	Validez le serveur EC2 de base de données Amazon : 1. Assurez-vous que la console AWS MGN indique que l'instance de test s'exécute correctement. 2. Utilisez un client RDP pour vous connecter. 3. Dans le menu Démarrer, ouvrez le Gestionnaire de configuration SQL Server. 4. Vérifiez l'état des services SQL Server, y compris SQL Server (`MSSQLSERVER`) et SQL Server Agent, en vous assurant qu'ils sont intacts et qu'ils sont définis sur le type de démarrage correct. 5. Comparez les paramètre s et les configurations de disque entre l'instance de test et le serveur de base de données source pour vérifier que les lettres de lecteur, les volumes, les allocations de disque et les répertoires nécessaires sont correctement mappés. 6. Connectez-vous au serveur SQL sur l' EC2 instance Amazon de test et vérifiez que toutes les bases de données sources ont migré	DBA, ingénieur en migration

Tâche	Description	Compétences requises
	et apparaissent dans la liste des bases de données. Effectuez des tests de validation pour vous assurer que la base de données fonctionne comme prévu.	

Tâche	Description	Compétences requises

Renommez le serveur.	AWS La migration MGN implique une copie au niveau du stockage de votre serveur source sur site. Votre EC2 instance SQL Server contient uniquement les informati ons du serveur source d'origine dans ses fichiers binaires. Mettez donc à jour les informations binaires pour qu'elles reflètent le nom du nouveau serveur.
	
	1. Utilisez SQL Server Management Studio (SSMS) pour vous connecter à votre EC2 instance SQL Server.
	2. Vérifiez le nom du serveur :
	
	`SELECT @@SERVERNAME AS 'Current Server Name';`
	
	3. Renommez l'instance SQL Server en la `NEW_SERVE R_NAME` remplaçant par le nom de votre serveur :
	
	`EXEC sp_dropserver 'OLD_SERVER_NAME'`
	`EXEC sp_addserver 'NEW_SERVER_NAME', 'local';`
	
	4. Vérifiez que le nom du serveur est correct :
		DBA, ingénieur en migration

Tâche	Description	Compétences requises
	``` SELECT @@SERVERNAME AS 'Updated Server Name'; ``` 5. Redémarrez l'instance SQL Server.	

Tâche	Description	Compétences requises
Lancez l'instance de transition.	Dans la console AWS MGN, sur la page Serveurs source, vérifiez que l'état du cycle de vie de migration du serveur est « Prêt pour le passage ». Configurez les paramètres de lancement de l'instance de transition, en veillant à ce qu'ils reflètent votre environnement sur site. Avant de lancer le transfert, arrêtez votre base de données locale, ce qui garantit les points suivants : • Toutes les transactions en cours sont terminées. • Aucune nouvelle transaction n'aura lieu pendant le processus de transfert. • La synchronisation des données entre les disques source et cible est terminée. Initiez l'instance de transition dans la console AWS MGN. Lorsque l'instance de transition est opérationnelle, connectez-vous à l'instance et effectuez les tests suivants : 1. Assurez-vous que SQL Server démarre correctem	Propriétaire de l'application, DBA, ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	ent et que les bases de données sont accessibles. 2. Vérifiez que vos données sont intactes et cohérentes avec le serveur source. 3. Exécutez tous les tests d'application pour vérifier qu'ils fonctionnent comme prévu. 4. Dans la console AWS MGN, définissez l'état de migration sur Cutover complete. 5. Commencez à acheminer le trafic vers l' EC2 instance.	

Résolution des problèmes

Problème	Solution
La synchronisation initiale échoue à l'étape d'authentification.	Il s'agit d'un problème de connectivité réseau. Le serveur de réplication ne peut pas se connecter à AWS MGN.

Ressources connexes

Documentation AWS

- Commencer avec AWS Application Migration Service
- Migrer une base de données Microsoft SQL Server sur site vers Amazon EC2
- Qu'est-ce que Microsoft SQL Server sur Amazon EC2 ?

Vidéos

- Effectuer une migration par levage et changement de vitesse avec AWS Application Migration Service (vidéo)

Migrez VMware VMs avec HCX Automation à l'aide de PowerCLI

Créée par Giri Nadiminty (AWS), Hassan Adekoya (AWS) et Naveen Deshwal

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

Ce modèle décrit comment migrer des machines virtuelles VMware sur site (VMs) vers le VMware cloud sur AWS à l'aide de l'automatisation VMware Hybrid Cloud Extension (HCX) basée sur des scripts VMware PowerCLI. PowerCLI est un outil de ligne de commande basé sur Windows. PowerShell Il vous aide à gérer les VMware logiciels et automatise les tâches d'infrastructure et de migration.

Vous pouvez adapter ce modèle pour la migration entre n'importe quelle combinaison de vCenters, de centres de données définis par logiciel (SDDCs) et d'environnements cloud. Les scripts PowerCLI inclus dans ce modèle utilisent l'automatisation plutôt que des clics de souris pour toutes les tâches de configuration et de planification des machines virtuelles. Ils permettent ainsi de gagner du temps dans les activités de migration et de réduire le risque d'erreur humaine.

Conditions préalables et limitations

Prérequis

- Un compte VMware Cloud on AWS avec SDDC
- Un vCenter ou un SDDC existant sur site ou dans le cloud
- Un compte utilisateur disposant des autorisations nécessaires pour les vCenters source et de destination ou SDDCs
- Couplage de sites HCX avec l'extension réseau HCX (HCX-NE) configuré entre les vCenters source et de destination ou SDDCs
- VMware PowerCLI installé sur le serveur de votre choix

Limites

- Si le vCenter source utilise Cross-vCenter NSX, le module PowerCLI ne fonctionnera pas. Utilisez une méthode de script (telle que Python) avec l'API HCX au lieu de PowerCLI.
- Si les personnes migrées VMs ont besoin de nouveaux noms ou adresses IP, utilisez une méthode de script (telle que Python) avec l'API HCX.
- Ce modèle ne remplit pas le fichier .csv, qui est obligatoire. Vous pouvez remplir le fichier à l'aide de VMware vRealize Network Insight (vRNI) ou d'une autre méthode.

Versions du produit

- VMware vSphere version 5 ou ultérieure
- VMware HCX version 4.4 ou ultérieure
- VMware PowerCLI version 12.7 ou ultérieure

Architecture

Pile technologique source

- Sur site ou dans le cloud VMware

Pile technologique cible

- VMware Cloud sur AWS

Architecture cible

Outils

Services AWS

- VMware Cloud on AWS est un service conçu conjointement par AWS pour vous aider VMware à migrer et à étendre vos environnements VMware vSphere sur site vers le cloud AWS.

Autres outils

- VMware Hybrid Cloud Extension (HCX) est un utilitaire permettant de migrer des charges de travail de votre VMware environnement sur site vers Cloud VMware on AWS sans modifier la

plateforme sous-jacente. Remarque : Ce produit était auparavant connu sous le nom de Hybrid Cloud Extension et NSX Hybrid Connect. Ce modèle utilise HCX pour la migration des machines virtuelles.

- VMware PowerCLI est un outil de ligne de commande permettant d'automatiser la gestion de vSphere et de vCloud VMware . Vous exécutez des commandes PowerCLI sous Windows à l'aide PowerShell PowerShell d'applets de commande. Ce modèle utilise PowerCLI pour exécuter des commandes de migration.

Code

Script simple et autonome

Nous vous recommandons d'utiliser ce script mono-machine pour les tests initiaux, afin de vérifier que les options de configuration sont acceptées et se comportent comme prévu. Pour obtenir des instructions, consultez la section Epics.

```
<# Manual Variables #>
$HcxServer = "[enterValue]"
$SrcNetworkName = "[enterValue]"
$DstNetworkName = "[enterValue]"
$DstComputeName = "[enterValue]"
$DstDSName = "[enterValue]"
$DstFolderName = "[enterValue]"
$vmName = "[enterValue]"

<# Environment Setup #>
Connect-HCXServer -Server $HcxServer
$HcxDstSite = Get-HCXSite -Destination
$HcxSrcSite = Get-HCXSite -Source
$SrcNetwork = Get-HCXNetwork -Name $SrcNetworkName -Type VirtualWire -Site $HcxSrcSite
$DstNetwork = Get-HCXNetwork -Name $DstNetworkName -Type NsxtSegment -Site $HcxDstSite
$DstCompute = Get-HCXContainer -Name $DstComputeName -Site $HcxDstSite
$DstDS = Get-HCXDatastore -Name $DstDSName -Site $HcxDstSite
$DstFolder = Get-HCXContainer -name $DstFolderName -Site $HcxDstSite
$vm = Get-HCXVM -Name $vmName

<# Migration #>
$NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -DestinationNetwork
 $DstNetwork
$NewMigration = New-HCXMigration -VM $vm -MigrationType vMotion -SourceSite $HcxSrcSite
 -DestinationSite $HcxDstSite -Folder $DstFolder -TargetComputeContainer $DstCompute
```

```
 -TargetDatastore $DstDS -NetworkMapping $NetworkMapping -DiskProvisionType Thin
 -UpgradeVMTools $True -RemoveISOs $True -ForcePowerOffVm $True -RetainMac $True -
UpgradeHardware $True -RemoveSnapshots $True
```

Script complet basé sur .csv

Une fois les tests terminés, vous pouvez utiliser le script suivant dans vos environnements de production. Pour obtenir des instructions, consultez la section Epics.

```
<# Schedule #>
write-host("Getting Time for Scheduling")
$startTime = [DateTime]::Now.AddDays(12)
$endTime = [DateTime]::Now.AddDays(15)

<# Migration #>
Connect-HCXServer -Server [enterValue]
write-host("Getting Source Site")
$HcxSrcSite = Get-HCXSite
write-host("Getting Target Site")
$HcxDstSite = Get-HCXSite -Destination
$HCXVMS = Import-CSV .\Import_VM_list.csv
ForEach ($HCXVM in $HCXVMS) {
    $DstFolder = Get-HCXContainer $HCXVM.DESTINATION_VM_FOLDER -Site $HcxDstSite
    $DstCompute = Get-HCXContainer $HCXVM.DESTINATION_COMPUTE  -Site $HcxDstSite
    $DstDatastore = Get-HCXDatastore $HCXVM.DESTINATION_DATASTORE -Site $HcxDstSite
    $SrcNetwork = Get-HCXNetwork $HCXVM.SOURCE_NETWORK -Type VirtualWire -Site
 $HcxSrcSite
    $DstNetwork = Get-HCXNetwork $HCXVM.DESTINATION_NETWORK -Type NsxtSegment -Site
 $HcxDstSite
    $NetworkMapping = New-HCXNetworkMapping -SourceNetwork $SrcNetwork -
DestinationNetwork $DstNetwork
    $NewMigration = New-HCXMigration -VM (Get-HCXVM $HCXVM.VM_NAME) -MigrationType
 Bulk -SourceSite $HcxSrcSite -DestinationSite $HcxDstSite -Folder $DstFolder -
TargetComputeContainer $DstCompute -TargetDatastore $DstDatastore -NetworkMapping
 $NetworkMapping -DiskProvisionType Thin -UpgradeVMTools $True -RemoveISOs $True -
ForcePowerOffVm $True -RetainMac $True -UpgradeHardware $True -RemoveSnapshots $True -
ScheduleStartTime $startTime -ScheduleEndTime $endTime
    Start-HCXMigration -Migration $NewMigration -Confirm:$false
}
```

Épopées

Collectez des informations pour les variables manuelles

Tâche	Description	Compétences requises
Trouvez les noms des serveurs vCenter et SDDC source et de destination.	Les scripts PowerCLI nécessitent les variables décrites dans cette épopée. Vous pouvez recueillir ces informations à l'avance pour faciliter l'utilisation des scripts. Dans la section HCX de la console vSphere, choisisse z Infrastructure, Site Pairing. Notez les noms des serveurs source et de destination affichés.	Architecte du cloud
Trouvez les noms HCX source et destination.	Dans la section HCX de la console vSphere, choisissez System, Administration. Notez les noms HCX de source et de destination qui sont affichés.	Architecte du cloud
Trouvez les noms des réseaux source et de destination.	Dans la section HCX de la console vSphere, choisissez System, Network Extension. Notez les noms des réseaux source et de destination. **Note** Vous pouvez également obtenir les noms des réseaux source et de destinati	Architecte du cloud

Tâche	Description	Compétences requises
	on à l'aide des commandes PowerCLI HCXNetworkGet-HCXNetwork -Destination après vous être connecté au serveur HCX.	
Collectez des informations supplémentaires à partir de la console vSphere.	Sur la console vSphere, collectez les informations suivantes : • Noms des VMs personnes que vous souhaitez migrer • Environnement informatique de destination (cluster/hôte) • Banque de données de destination • Nom du dossier de la machine virtuelle de destination	Architecte du cloud

Prendre des décisions en matière de migration

Tâche	Description	Compétences requises
Déterminez les options de migration.	Déterminez les éléments suivants : • `MigrationType` — Les types de migration assistée par HCX sont VMotion, Bulk, Cold et RAV. Votre choix dépend de vos	Architecte du cloud

Tâche	Description	Compétences requises
	besoins en temps d'arrêt, de la bande passante du réseau, du délai de migration et du type de charge de travail. Pour plus d'informations, consultez le billet de blog AWS Migrating Workloads to VMware Cloud on AWS with Hybrid Cloud Extension (HCX). • `DiskProvisionType (Thin, Thick)` • `UpgradeVMTools ($True, $False)` • `RemoveISOs ($True, $False)` • `ForcePowerOffVm ($True, $False)` • `RetainMac ($True, $False)` • `UpgradeHardware ($True, $False)` • `RemoveSnapshots ($True, $False)` Pour plus d'informations sur chaque option, consultez la documentation destinée aux VMware développeurs.	

Exécutez le script simple pour les tests initiaux

Tâche	Description	Compétences requises
Copiez le script.	La version simple du script est intégrée dans un seul fichier. Vous pouvez l'utiliser pour tester la migration d'une seule machine. Copiez le premier script de la section Code de ce modèle et stockez-le sur l'ordinateur sur lequel le module VMware PowerCLI est installé. (Pour installer PowerCLI, suivez les instructions de la VMware documentation.)	Architecte du cloud
Définissez les variables de script.	Définissez toutes les variables dans la `Manual Variables` section du script.	Architecte du cloud
Définissez les variables de migration.	Définissez tous les `New-HCXMigration` paramètres dans la `Migration` section du script.	Architecte du cloud
Spécifiez les sites.	(Facultatif) Si la source ou la destination comporte plusieurs sites, spécifiez les sites manuellement dans la `Environment Setup` section du script. Si la source et la destination ont des sites uniques, le script	Architecte du cloud

Tâche	Description	Compétences requises
	recherchera automatiquement les informations.	
Exécutez le script.	Sur le serveur où PowerCLI est installé, à partir d'une PowerShell fenêtre surélevée , exécutez le script et entrez vos informations d'identif ication lorsque vous y êtes invité.	Architecte du cloud
Validez le script.	Vérifiez que la migration des machines virtuelles a été lancée.	Architecte du cloud

Exécutez le script complet pour migrer plusieurs VMs

Tâche	Description	Compétences requises
Créez et remplissez le fichier .csv.	Créez un fichier .csv appelé `Import_VM_list.csv` sur votre ordinateur et remplissez-le avec l'exemple de contenu suivant : `VM_NAME,DESTINATIO N_VM_FOLDER,DESTIN ATION_COMPUTE,DEST INATION_DATASTORE, SOURCE_NETWORK,DES TINATION_NETWORK [enterValue],[enter Value],[enterValue ],[enterValue],[en terValue],[enterVa lue]`	Architecte du cloud

Tâche	Description	Compétences requises
	Remplacez chaque `[enterValue]` élément du fichier .csv par les informations que vous avez collectées précédemment. **Note** Vous pouvez remplir le fichier .csv à l'aide de VMware vRealize Network Insight (vRNI) ou d'une autre méthode.	
Copiez le script.	La version complète du script utilise les informations d'un fichier .csv externe pour en migrer automatiquement plusieurs. VMs Copiez le second script de la section Code de ce modèle et stockez-le sur l'ordinateur sur lequel le module VMware PowerCLI est installé, dans le même dossier que le fichier .csv.	Architecte du cloud

Tâche	Description	Compétences requises
Modifiez le script.	Modifiez le script pour apporter les modifications suivantes : • Ligne 7 : Définissez la variable du serveur HCX (`Connect-HCXServer`). • Ligne 12 : (Facultatif) Si vous définissez le nom de fichier .csv différemment, mettez-le à jour. • Lignes 3 et 4 : (Facultatif) Définissez l'horaire. • Ligne 20 : (Facultatif) Spécifiez les `New-HCXMigration` paramètres dans la `Migration` section. • Lignes 9 et 11 : (Facultatif) Si la source ou la destination inclut plusieurs sites, spécifiez les sites souhaités manuellement.	Architecte du cloud
Exécutez le script.	Sur le serveur où PowerCLI est installé, à partir d'une PowerShell fenêtre surélevée , exécutez le script et entrez vos informations d'identification lorsque vous y êtes invité.	Architecte du cloud
Validez le script.	Vérifiez que la migration des machines virtuelles a été lancée.	Architecte du cloud

Résolution des problèmes

Problème	Solution
Le script échoue avec le message d'erreur suivant : « Tous les réseaux sources ne sont pas mappés à la cible ! »	Si le vCenter source utilise Cross-vCenter NSX, le module PowerCLI ne fonctionnera pas. Utilisez une méthode de script (telle que Python) avec l'API HCX au lieu de PowerCLI. Il s'agit d'une limitation connue du script PowerCLI.
Le script échoue avec le message d'erreur suivant : « HCXServer Erreur de connexion : non autorisée »	Les informations d'identification que vous avez saisies ne fournissent pas les autorisations nécessaires.

Ressources connexes

- Migration de charges de travail vers VMware le cloud sur AWS avec Hybrid Cloud Extension (HCX) (article de blog AWS)
- Choix d'une approche de migration pour déplacer vos VMware applications et charges de travail vers le cloud AWS (AWS Prescriptive Guidance)
- Migrer le VMware SDDC vers le VMware cloud sur AWS à l'aide de VMware HCX (AWS Prescriptive Guidance)
- Commencer à utiliser le module HCX (article de VMware blog)

Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS

Créée par Will Bauer (AWS)

Récapitulatif

Organisations cherchent à migrer vers le cloud Amazon Web Services (AWS) afin d'accroître leur agilité et leur résilience. Après avoir migré vos solutions de sécurité et de gestion du trafic F5 BIG-IP vers le cloud AWS, vous pouvez vous concentrer sur l'agilité et l'adoption de modèles opérationnels à forte valeur ajoutée dans l'architecture de votre entreprise.

Ce modèle décrit comment migrer une charge de travail F5 BIG-IP vers une charge de travail F5 BIG-IP Virtual Edition (VE) sur le cloud AWS. La charge de travail sera migrée en réhébergeant l'environnement existant et en déployant certains aspects de la replateforme, tels que la découverte de services et les intégrations d'API. CloudFormation Les modèles AWS accélèrent la migration de votre charge de travail vers le cloud AWS.

Ce modèle est destiné aux équipes d'ingénierie technique et d'architecture qui migrent des solutions de sécurité et de gestion du trafic F5, et accompagne le guide Migration de F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS sur le site Web AWS Prescriptive Guidance.

Conditions préalables et limitations

Prérequis

- Charge de travail F5 BIG-IP existante sur site.
- Licences F5 existantes pour les versions BIG-IP VE.
- Un compte AWS actif.
- Cloud privé virtuel (VPC) existant configuré avec une sortie via une passerelle NAT ou une adresse IP élastique, et configuré avec accès aux points de terminaison suivants : Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (EC2Amazon), AWS Security Token Service (AWS STS) et Amazon. CloudWatch Vous pouvez également modifier l'architecture VPC modulaire et évolutive Quick Start comme élément de base de vos déploiements.
- Une ou deux zones de disponibilité existantes, selon vos besoins.
- Trois sous-réseaux privés existants dans chaque zone de disponibilité.
- CloudFormation Modèles AWS, disponibles dans le GitHub référentiel F5.

Au cours de la migration, vous pouvez également utiliser les éléments suivants, en fonction de vos besoins :

- Une extension F5 Cloud Failover pour gérer le mappage des adresses IP élastiques, le mappage des adresses IP secondaires et les modifications des tables de routage.
- Si vous utilisez plusieurs zones de disponibilité, vous devrez utiliser les extensions F5 Cloud Failover pour gérer le mappage IP élastique vers les serveurs virtuels.
- Vous devriez envisager d'utiliser F5 Application Services 3 (AS3), F5 Application Services Templates (FAST) ou un autre modèle d'infrastructure sous forme de code (IaC) pour gérer les configurations. La préparation des configurations dans un modèle IaC et l'utilisation de référentiels de code faciliteront la migration et vos efforts de gestion continus.

Expertise

- Ce modèle nécessite de connaître la manière dont un ou plusieurs VPCs peuvent être connectés aux centres de données existants. Pour plus d'informations à ce sujet, consultez les options de connectivité Network-to-Amazon VPC dans la documentation Amazon VPC.
- Il est également nécessaire de connaître les produits et modules F5, notamment le système d'exploitation de gestion du trafic (TMOS), le gestionnaire de trafic local (LTM), le gestionnaire de trafic mondial (GTM), le gestionnaire de politiques d'accès (APM), le gestionnaire de sécurité des applications (ASM), le gestionnaire de pare-feu avancé (AFM)et le BIG-IQ.

Versions du produit

- Nous vous recommandons d'utiliser F5 BIG-IP version 13.1 ou ultérieure, bien que le modèle soit compatible avec F5 BIG-IP version 12.1 ou ultérieure.

Architecture

Pile technologique source

- Charge de travail F5 BIG-IP

Pile technologique cible

- Amazon CloudFront

- Amazon CloudWatch
- Amazon EC2
- Amazon S3
- Amazon VPC
- AWS Global Accelerator
- AWS STS
- AWS Transit Gateway
- V5 À GRANDE OUVERTURE

Architecture cible

Outils

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- Amazon CloudFront accélère la diffusion de votre contenu Web en le diffusant via un réseau mondial de centres de données, ce qui réduit le temps de latence et améliore les performances.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Security Token Service (AWS STS) vous aide à demander des informations d'identification temporaires à privilèges limités pour les utilisateurs.
- AWS Transit Gateway est un hub central qui connecte des clouds privés virtuels (VPCs) et des réseaux sur site.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que

vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Épopées

Découverte et évaluation

Tâche	Description	Compétences requises
Évaluez les performances du F5 BIG-IP.	Collectez et enregistrez les indicateurs de performance des applications sur le serveur virtuel, ainsi que les indicateurs des systèmes qui seront migrés. Cela permettra de dimensionner correctement l'infrastructure AWS cible pour une meilleure optimisation des coûts.	F5 Architecte, ingénieur et architecte réseau, ingénieur
Évaluez le système d'exploitation et la configuration du F5 BIG-IP.	Évaluez quels objets seront migrés et si une structure de réseau doit être maintenue, par exemple VLANs.	F5 Architecte, ingénieur
Évaluez les options de licence F5.	Évaluez le modèle de licence et de consommation dont vous aurez besoin. Cette évaluation doit être basée sur votre évaluation du système d'exploitation et de la configuration du F5 BIG-IP.	F5 Architecte, ingénieur
Évaluez les applications publiques.	Déterminez quelles applications nécessiteront des adresses IP publiques. Alignez ces applications sur les instances et les clusters requis	Architecte F5, architecte cloud, architecte réseau, ingénieur, équipes d'applications

Tâche	Description	Compétences requises
	pour répondre aux exigences de performance et d'accord de niveau de service (SLA).	
Évaluez les candidatures internes.	Évaluez les applications qui seront utilisées par les utilisateurs internes. Assurez-vous de savoir où se situent ces utilisateurs internes au sein de l'organisation et comment ces environnements se connectent au cloud AWS. Vous devez également vous assurer que ces applications peuvent utiliser le système de noms de domaine (DNS) dans le cadre du domaine par défaut.	Architecte F5, architecte cloud, architecte réseau, ingénieur, équipes d'applications
Finalisez l'AMI.	Toutes les versions de F5 BIG-IP ne sont pas créées en tant qu'Amazon Machine Images (). AMIs Vous pouvez utiliser l'outil de génération d'images F5 BIG-IP si vous avez des versions spécifiques d'ingénierie de correction rapide (QFE) requises. Pour plus d'informations sur cet outil, consultez la section « Ressources associées ».	Architecte F5, architecte cloud, ingénieur
Finalisez les types et l'architecture des instances.	Décidez des types d'instances, de l'architecture VPC et de l'architecture interconnectée.	Architecte F5, architecte cloud, architecte réseau, ingénieur

Activités complètes liées à la sécurité et à la conformité

Tâche	Description	Compétences requises
Documentez les politiques de sécurité F5 existantes.	Collectez et documentez les politiques de sécurité F5 existantes. Assurez-vous d'en créer une copie dans un référentiel de code sécurisé.	F5 Architecte, ingénieur
Chiffrez l'AMI.	(Facultatif) Votre organisation peut avoir besoin de chiffrer les données au repos. Pour plus d'informations sur la création d'une image personnalisée Bring Your Own License (BYOL), consultez la section « Ressources associées ».	Architecte F5, ingénieur, architecte cloud, ingénieur
Durcissez les appareils.	Cela aidera à vous protéger contre les vulnérabilités potentielles.	F5 Architecte, ingénieur

Configurez votre nouvel environnement AWS

Tâche	Description	Compétences requises
Créez des comptes Edge et Security.	Connectez-vous à la console de gestion AWS et créez les comptes AWS qui fourniront et géreront les services de périphérie et de sécurité. Ces comptes peuvent être différents de ceux qui fonctionnent VPCs pour les services et applications partagés. Cette	Architecte cloud, ingénieur

Tâche	Description	Compétences requises
	étape peut être réalisée dans le cadre d'une zone d'atterri ssage.	
Déployez la périphérie et la sécurité VPCs.	Configurez et configurez les éléments VPCs nécessaires pour fournir des services de périphérie et de sécurité.	Architecte cloud, ingénieur
Connectez-vous au centre de données source.	Connectez-vous au centre de données source qui héberge votre charge de travail F5 BIG-IP.	Architecte cloud, architecte réseau, ingénieur
Déployez les connexions VPC.	Connectez le service Edge et de sécurité VPCs à l'applica tion VPCs.	Architecte réseau, ingénieur
Déployez les instances.	Déployez les instances en utilisant les CloudFormation modèles AWS de la section « Ressources associées ».	F5 Architecte, ingénieur
Testez et configurez le basculement de l'instance.	Assurez-vous que le modèle AWS Advanced HA iApp ou l'extension F5 Cloud Failover sont configurés et fonctionnent correctement.	F5 Architecte, ingénieur

Configuration de la mise en réseau

Tâche	Description	Compétences requises
Préparez la topologie VPC.	Ouvrez la console Amazon VPC et assurez-vous que votre VPC dispose de tous les	Architecte réseau, architecte F5, architecte cloud, ingénieur

Tâche	Description	Compétences requises
	sous-réseaux et protections requis pour le déploiement de F5 BIG-IP VE.	
Préparez vos points de terminaison VPC.	Préparez les points de terminaison VPC pour Amazon, Amazon EC2 S3 et AWS STS si une charge de travail F5 BIG-IP n'a pas accès à une passerelle NAT ou à une adresse IP élastique sur une interface TMM.	Architecte cloud, ingénieur

Migrer les données

Tâche	Description	Compétences requises
Migrez la configuration.	Migrez la configuration F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS.	F5 Architecte, ingénieur
Associez le secondaire IPs.	Les adresses IP des serveurs virtuels ont une relation avec les adresses IP secondair es attribuées aux instances . Attribuez des adresses IP secondaires et assurez-vous que l'option « Autoriser le remappage/la réaffectation » est sélectionnée.	F5 Architecte, ingénieur

Configurations de test

Tâche	Description	Compétences requises
Validez les configurations du serveur virtuel.	Testez les serveurs virtuels.	Architecte F5, équipes d'applications

Finaliser les opérations

Tâche	Description	Compétences requises
Créez la stratégie de sauvegarde.	Les systèmes doivent être arrêtés pour créer un instantané complet. Pour plus d'informations, consultez « Mise à jour d'une machine virtuelle F5 BIG-IP » dans la section « Ressources associées ».	Architecte F5, architecte cloud, ingénieur
Créez le runbook de basculement du cluster.	Assurez-vous que le processus d'exécution du failover est terminé.	F5 Architecte, ingénieur
Configurez et validez la journalisation.	Configurez F5 Telemetry Streaming pour envoyer les journaux aux destinations requises.	F5 Architecte, ingénieur

Terminez le découpage

Tâche	Description	Compétences requises
Passons au nouveau déploiement.		Architecte F5, architecte cloud, architecte réseau, ingénieur, AppTeams

Ressources connexes

Guide de migration

- Migration de F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS

Ressources F5

- CloudFormation Modèles AWS dans le référentiel F5 GitHub
- F5 sur AWS Marketplace
- Présentation du F5 BIG-IP VE
- Exemple de démarrage rapide - Édition virtuelle BIG-IP avec WAF (LTM + ASM)
- Services applicatifs F5 sur AWS : présentation (vidéo)
- Guide de l'utilisateur de l'extension F5 Application Services 3
- Documentation sur le cloud F5
- Wiki REST F5 iControl
- F5 Vue d'ensemble des fichiers de configuration uniques (11.x - 15.x)
- Laboratoire de topologie F5
- Livres blancs F5
- Outil de génération d'images F5 BIG-IP
- Mise à jour d'une machine virtuelle F5 BIG-IP VE
- Présentation de l'option « platform-migrate » de l'archive UCS

Migrer une application Web Go sur site vers AWS Elastic Beanstalk à l'aide de la méthode binaire

Créée par Suhas Basavaraj (AWS) et Shumaz Mukhtar Kazi (AWS)

Récapitulatif

Ce modèle décrit comment migrer une application Web Go sur site vers AWS Elastic Beanstalk. Une fois l'application migrée, Elastic Beanstalk crée le binaire du bundle source et le déploie sur une instance Amazon Elastic Compute Cloud (Amazon). EC2

En tant que stratégie de migration de réhébergement, l'approche de ce modèle est rapide et ne nécessite aucune modification de code, ce qui réduit le temps de test et de migration.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une application Web Go sur site.
- Un GitHub référentiel qui contient le code source de votre application Go. Si vous ne l'utilisez pas GitHub, il existe d'autres moyens de créer un bundle de sources d'applications pour Elastic Beanstalk.

Versions du produit

- La version de Go la plus récente prise en charge par Elastic Beanstalk. Pour plus d'informations, consultez la documentation d'Elastic Beanstalk.

Architecture

Pile technologique source

- Une application Web Go sur site

Pile technologique cible

- AWS Elastic Beanstalk
- Amazon CloudWatch

Architecture cible

Outils

- AWS Elastic Beanstalk déploie et gère rapidement des applications dans le cloud AWS sans que les utilisateurs aient à se renseigner sur l'infrastructure qui exécute ces applications. Elastic Beanstalk réduit la complexité inhérente à la gestion sans pour autant sacrifier le choix ou le niveau de contrôle.
- GitHubest un système de contrôle de version distribué open source.

Épopées

Créez le fichier .zip du bundle d'applications Web Go

Tâche	Description	Compétences requises
Créez le bundle source pour l'application Go.	Ouvrez le GitHub référentiel qui contient le code source de votre application Go et préparez le bundle source. Le bundle source contient un fichier `application.go` source dans le répertoire racine, qui héberge le package principal de votre application Go. Si vous ne l'utilisez pas GitHub, consultez la section Prérequis plus haut dans ce modèle pour découvrir d'autres méthodes de création du bundle de sources de votre application.	Administrateur système, développeur d'applications
Créez un fichier de configura tion.	Créez un `.ebextensions` dossier dans votre ensemble de sources, puis créez un `options.config` fichier	Administrateur système, développeur d'applications

Tâche	Description	Compétences requises
	dans ce dossier. Pour plus d'informations, consultez la documentation d'Elastic Beanstalk.	
Créez le fichier .zip du bundle source.	Exécutez la commande suivante. `git archive -o ../godemoapp.zip HEAD` Cela crée le fichier .zip du bundle source. Téléchargez et enregistrez le fichier .zip en tant que fichier local. ⚠ Important Le fichier .zip ne peut pas dépasser 512 Mo et ne peut pas inclure de dossier parent ou de répertoire de premier niveau.	Administrateur système, développeur d'applications

Migrer l'application Web Go vers Elastic Beanstalk

Tâche	Description	Compétences requises
Choisissez l'application Elastic Beanstalk.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Elastic Beanstalk.	Administrateur système, développeur d'applications

Tâche	Description	Compétences requises
	2. Dans la liste des régions, choisissez votre région AWS. 3. Dans le volet de navigation, choisissez Applications, puis choisissez une application Elastic Beanstalk existante ou créez-en une. Pour savoir comment créer une application Elastic Beanstalk, consultez la documentation Elastic Beanstalk.	
Lancez l'environnement du serveur Web Elastic Beanstalk.	1. Sur la page de présentation de l'application, choisissez Créer un nouvel environnement, puis sélectionnez Environnement de serveur Web. 2. Renseignez les champs Nom de l'environnement et Nom de domaine. 3. Choisissez la version de la plateforme, puis sélectionnez Go comme plateforme.	Administrateur système, développeur d'applications

Tâche	Description	Compétences requises
Téléchargez le fichier .zip du bundle source sur Elastic Beanstalk.	1. Dans Code de l'application, choisissez Télécharger votre code, puis sélectionnez Fichier local. 2. Choisissez le fichier .zip qui contient votre ensemble de sources. 3. Dans Libellé de version, attribuez un nom unique au fichier, puis choisissez Create environment.	Administrateur système, développeur d'applications
Testez l'application Web Go déployée.	Vous serez redirigé vers la page de présentation de l'application Elastic Beanstalk. En haut de l'aperçu, à côté de Environment ID, choisissez l'URL qui se termine par `elasticbeanstalk.com` pour accéder à votre application. Votre application doit utiliser ce nom dans son fichier de configuration en tant que variable d'environnement et l'afficher sur la page Web.	Administrateur système, développeur d'applications

Résolution des problèmes

Problème	Solution
Impossible d'accéder à l'application via un Application Load Balancer.	Vérifiez le groupe cible qui contient votre application Elastic Beanstalk. S'il ne fonctionne pas correctement, connectez-vous à votre instance Elastic Beanstalk et `nginx.conf`

Problème	Solution
	vérifiez la configuration du fichier pour vérifier qu'il est acheminé vers l'URL d'état de santé correcte. Vous devrez peut-être modifier l'URL de vérification de l'état du groupe cible.

Ressources connexes

- Versions de la plateforme Go prises en charge par Elastic Beanstalk
- Utilisation de fichiers de configuration avec Elastic Beanstalk
- Création d'un exemple d'application dans Elastic Beanstalk

Migrer un serveur SFTP sur site vers AWSAWS Transfer for SFTP

Créée par Akash Kumar (AWS)

Récapitulatif

Ce modèle décrit comment migrer une solution de transfert de fichiers sur site qui utilise le protocole de transfert de fichiers (SFTP) Secure Shell (SSH) vers le en AWS Cloud utilisant le service. AWS Transfer for SFTP Les utilisateurs se connectent généralement à un serveur SFTP par le biais de son nom de domaine ou via une adresse IP fixe. Ce schéma couvre les deux cas.

AWS Transfer for SFTP est membre du AWS Transfer Family. Il s'agit d'un service de transfert sécurisé que vous pouvez utiliser pour transférer des fichiers vers et depuis des services de AWS stockage via SFTP. Vous pouvez l'utiliser AWS Transfer for SFTP avec Amazon Simple Storage Service (Amazon S3) ou Amazon Elastic File System (Amazon EFS). Ce modèle utilise Amazon S3 pour le stockage.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Un nom de domaine SFTP existant ou une adresse IP SFTP fixe.

Limites

- Le plus gros objet que vous pouvez transférer en une seule demande est actuellement de 5 GiB. Pour les fichiers dont la taille est supérieure à 100 MiB, pensez à utiliser le téléchargement partitionné sur Amazon S3.

Architecture

Pile technologique source

- Fichiers plats ou fichiers de vidage de base de données locaux.

Pile technologique cible

- AWS Transfer for SFTP

- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS Identity and Access Management Rôles et politiques (IAM)
- Adresses IP Elastic
- Groupes de sécurité
- Amazon CloudWatch Logs (facultatif)

Architecture cible

Automatisation et mise à l'échelle

Pour automatiser l'architecture cible pour ce modèle, utilisez les AWS CloudFormation modèles ci-joints :

- `amazon-vpc-subnets.yml`fournit un cloud privé virtuel (VPC) avec deux sous-réseaux publics et deux sous-réseaux privés.
- `amazon-sftp-server.yml`approvisionne le serveur SFTP.
- `amazon-sftp-customer.yml`ajoute des utilisateurs.

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données. Ce modèle utilise Amazon S3 comme système de stockage pour les transferts de fichiers.
- AWS Transfer for SFTPvous permet de transférer des fichiers vers et depuis les services de AWS stockage via le protocole SFTP.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que

vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Épopées

Création d'un VPC

Tâche	Description	Compétences requises
Créez un VPC avec des sous-réseaux.	Ouvrez la console VPC Amazon. Créez un cloud privé virtuel (VPC) avec deux sous-réseaux publics. (Le deuxième sous-réseau assure une haute disponibilité.) —ou— Vous pouvez déployer le CloudFormation modèle ci-joint dans la CloudFormation console pour automatiser les tâches de cette épopée. `amazon-vpc-subnets.yml`	Développeur, administrateur système
Ajoutez une passerelle Internet.	Provisionnez une passerelle Internet et connectez-la au VPC.	Développeur, administrateur système
Migrez une adresse IP existante.	Associez une adresse IP existante à l'adresse IP élastique. Vous pouvez créer une adresse IP élastique à partir de votre pool d'adresses et l'utiliser.	Développeur, administrateur système

Provisionner un serveur SFTP

Tâche	Description	Compétences requises
Créez un serveur SFTP.	Ouvrez la AWS Transfer Family console. Suivez les instructions de la section Créer un point de terminaison connecté à Internet pour votre serveur dans la AWS Transfer Family documentation afin de créer un serveur SFTP avec un point de terminaison connecté à Internet. Pour le type de point de terminaison, choisissez VPC hébergé. Pour Access, choisissez Internet Facing. Pour le VPC, choisissez le VPC que vous avez créé dans l'épopée précédente. —ou— Vous pouvez déployer le CloudFormation modèle ci-joint dans la CloudFormation console pour automatiser les tâches de cette épopée. `amazon-sftp-server.yml`	Développeur, administrateur système
Migrez le nom de domaine.	Associez le nom de domaine existant au nom d'hôte personnalisé. Si vous utilisez un nouveau nom de domaine, utilisez l'alias DNS Amazon Route 53. Pour un nom de	Développeur, administrateur système

Tâche	Description	Compétences requises
	domaine existant, sélectionnez Autre DNS. Pour plus d'informations, consultez la section Utilisation de noms d'hôtes personnalisés dans la AWS Transfer Family documentation.	
Ajoutez un rôle de CloudWatch journalisation.	(Facultatif) Si vous souhaitez activer la CloudWatch journalisation, créez un `Transfer` rôle avec les opérations de l'API CloudWatch Logs `logs:CreateLogGroup logs:CreateLogStream` , `logs:DescribeLogStreams` , et`logs:PutLogEvents` . Pour plus d'informations, consultez la section Enregistrer l'activité avec CloudWatch dans la AWS Transfer Family documentation.	Développeur, administrateur système
Enregistrez et soumettez.	Choisissez Enregistrer. Pour Actions, choisissez Démarrer et attendez que le serveur SFTP soit créé avec le statut En ligne.	Développeur, administrateur système

Mappez les adresses IP Elastic au serveur SFTP

Tâche	Description	Compétences requises
Arrêtez le serveur afin de pouvoir modifier les paramètres.	Sur la AWS Transfer Family console, choisissez Servers, puis sélectionnez le serveur SFTP que vous avez créé. Pour Actions, choisissez Arrêter. Lorsque le serveur est hors ligne, choisissez Modifier pour modifier ses paramètres.	Développeur, administrateur système
Choisissez les zones de disponibilité et les sous-réseaux.	Dans la section Zones de disponibilité, choisissez les zones de disponibilité et les sous-réseaux pour votre VPC.	Développeur, administrateur système
Ajoutez des adresses IP élastiques.	Pour IPv4 Adresses, choisissez une adresse IP élastique pour chaque sous-réseau, puis sélectionnez Enregistrer.	Développeur, administrateur système

Ajout d'utilisateurs

Tâche	Description	Compétences requises
Créez un rôle IAM pour que les utilisateurs puissent accéder au compartiment S3.	Créez un rôle IAM pour `Transfer` et ajoutez-y `s3:ListBucket` `s3:GetBucketLocation` , et `s3:PutObject` avec le nom du compartiment S3 en tant que ressource. Pour plus d'informations, consultez la section Création d'un rôle	Développeur, administrateur système

Tâche	Description	Compétences requises
	et d'une politique IAM dans la AWS Transfer Family documentation. —ou— Vous pouvez déployer le CloudFormation modèle ci-joint dans la CloudFormation console pour automatiser les tâches de cette épopée. `amazon-sftp-customer.yml`	
Créez un compartiment S3.	Créez un compartiment S3 pour l'application.	Développeur, administrateur système
Créez des dossiers facultatifs.	(Facultatif) Si vous souhaitez stocker les fichiers des utilisateurs séparément, dans des dossiers Amazon S3 spécifiques, ajoutez des dossiers selon les besoins.	Développeur, administrateur système
Créez une clé publique SSH.	Pour créer une paire de clés SSH, consultez la section Générer des clés SSH dans la AWS Transfer Family documentation.	Développeur, administrateur système

Tâche	Description	Compétences requises
Ajouter des utilisateurs.	Sur la AWS Transfer Family console, choisissez Servers, sélectionnez le serveur SFTP que vous avez créé, puis choisissez Ajouter un utilisateur. Pour le répertoir e personnel, choisissez le compartiment S3 que vous avez créé. Pour la clé publique SSH, spécifiez la partie clé publique de la paire de clés SSH. Ajoutez des utilisateurs pour le serveur SFTP, puis choisissez Ajouter.	Développeur, administrateur système

Testez le serveur SFTP

Tâche	Description	Compétences requises
Mettez à jour le groupe de sécurité.	Dans la section Groupes de sécurité de votre serveur SFTP, ajoutez l'adresse IP de votre machine de test pour obtenir un accès SFTP.	Developer
Utilisez un utilitaire client SFTP pour tester le serveur.	Testez les transferts de fichiers à l'aide de n'importe quel utilitaire client SFTP. Pour obtenir la liste des clients et des instructions, consultez la section Transfert de fichiers à l'aide d'un client dans la AWS Transfer Family documentation.	Developer

Ressources connexes

- AWS Transfer Family Guide de l'utilisateur
- Guide de l'utilisateur d'Amazon S3
- Adresses IP élastiques dans la EC2 documentation Amazon

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer une machine virtuelle sur site vers Amazon à l'aide EC2 d'AWS Application Migration Service

Créée par Thanh Nguyen (AWS)

Récapitulatif

En matière de migration d'applications, les entreprises peuvent adopter différentes approches pour réhéberger (déplacer) les serveurs de l'application de l'environnement sur site vers le cloud Amazon Web Services (AWS). L'une des solutions consiste à fournir de nouvelles instances Amazon Elastic Compute Cloud (Amazon EC2), puis à installer et configurer l'application à partir de zéro. Une autre approche consiste à utiliser des services de migration natifs tiers ou AWS pour migrer plusieurs serveurs en même temps.

Ce modèle décrit les étapes de migration d'une machine virtuelle (VM) prise en charge vers une EC2 instance Amazon sur le cloud AWS à l'aide d'AWS Application Migration Service. Vous pouvez utiliser l'approche de ce modèle pour migrer une ou plusieurs machines virtuelles manuellement, une par une, ou automatiquement en créant des scripts d'automatisation appropriés en fonction des étapes décrites.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif dans l'une des régions AWS prenant en charge le service de migration d'applications
- Connectivité réseau entre le serveur source et le EC2 serveur cible via un réseau privé à l'aide d'AWS Direct Connect ou d'un réseau privé virtuel (VPN), ou via Internet

Limites

- Pour obtenir la dernière liste des régions prises en charge, consultez les régions AWS prises en charge.
- Pour obtenir la liste des systèmes d'exploitation pris en charge, consultez les sections Systèmes d'exploitation pris en charge et Général d'Amazon EC2 FAQs.

Architecture

Pile technologique source

- Un serveur physique, virtuel ou hébergé dans le cloud exécutant un système d'exploitation pris en charge par Amazon EC2

Pile technologique cible

- Une EC2 instance Amazon exécutant le même système d'exploitation que la machine virtuelle source
- Amazon Elastic Block Store (Amazon EBS)

Architecture source et cible

Le schéma suivant montre l'architecture de haut niveau et les principaux composants de la solution. Dans le centre de données sur site, il existe des machines virtuelles dotées de disques locaux. Sur AWS, il existe une zone intermédiaire avec des serveurs de réplication et une zone de ressources migrées avec des EC2 instances de test et de transfert. Les deux sous-réseaux contiennent des volumes EBS.

1. Initialisez le service de migration d'applications AWS.
2. Configurez la configuration et les rapports du serveur de la zone de transit, y compris les ressources de la zone de transit.
3. Installez des agents sur les serveurs sources et utilisez la réplication continue des données au niveau des blocs (compressées et chiffrées).
4. Automatisez l'orchestration et la conversion du système pour raccourcir la fenêtre de transition.

Architecture réseau

Le schéma suivant montre l'architecture de haut niveau et les principaux composants de la solution du point de vue de la mise en réseau, notamment les protocoles et les ports requis pour la communication entre les composants principaux du centre de données sur site et sur AWS.

Outils

- Le service de migration d'applications AWS vous aide à réhéberger (transférer et transférer) des applications vers le cloud AWS sans modification et avec un temps d'arrêt minimal.

Bonnes pratiques

- Ne mettez pas le serveur source hors ligne et n'effectuez pas de redémarrage tant que le transfert vers l' EC2 instance cible n'est pas terminé.
- Offrez aux utilisateurs de nombreuses opportunités d'effectuer des tests d'acceptation utilisateur (UAT) sur le serveur cible afin d'identifier et de résoudre les problèmes éventuels. Idéalement, ces tests devraient commencer au moins deux semaines avant le passage.
- Surveillez fréquemment l'état de réplication du serveur sur la console du service de migration des applications afin d'identifier les problèmes à un stade précoce.
- Utilisez des informations d'identification AWS Identity and Access Management (IAM) temporaires pour l'installation de l'agent plutôt que des informations d'identification utilisateur IAM permanentes.

Épopées

Générer des informations d'identification AWS

Tâche	Description	Compétences requises
Créez le rôle IAM de l'agent de réplication AWS.	Connectez-vous avec des autorisations administratives sur le compte AWS. Sur la console AWS Identity and Access Management (IAM), créez un rôle IAM : 1. Sur la console IAM, sélectionnez Rôles. 2. Choisissez Créer un rôle. 3. Sur la page Sélectionner une entité de confiance , dans la section Type d'entité fiable, sélectionnez un compte AWS. 4. Dans la section Un compte AWS, sélectionnez Ce compte (< account-id>).	Administrateur AWS, ingénieur en migration

Tâche	Description	Compétences requises
	5. Choisissez Suivant. 6. Sur la page Ajouter des autorisations, recherchez la `AWSApplicationMigrationAgentInstallationPolicy` politique, cochez la case à côté du nom de la politique. 7. Choisissez Suivant. 8. Sur la page Détails du rôle, entrez MGN_Agent_Installation_Role comme nom du rôle. 9. Vérifiez que les champs sont corrects, puis choisissez Create role.	

Tâche	Description	Compétences requises
Générez des informations d'identification de sécurité temporaires.	Sur une machine sur laquelle l'interface de ligne de commande (AWS CLI) est installée, connectez-vous avec des autorisations administratives. Ou bien (dans une région AWS prise en charge), sur la console de gestion AWS, connectez-vous avec des autorisations administratives sur le compte AWS et ouvrez AWS CloudShell. Générez des informations d'identification temporaires à l'aide de la commande suivante, en les `<account-id>` remplaçant par l'ID de compte AWS. `aws sts assume-role --role-arn arn:aws:iam::<account-id>:role/MGN_Agent_Installation_Role --role-session-name mgn_installation_session_role` À partir de la sortie de la commande, copiez les valeurs pour `AccessKeyId` **`SecretAccessKey`** , et **`SessionToken`** . Conservez	Administrateur AWS, ingénieur en migration

Tâche	Description	Compétences requises
	-les dans un endroit sûr pour une utilisation ultérieure. ⚠ Important Ces informations d'identification temporaires expireront au bout d'une heure. Si vous avez besoin d'informations d'identification au bout d'une heure, répétez les étapes précédentes.	

Initialisez le service de migration des applications et créez le modèle de paramètres de réplication

Tâche	Description	Compétences requises
Initialisez le service.	Sur la console, connectez-vous au compte AWS avec des autorisations administratives. Choisissez Application Migration Service, puis Get started.	Administrateur AWS, ingénieur en migration
Créez et configurez le modèle de paramètres de réplication.	1. Fournissez les détails de configuration suivants : a. Sélectionnez le sous-réseau de la zone de transit.	Administrateur AWS, ingénieur en migration

Tâche	Description	Compétences requises
	b. Sélectionnez le type d'instance du serveur de réplication (`t3.small`par défaut). c. Sélectionnez le type de volume EBS (gp3 par défaut). d. Sélectionnez l'option de chiffrement EBS. e. Assurez-vous que la case à cocher Toujours utiliser le groupe de sécurité du service de migration des applicati ons est cochée. f. Cochez la case Utiliser une adresse IP privée pour la réplication des données (VPN DirectCon nect, peering VPC) si vous utilisez une connectivité réseau privée entre l'environ nement sur site et AWS. g. Cochez la case Throttle network bandwidth (par serveur, en Mbits/ s) si vous souhaitez limiter la bande passante réseau pour le service de migration d'applications. 2. Sélectionnez Create template (Créer un modèle).	

Tâche	Description	Compétences requises
	Le service de migration des applications créera automatiquement tous les rôles IAM nécessaires pour faciliter la réplication des données et le lancement des serveurs migrés.	

Installation des agents de réplication AWS sur les machines sources

Tâche	Description	Compétences requises
Ayez à portée de main les informations d'identification AWS requises.	Lorsque vous exécutez le fichier d'installation sur un serveur source, vous devez saisir les informations d'identification temporaires que vous avez générées précédemment `AccessKeyId` , notamment `SecretAccessKey` , et `SessionToken` .	Ingénieur de migration, administrateur AWS
Pour les serveurs Linux, installez l'agent.	Copiez la commande du programme d'installation, connectez-vous à vos serveurs sources et exécutez le programme d'installation. Pour obtenir des instructions détaillées, consultez la documentation AWS.	Administrateur AWS, ingénieur en migration
Pour les serveurs Windows, installez l'agent.	Téléchargez le fichier d'installation sur chaque serveur, puis exécutez la commande d'installation. Pour obtenir	Administrateur AWS, ingénieur en migration

Tâche	Description	Compétences requises
	des instructions détaillées, consultez la documentation AWS.	
Attendez que la réplicati on initiale des données soit terminée.	Une fois l'agent installé, le serveur source apparaît sur la console du service de migration d'applications, dans la section Serveurs source. Patientez pendant que le serveur effectue la réplication initiale des données.	Administrateur AWS, ingénieur en migration

Configuration des paramètres de lancement

Tâche	Description	Compétences requises
Spécifiez les détails du serveur.	Sur la console Application Migration Service, choisisse z la section Serveurs source, puis choisissez un nom de serveur dans la liste pour accéder aux détails du serveur.	Administrateur AWS, ingénieur en migration
Configurez les paramètres de lancement.	Choisissez l'onglet Paramètre s de lancement. Vous pouvez configurer divers paramètre s, notamment les paramètres généraux de lancement et les paramètres EC2 du modèle de lancement. Pour obtenir des instructions détaillées, consultez la documentation AWS.	Administrateur AWS, ingénieur en migration

Réaliser un test

Tâche	Description	Compétences requises
Testez les serveurs sources.	1. Sur la console du service de migration des applications, dans la section Serveurs source, assurez-vous que le cycle de vie de migration des serveurs source est prêt pour les tests et que l'état de réplication des données est sain. 2. Cochez la case située à gauche de chaque serveur source. 3. Choisissez Test and Cutover, puis choisissez Launch Test Instance. 4. Lorsque vous y êtes invité, choisissez Launch. Les serveurs seront lancés.	Administrateur AWS, ingénieur en migration
Vérifiez que le test s'est bien déroulé.	Une fois le serveur de test complètement lancé, l'état des alertes sur la page indiquera Lancé pour chaque serveur.	Administrateur AWS, ingénieur en migration
Testez le serveur.	Effectuez des tests sur le serveur de test pour vous assurer qu'il fonctionne comme prévu.	Administrateur AWS, ingénieur en migration

Planifier et effectuer une transition

Tâche	Description	Compétences requises
Planifiez une fenêtre de transition.	Planifiez un calendrier de transition approprié avec les équipes concernées.	Administrateur AWS, ingénieur en migration
Effectuez le découpage.	1. Sur la console de migration d'applications, sur la page Serveurs source, cochez la case située à gauche de chaque serveur source. 2. Choisissez Test et Cutover, puis sélectionnez Marquer comme « Prêt pour le découpage ». 3. Vérifiez que le cycle de vie de migration de chaque serveur source est prêt pour le transfert. 4. Choisissez Test and Cutover, puis sélectionnez Launch Cutover instances. 5. Lorsque vous y êtes invité, choisissez Launch. Les serveurs seront lancés. Le cycle de vie de migration du serveur source deviendra Cutover en cours.	Administrateur AWS, ingénieur en migration
Vérifiez que le transfert s'est effectué correctement.	Une fois les serveurs de transition complètement lancés, l'état des alertes sur la page Serveurs sources	Administrateur AWS, ingénieur en migration

Tâche	Description	Compétences requises
	indiquera Lancé pour chaque serveur.	
Testez le serveur.	Effectuez des tests sur le serveur de transition pour vous assurer qu'il fonctionne comme prévu.	Administrateur AWS, ingénieur en migration
Finalisez le découpage.	Choisissez Test and Cutover, puis sélectionnez Finaliser le transfert pour finaliser le processus de migration.	Administrateur AWS, ingénieur en migration

Ressources connexes

- AWS Application Migration Service
- Guide de l'utilisateur du service de migration d'applications AWS

Migrez de petits ensembles de données sur site vers Amazon S3 à l'aide d'AWS SFTP

Créée par Charles Gibson (AWS) et Sergiy Shevchenko (AWS)

Récapitulatif

Ce modèle décrit comment migrer de petits ensembles de données (5 To ou moins) depuis des centres de données sur site vers Amazon Simple Storage Service (Amazon S3) à l'aide d'AWS Transfer for SFTP (AWS SFTP). Les données peuvent être des dumps de base de données ou des fichiers plats.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un lien AWS Direct Connect établi entre votre centre de données et AWS

Limitations liées à

- La taille des fichiers de données doit être inférieure à 5 To. Pour les fichiers de plus de 5 To, vous pouvez effectuer un chargement partitionné vers Amazon S3 ou choisir une autre méthode de transfert de données.

Architecture

Pile technologique source

- Fichiers plats ou vidages de base de données sur site

Pile technologique cible

- Amazon S3

Architecture source et cible

Outils

- AWS SFTP — Permet le transfert de fichiers directement depuis et vers Amazon S3 à l'aide du protocole SFTP (Secure File Transfer Protocol).
- AWS Direct Connect : établit une connexion réseau dédiée entre vos centres de données sur site et AWS.
- Points de terminaison VPC : vous permettent de connecter de manière privée un VPC aux services AWS pris en charge et aux services de point de terminaison VPC optimisés par PrivateLink AWS sans passerelle Internet, dispositif de traduction d'adresses réseau (NAT), connexion VPN ou connexion AWS Direct Connect. Les instances d'un VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les ressources du service.

Épopées

Préparer la migration

Tâche	Description	Compétences requises
Documentez les exigences SFTP actuelles.		Propriétaire de l'application, SA
Identifiez les exigences en matière d'authentification.	Les exigences peuvent inclure l'authentification par clé, le nom d'utilisateur ou le mot de passe, ou le fournisseur d'identité (IdP).	Propriétaire de l'application, SA
Identifiez les exigences en matière d'intégration des applications.		Propriétaire de l'application
Identifiez les utilisateurs qui ont besoin du service.		Propriétaire de l'application
Déterminez le nom DNS du point de terminaison du serveur SFTP.		Réseaux

Tâche	Description	Compétences requises
Déterminez la stratégie de sauvegarde.		SA, DBA (si les données sont transférées)
Identifiez la stratégie de migration ou de transfert des applications.		Propriétaire de l'application, SA, DBA

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un ou plusieurs clouds privés virtuels (VPCs) et sous-réseaux dans votre compte AWS.		Propriétaire de l'application, AMS
Créez les groupes de sécurité et la liste de contrôle d'accès réseau (ACL).		Sécurité, mise en réseau, AMS
Créez le compartiment S3.		Propriétaire de l'application, AMS
Créez le rôle de gestion des identités et des accès (IAM).	Créez une politique IAM qui inclut les autorisations permettant à AWS SFTP d'accéder à votre compartiment S3. Cette politique IAM détermine le niveau d'accès que vous offrez aux utilisateurs SFTP. Créez une autre politique IAM pour établir une relation de confiance avec AWS SFTP.	Sécurité, AMS

Tâche	Description	Compétences requises
Associez un domaine enregistré (facultatif).	Si vous avez enregistré votre propre domaine, vous pouvez l'associer au serveur SFTP. Vous pouvez acheminer le trafic SFTP vers le point de terminaison de votre serveur SFTP à partir d'un domaine ou d'un sous-domaine.	Réseautage, AMS
Créez un serveur SFTP.	Spécifiez le type de fournisseur d'identité utilisé par le service pour authentifier vos utilisateurs.	Propriétaire de l'application, AMS
Ouvrez un client SFTP.	Ouvrez un client SFTP et configurez la connexion pour utiliser l'hôte du point de terminaison SFTP. AWS SFTP prend en charge n'importe quel client SFTP standard. Les clients SFTP couramment utilisés incluent OpenSSH, WinSCP, Cyberduck et. FileZilla Vous pouvez obtenir le nom d'hôte du serveur SFTP depuis la console AWS SFTP.	Propriétaire de l'application, AMS

Planifier et tester

Tâche	Description	Compétences requises
Planifiez la migration des applications.	Planifiez les modifications de configuration de l'application requises, définissez la date	Propriétaire de l'application, AMS

Tâche	Description	Compétences requises
	de migration et déterminez le calendrier des tests.	
Testez l'infrastructure.	Testez dans un environnement hors production.	Propriétaire de l'application, AMS

Ressources connexes

Références

- Guide de l'utilisateur d'AWS Transfer for SFTP
- Ressources AWS Direct Connect
- Points de terminaison d’un VPC

Tutoriels et vidéos

- AWS Transfer pour SFTP (vidéo)
- Guide de l'utilisateur d'AWS Transfer for SFTP
- Tableau blanc AWS SA - Direct Connect (vidéo)

Migrer d'Oracle GlassFish vers AWS Elastic Beanstalk

Créée par Sandeep Bondugula (AWS)

Récapitulatif

Ce modèle décrit comment migrer une application Java exécutée sur un GlassFish serveur Oracle sur site vers AWS Elastic Beanstalk dans le cloud AWS.

Sur AWS, l'application Java est déployée sur un GlassFish serveur Docker avec AWS Elastic Beanstalk, qui s'exécute dans un groupe Amazon Elastic Compute Cloud (Amazon) Auto Scaling EC2.

Fonctionnalités supplémentaires :

- Amazon Elastic Beanstalk agit comme un wrapper pour plusieurs ressources sous-jacentes. Il configure Elastic Load Balancing (qui gère le trafic entrant en provenance d'Amazon Route 53), répartit le trafic vers une ou plusieurs EC2 instances et sert également d'outil de déploiement.
- Pour migrer une base de données sur site vers Amazon Relational Database Service (Amazon RDS), mettez à jour les informations de connexion à la base de données. Dans la base de données principale, vous pouvez configurer les déploiements Amazon RDS Multi-AZ et choisir le type de moteur de base de données.
- Vous pouvez utiliser le déploiement multi-AZ pour une haute disponibilité, ainsi que le groupe Auto Scaling et la politique de dimensionnement pour améliorer la résilience.
- Vous pouvez définir une politique de dimensionnement basée sur les CloudWatch métriques Amazon.
- Dans AWS Elastic Beanstalk, vous pouvez configurer les paramètres sous-jacents d'Elastic Load Balancing et d'Amazon Auto Scaling. EC2

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une application Java sur site exécutée sur GlassFish
- Un fichier WAR (Java Web Application Resource)

Versions du produit

- Oracle Glassfish 4.1.2 et 5.0
- Java 7 GlassFish 4.0
- Java 8 GlassFish 4.1 ou version ultérieure

Architecture

Pile technologique source

- Applications développées dans GlassFish

Pile technologique cible

- Elastic Beanstalk

Architecture cible

Flux de travail de déploiement

Outils

- Amazon Elastic Beanstalk : service de déploiement et de mise à l'échelle d'applications et de services Web développés avec Java, .NET, PHP, Node.js, Python, Ruby, Go et Docker sur des serveurs tels qu'Apache, NGINX, Passenger et IIS.
- Amazon CloudWatch — Fournit des données et des informations exploitables pour surveiller les applications, répondre aux changements de performances à l'échelle du système, optimiser l'utilisation des ressources et fournir une vue unifiée de la santé opérationnelle.
- Docker : plate-forme qui regroupe les logiciels dans des unités standardisées pour créer, tester et déployer rapidement des applications.
- Java — Langage de programmation à usage général. Java est basé sur les classes, orienté objet et conçu pour réduire les dépendances d'implémentation.

Épopées

Configurez un VPC

Tâche	Description	Compétences requises
Créez une instance de cloud privé virtuel (VPC) avec les informations requises.		SysAdmin
Créez au moins deux sous-réseaux au sein du VPC.		SysAdmin
Créez une table de routage selon les exigences.		SysAdmin

Configuration d'Amazon S3

Tâche	Description	Compétences requises
Créez un compartiment Amazon Simple Storage Service (Amazon S3).		SysAdmin
Copiez le fichier WAR dans le compartiment S3 et télécharg ez le code de l'application.		SysAdmin

Créer un rôle IAM

Tâche	Description	Compétences requises
Créez un rôle AWS Identity and Access Management (IAM).	Vous pouvez utiliser le profil « aws-elasticbeanstalk-ec 2 rôles » par défaut ou laisser Elastic Beanstalk le créer automatiquement.	SysAdmin

Configurer Elastic Beanstalk

Tâche	Description	Compétences requises
Ouvrez le tableau de bord Elastic Beanstalk.		SysAdmin
Créez une nouvelle application et choisissez l'environnement du serveur Web.		SysAdmin
Choisissez GlassFish Docker comme plateforme préconfig urée.		SysAdmin
Téléchargez le code.	Fournissez l'URL du fichier du compartiment S3 ou le fichier ZIP à partir des fichiers système locaux.	SysAdmin
Choisissez le type d'environ nement.	Dans les paramètres de capacité de configuration, choisissez Single Instance ou Load Balancer.	SysAdmin
Configurez Load Balancer.	Si vous avez choisi Load Balancer à l'étape précédent e, configurez le déploiement multi-AZ.	SysAdmin
Dans les paramètres de sécurité de configuration, choisissez le rôle IAM créé précédemment.		SysAdmin
Dans les paramètres de sécurité de la configuration, si vous possédez déjà une paire de clés, utilisez-la ou créez-		SysAdmin

Tâche	Description	Compétences requises
en une nouvelle pour Amazon EC2 .		
Dans les paramètres de surveillance de la configura tion, configurez Amazon CloudWatch.		SysAdmin
Dans les paramètres de sécurité de configuration, choisissez le VPC créé précédemment.		SysAdmin
Choisissez Create Environme nt.		SysAdmin

Tester l'application

Tâche	Description	Compétences requises
Testez l'application à l'aide de l'URL fournie dans l'environ nement créé.		
Appliquez les modifications apportées au service DNS (Domain Name Service) dans Amazon Route 53.		

Ressources connexes

- GlassFish Documentation Oracle
- GlassFish Implémentation de référence Java EE Open Source
- Documentation d'AWS Elastic Beanstalk
- Utilisation d'Elastic Beanstalk avec Amazon CloudWatch

- Tarification d'AWS Elastic Beanstalk
- EC2 Groupe Auto Scaling
- Diminution de la taille de votre groupe Auto Scaling
- Déploiements multi-AZ d'Amazon RDS

Migrer une base de données Oracle sur site vers Oracle sur Amazon EC2

Créée par Baji Shaik (AWS) et Pankaj Choudhary (AWS)

Récapitulatif

Ce modèle explique les étapes de migration d'une base de données Oracle sur site vers Oracle sur une instance Amazon Elastic Compute Cloud EC2 (Amazon). Il décrit deux options de migration : utiliser AWS Data Migration Service (AWS DMS) ou utiliser des outils Oracle natifs tels que RMAN, Data Pump import/export, tablespaces transportables et Oracle. GoldenGate

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle source dans un centre de données sur site

Limites

- Le système d'exploitation (OS) cible doit être pris en charge par Amazon EC2. Pour obtenir la liste complète des systèmes pris en charge, consultez Amazon EC2 FAQs.

Versions du produit

- Versions Oracle 10.2 et ultérieures (pour les versions 10.x), 11g et jusqu'à 12.2, et 18c pour les éditions Enterprise, Standard, Standard One et Standard Two. Pour obtenir la dernière liste des versions prises en charge par AWS DMS, consultez la section « Bases de données sur site et d' EC2 instances Amazon » dans la section Sources pour la migration des données de la documentation AWS DMS.

Architecture

Pile technologique source

- Une base de données Oracle sur site

Pile technologique cible

- Une instance de base de données Oracle sur Amazon EC2

Architecture cible

Architecture de migration des données

À l'aide d'AWS DMS :

À l'aide des outils Oracle natifs :

Outils

- AWS DMS - AWS Database Migration Services (AWS DMS) prend en charge plusieurs types de bases de données source et cible. Pour plus d'informations sur les versions et éditions de base de données prises en charge, consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.
- Outils Oracle natifs : RMAN, import/export de Data Pump, tablespaces transportables, Oracle GoldenGate

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions des bases de données source et cible.		DBA
Identifiez la version du système d'exploitation cible.		DBA, SysAdmin
Identifiez les exigences matérielles pour l'instance de serveur cible sur la base de la		DBA, SysAdmin

Tâche	Description	Compétences requises
liste de compatibilité Oracle et des exigences de capacité.		
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Identifiez les exigences du réseau (latence et bande passante).		DBA, SysAdmin
Choisissez le type d'instanc e approprié en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau/hô te pour les bases de données source et cible.		DBA, SysAdmin
Identifiez la liste des utilisate urs du système d'exploitation requis pour l'installation du logiciel Oracle.		DBA, SysAdmin
Téléchargez AWS Schema Conversion Tool (AWS SCT) et ses pilotes.		DBA
Créez un projet AWS SCT pour la charge de travail et connectez-vous à la base de données source.		DBA

Tâche	Description	Compétences requises
Générez des fichiers SQL pour la création d'objets (tables, index, séquences, etc.).		DBA
Déterminez une stratégie de sauvegarde.		DBA, SysAdmin
Déterminez les exigences de disponibilité.		DBA
Identifiez la stratégie de migration/commutation des applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux dans votre compte AWS.		SysAdmin
Créez des groupes de sécurité et des listes de contrôle d'accès au réseau (ACLs).		SysAdmin
Configurez et démarrez l' EC2 instance.		SysAdmin

Installation du logiciel Oracle

Tâche	Description	Compétences requises
Créez les utilisateurs et les groupes du système d'exploit ation requis pour le logiciel Oracle.		DBA, SysAdmin
Téléchargez la version requise du logiciel Oracle.		
Installez le logiciel Oracle sur l' EC2 instance.		DBA, SysAdmin
Créez des objets tels que des tables, des clés primaires, des vues et des séquences à l'aide des scripts générés par AWS SCT.		DBA

Migrer les données - option 1

Tâche	Description	Compétences requises
Utilisez des outils Oracle natifs ou des outils tiers pour migrer les objets et les données de base de données.	Les outils Oracle incluent l'importation/exportation de Data Pump, RMAN, les tablespaces transportables et. GoldenGate	DBA

Migrer les données - option 2

Tâche	Description	Compétences requises
Déterminez la méthode de migration.		DBA
Créez une instance de réplication dans la console AWS DMS.		DBA
Créez des points de terminaison source et cible.		DBA
Créez une tâche de réplication.		DBA
Activez la capture des données de modification (CDC) pour capturer les modifications en vue d'une réplication continue.		DBA
Exécutez la tâche de réplication et surveillez les journaux.		DBA
Créez des objets secondaires tels que des index et des clés étrangères lorsque le chargement complet est terminé.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.		DBA, propriétaire de SysAdmin l'application

Découper

Tâche	Description	Compétences requises
Suivez la stratégie de transfert et de commutation des applications.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources temporaires d'AWS Secrets Manager.		DBA, SysAdmin
Passez en revue et validez les documents du projet.		DBA, propriétaire de SysAdmin l'application
Collectez des indicateurs concernant le délai de migration, le pourcentage de manuel par rapport à l'outil, les économies de coûts, etc.		DBA, propriétaire de SysAdmin l'application
Clôturez le projet et faites part de vos commentaires.		

Ressources connexes

Références

- Stratégies de migration des bases de données Oracle vers AWS
- Migration de bases de données Oracle vers le cloud AWS
- EC2 Site Web d'Amazon
- Site Web AWS DMS

- Articles de blog AWS DMS
- EC2 Tarifs Amazon
- Octroi de licences aux logiciels Oracle dans un environnement de cloud computing

Tutoriels et vidéos

- Commencer à utiliser Amazon EC2
- Commencer à utiliser AWS DMS
- Présentation d'Amazon EC2 - Serveur cloud élastique et hébergement avec AWS (vidéo)

Migrer une base de données Oracle sur site vers Amazon à l'aide EC2 d'Oracle Data Pump

Créée par Navakanth Talluri (AWS)

Récapitulatif

Lorsque vous migrez des bases de données, vous devez tenir compte de facteurs tels que les moteurs et les versions de base de données source et cible, les outils et services de migration, ainsi que les périodes d'indisponibilité acceptables. Si vous migrez une base de données Oracle sur site vers Amazon Elastic Compute Cloud EC2 (Amazon), vous pouvez utiliser des outils Oracle, tels qu'Oracle Data Pump et Oracle Recovery Manager (RMAN). Pour plus d'informations sur les stratégies, consultez la section Migration de bases de données Oracle vers le cloud AWS.

Oracle Data Pump vous aide à extraire la sauvegarde logique et cohérente de la base de données et à la restaurer sur l' EC2 instance cible. Ce modèle décrit comment migrer une base de données Oracle sur site vers une EC2 instance à l'aide d'Oracle Data Pump et du `NETWORK_LINK` paramètre, avec un temps d'arrêt minimal. Le `NETWORK_LINK` paramètre lance une importation via un lien de base de données. Le client Oracle Data Pump Import (impdp) de l' EC2 instance cible se connecte à la base de données source, en extrait les données et les écrit directement dans la base de données de l'instance cible. Aucun fichier de sauvegarde ou de vidage n'est utilisé dans cette solution.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une base de données Oracle sur site qui :
  - N'est pas une base de données Oracle Real Application Clusters (RAC)
  - N'est pas une base de données Oracle Automatic Storage Management (Oracle ASM)
  - Est en mode lecture-écriture.
- Vous avez créé un lien AWS Direct Connect entre votre centre de données sur site et AWS. Pour plus d'informations, voir Créer une connexion (documentation Direct Connect).

Versions du produit

- Oracle Database 10g version 1 (10.1) et versions ultérieures

Architecture

Pile technologique source

- Un serveur de base de données Oracle autonome (non RAC et non ASM) dans un centre de données sur site

Pile technologique cible

- Une base de données Oracle exécutée sur Amazon EC2

Architecture cible

Le pilier de fiabilité d'AWS Well-Architected Framework recommande de créer des sauvegardes de données pour garantir une disponibilité et une résilience élevées. Pour plus d'informations, consultez Architecture pour une haute disponibilité dans Meilleures pratiques pour exécuter une base de données Oracle sur AWS. Ce modèle configure les bases de données principales et de secours sur EC2 les instances à l'aide d'Oracle Active Data Guard. Pour une haute disponibilité, les EC2 instances doivent se trouver dans des zones de disponibilité différentes. Toutefois, les zones de disponibilité peuvent se trouver dans la même région AWS ou dans différentes régions AWS.

Active Data Guard fournit un accès en lecture seule à une base de données de secours physique et applique les modifications de rétablissement en continu à partir de la base de données principale. En fonction de votre objectif de point de restauration (RPO) et de votre objectif de temps de restauration (RTO), vous pouvez choisir entre les options de redo transport synchrone et asynchrone.

L'image suivante montre l'architecture cible si les EC2 instances principales et de secours se trouvent dans des régions AWS différentes.

Architecture de migration des données

Une fois que vous avez terminé de configurer l'architecture cible, vous utilisez Oracle Data Pump pour migrer les données et les schémas locaux vers l'instance principale EC2 . Pendant le passage, les applications ne peuvent pas accéder à la base de données locale ou à la base de données cible. Vous arrêtez ces applications jusqu'à ce qu'elles puissent être connectées à la nouvelle base de données cible sur l' EC2 instance principale.

L'image suivante montre l'architecture lors de la migration des données. Dans cet exemple d'architecture, les EC2 instances principales et de secours se trouvent dans différentes régions AWS.

Outils

Services AWS

- AWS Direct Connect relie votre réseau interne à un emplacement Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les services AWS publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.

Autres outils et services

- Oracle Active Data Guard vous aide à créer, maintenir, gérer et surveiller des bases de données de secours.
- Oracle Data Pump vous aide à déplacer des données et des métadonnées d'une base de données à une autre à grande vitesse.

Bonnes pratiques

- Bonnes pratiques pour l'exécution d'une base de données Oracle sur AWS
- Importation de données à l'aide de NETWORK_LINK

Épopées

Configuration des EC2 instances sur AWS

Tâche	Description	Compétences requises
Identifiez la configuration matérielle source pour l'hôte local et les paramètres du noyau.	Validez la configuration sur site, y compris la taille du stockage, les opérations d'entrée/sortie par seconde (IOPS) et le processeur. Cela	DBA, SysAdmin

Tâche	Description	Compétences requises
	est important pour les licences Oracle, qui sont basées sur les cœurs de processeur.	
Créez l'infrastructure sur AWS.	Créez les clouds privés virtuels (VPCs), les sous-réseaux privés, les groupes de sécurité, les listes de contrôle d'accès réseau (ACLs), les tables de routage et la passerelle Internet. Pour plus d'informations, consultez les ressources suivantes : • VPCs et sous-réseaux • Tutoriel : Création d'un VPC à utiliser avec une instance de base de données	DBA, administrateur système AWS

Tâche	Description	Compétences requises
Configurez les EC2 instances à l'aide d'Active Data Guard.	Configurez EC2 les instances AWS à l'aide d'une configuration Active Data Guard, comme décrit dans le AWS Well-Architected Framework. La version d'Oracle Database sur l' EC2 instance peut être différente de la version locale car ce modèle utilise des sauvegardes logiques. Remarques : • Mettez la base de données cible en mode lecture-écriture. • Dans la base de données cible, fournissez le détail du substrat réseau transparent (TNS) pour la base de données source. Pour plus d'informations, consultez : • Démarrage d'une base de données (documentation Oracle) • Création et configuration d'une base de données Oracle (documentation Oracle)	DBA, administrateur système AWS

Migrer la base de données vers Amazon EC2

Tâche	Description	Compétences requises
Créez un dblink vers la base de données locale à partir de l'instance. EC2	Créez un lien de base de données (dblink) entre la base de données Oracle de l' EC2 instance et la base de données Oracle locale. Pour plus d'informations, voir Utilisation de l'importation de liens réseau pour déplacer des données (documentation Oracle).	DBA
Vérifiez la connexion entre l' EC2 instance et l'hôte local.	Utilisez le dblink pour vérifier que la connexion entre l' EC2 instance et la base de données locale fonctionne. Pour obtenir des instructions, voir CREATE DATABASE LINK (documentation Oracle).	DBA
Arrêtez toutes les applicati ons connectées à la base de données locale.	Une fois le temps d'arrêt de la base de données approuvé, arrêtez toutes les applications et les tâches dépendantes qui se connectent à votre base de données locale. Vous pouvez le faire directement depuis l'application ou depuis la base de données en utilisant cron. Pour plus d'informations, voir Utiliser l'utilitaire Crontab pour planifier des tâches sur Oracle Linux.	DBA, développeur d'applica tions

Tâche	Description	Compétences requises
Planifiez la tâche de migration des données.	Sur l'hôte cible, utilisez la commande `impdb` pour planifier l'importation de Data Pump. Cela connecte la base de données cible à l'hôte local et démarre la migration des données. Pour plus d'informations, consultez Data Pump Import et NETWORK_LINK (documentation Oracle).	DBA
Validez la migration des données.	La validation des données est une étape cruciale. Pour la validation des données, vous pouvez utiliser des outils personnalisés ou des outils Oracle, tels qu'une combinaison de requêtes dblink et SQL.	DBA

Découper

Tâche	Description	Compétences requises
Mettez la base de données source en mode lecture seule.	Vérifiez que l'application est arrêtée et qu'aucune modification n'est apportée à la base de données source. Ouvrez la base de données source en mode lecture seule. Cela vous permet d'éviter toute transaction ouverte. Pour plus d'informations, consultez `ALTER DATABASE` la section	DBA, DevOps ingénieur, développeur d'applications

Tâche	Description	Compétences requises
	Instructions SQL (document ation Oracle).	
Validez le nombre d'objets et les données.	Pour valider les données et l'objet, utilisez des outils personnalisés ou des outils Oracle, tels qu'une combinais on de requêtes dblink et SQL.	DBA, développeur d'applica tions
Connectez les applications à la base de données sur l' EC2 instance principale.	Modifiez l'attribut de connexion de l'application pour qu'il pointe vers la nouvelle base de données que vous avez créée sur l' EC2 instance principale.	DBA, développeur d'applica tions
Validez les performances de l'application.	Lancez l'application. Validez les fonctionnalités et les performances de l'applica tion à l'aide du référentiel de charge de travail automatisé (documentation Oracle).	Développeur d'applications, DevOps ingénieur, DBA

Ressources connexes

Références AWS

- Migration de bases de données Oracle vers le cloud AWS
- Amazon EC2 pour Oracle
- Migration de bases de données Oracle volumineuses vers AWS pour les environnements multiplateformes
- VPCs et sous-réseaux
- Tutoriel : Création d'un VPC à utiliser avec une instance de base de données

Références Oracle

- Configurations d'Oracle Data Guard
- Importation de pompes de données

Migrez les systèmes RHEL BYOL vers des instances incluses dans une licence AWS à l'aide d'AWS MGN

Créée par Mike Kuznetsov (AWS)

Récapitulatif

Lorsque vous migrez vos charges de travail vers AWS à l'aide d'AWS Application Migration Service (AWS MGN), il se peut que vous deviez déplacer (réhéberger) vos instances Red Hat Enterprise Linux (RHEL) et modifier la licence du modèle Bring Your Own License (BYOL) par défaut au modèle AWS License Included (LI) pendant la migration. AWS MGN prend en charge une approche évolutive qui utilise Amazon Machine Image (AMI). IDs Ce modèle décrit comment effectuer le changement de licence sur les serveurs RHEL lors de la migration de réhébergement à grande échelle. Il explique également comment modifier la licence d'un système RHEL déjà exécuté sur Amazon Elastic Compute Cloud (Amazon EC2).

Conditions préalables et limitations

Prérequis

- Accès au compte AWS cible
- AWS MGN initialisé dans le compte et la région AWS cibles pour la migration (non requis si vous avez déjà migré de votre système sur site vers AWS)
- Un serveur RHEL source avec une licence RHEL valide

Architecture

Ce modèle couvre deux scénarios :

- Migration d'un système sur site directement vers une instance AWS LI à l'aide d'AWS MGN. Pour ce scénario, suivez les instructions du premier épisode (Migrer vers une instance LI - option 1) et du troisième épisode.
- Modification du modèle de licence de BYOL à LI pour un système RHEL précédemment migré qui fonctionne déjà sur Amazon. EC2 Pour ce scénario, suivez les instructions du deuxième épisode (Migrer vers une instance LI - option 2) et du troisième épisode.

> **Note**
>
> La troisième étape consiste à reconfigurer la nouvelle instance RHEL pour utiliser les serveurs Red Hat Update Infrastructure (RHUI) fournis par AWS. Ce processus est le même pour les deux scénarios.

Outils

Services AWS

- AWS Application Migration Service (AWS MGN) vous aide à réhéberger (transférer et transférer) des applications vers le cloud AWS sans modification et avec un temps d'arrêt minimal.

Épopées

Migrer vers une instance LI - option 1 (pour un système RHEL sur site)

Tâche	Description	Compétences requises
Trouvez l'ID AMI de l'instance RHEL AWS LI dans la région cible.	Visitez AWS Marketplace ou utilisez la EC2 console Amazon pour trouver l'ID d'AMI RHEL correspondant à la version du système source RHEL (par exemple, RHEL-7.7) et notez l'ID d'AMI. Sur la EC2 console Amazon, vous pouvez filtrer les AMIs en utilisant l'un des termes de recherche suivants : • Description = Fourni par Red Hat, Inc. • Nom de l'AMI = RHEL-7.7	Administrateur du cloud
Configurez les paramètres de lancement d'AWS MGN.	1. Sur la console AWS MGN, ajoutez le système RHEL	Administrateur du cloud

Tâche	Description	Compétences requises
	source : installez l'agent de réplication AWS et ajoutez le serveur source en suivant les instructions de la documentation AWS MGN. 2. Sur la page Serveurs source, choisissez le système RHEL source, puis cliquez sur l'onglet Paramètres de lancement. 3. Dans la section Paramètres généraux de lancement, choisissez Modifier. Pour désactiver la sélection automatique et spécifier manuellement le type d'instance cible, remplacez le dimensionnement correct du type d'instance par Aucun, puis choisissez Enregistrer les paramètres. Cela vous permet d'utiliser le type d'instance que vous configurez dans votre modèle de EC2 lancement Amazon. Pour plus d'informations, consultez la documentation AWS MGN. 4. Dans la section Modèle de EC2 lancement, choisissez Modifier. Dans la boîte de dialogue À propos	

Tâche	Description	Compétences requises
	de la modification des modèles de EC2 lancement , sélectionnez à nouveau Modifier. Cela ouvre la EC2 console Amazon afin que vous puissiez modifier le modèle de cette instance. 5. Consultez les principaux points à prendre en compte dans la documentation AWS MGN. **Note** Vous pouvez ignorer la mise en garde contre le choix de votre propre AMI. 6. Sur la EC2 console Amazon, dans le nouveau modèle de lancement , modifiez les éléments suivants : • Pour l'AMI, spécifiez l'ID d'AMI que vous avez identifié précédemment, ou recherchez RHEL-x et spécifiez la version dont vous avez besoin (par exemple, RHEL-7.7). • Pour Type d'instanc e, définissez le type d'instance cible souhaité.	

Tâche	Description	Compétences requises
	• Laissez les sections suivantes inchangées : paire de clés (connexion), paramètres réseau (sauf si vous souhaitez spécifier un sous-réseau cible et des groupes de sécurité), stockage, balises de ressources (sauf si vous souhaitez ajouter ou modifier des balises). • (Facultatif) Dans la section Informations avancées, spécifiez le rôle du profil d'instance IAM, si nécessaire pour une gestion future par AWS Systems Manager. 7. Choisissez Créer une version du modèle, puis cliquez sur le lien dans le message de réussite pour afficher le modèle de lancement. 8. Choisissez Actions, puis Définissez la version par défaut. Pour la version du modèle, sélectionnez la dernière version (version 2 pour un nouveau système), puis choisissez Définir comme version par défaut.	

Tâche	Description	Compétences requises
	AWS MGN va désormais utiliser cette version du modèle de lancement pour lancer des instances de test ou de transition. Pour plus d'informations, consultez la documentation AWS MGN.	

Tâche	Description	Compétences requises
Validez les paramètres.	1. Sur la console AWS MGN, sur la page Serveurs source, choisissez votre serveur source, puis choisissez l'onglet Paramètres de lancement. 2. Dans la section Modèle de EC2 lancement, vérifiez que les paramètres du type d'instance, du sous-réseau et des groupes de sécurité sont correctement définis. **Note** Cette section n'affiche pas l'ID d'AMI que vous avez sélectionné. Pour voir l'identif iant, vous pouvez ouvrir la EC2 console Amazon, la vue Launch Templates et rechercher l'ID du modèle indiqué dans cette section.	Administrateur du cloud

Tâche	Description	Compétences requises
Lancez la nouvelle instance LI.	1. Lorsque la synchronisation initiale est terminée, la colonne Cycle de vie de migration du serveur sur la page Serveurs sources de la console AWS MGN devient Ready for testing. Pour lancer la nouvelle instance de test, choisissez votre serveur source, ouvrez le menu Test and Cutover, puis choisissez Launch test instances. Choisissez Afficher les détails de la tâche pour suivre l'état de la tâche de lancement. Pour plus d'informations, consultez la documentation AWS MGN. 2. Attendez que la tâche de lancement soit terminée, puis ouvrez la page des détails de l' EC2 instance lancée. Choisissez l'onglet Détails et vérifiez que la section Détails de l'instance contient les éléments suivants : • Détails de la plateforme : « Red Hat Enterprise Linux » • Nom de l'AMI : nom de l'AMI que vous avez	Administrateur du cloud

Tâche	Description	Compétences requises
	spécifié dans le modèle de EC2 lancement 3. Passez à la nouvelle instance LI en suivant les instructions de la documentation AWS MGN. 4. Reconfigurez la nouvelle instance pour utiliser les serveurs RHUI fournis par AWS en suivant les étapes décrites dans le dernier épisode.	

Migrer vers une instance LI - option 2 (pour une instance RHEL BYOL EC2)

Tâche	Description	Compétences requises
Migrez votre instance RHEL BYOL vers une EC2 instance AWS LI.	Vous pouvez faire passer les systèmes RHEL que vous avez précédemment migrés vers AWS en tant que BYOL vers des instances AWS LI en déplaçant leurs disques (volumes Amazon Elastic Block Store) et en les attachant à une nouvelle instance LI. Pour effectuer ce changement, procédez comme suit : 1. Lancez une nouvelle instance RHEL cible à partir d'une AMI RHEL LI.	Administrateur du cloud

Tâche	Description	Compétences requises
	Assurez-vous que l'AMI que vous avez sélectionnée : • Utilise la même version de RHEL que votre instance RHEL actuelle. • Dispose du même processus de démarrage (BIOS ou UEFI) que votre instance RHEL actuelle. Par exemple, si le serveur source est basé sur le BIOS, utilisez l'AMI RHEL d'AWS Marketplace qui est également basée sur le BIOS ; pour les systèmes basés sur UEFI, choisissez l'AMI basée sur UEFI. 2. Arrêtez les deux instances : la nouvelle instance LI et l'instance source d'origine. 3. Détachez tous les volumes EBS (y compris le disque racine) de la nouvelle instance LI et supprimez-les. 4. Détachez tous les volumes EBS (y compris le disque racine) de l'ancienne instance source et attachez-les à la nouvelle instance LI. Conservez le même mappage entre les volumes et les appareils. (Par	

Tâche	Description	Compétences requises
	exemple, le volume EBS précédemment attaché au `/dev/sda` lecteur doit être attaché `/dev/sda` à la nouvelle instance.) 5. Supprimez l'instance source (désormais sans disque). 6. Démarrez la nouvelle instance LI. Connectez -vous à l'instance et reconfigurez-la pour utiliser les serveurs RHUI fournis par AWS en suivant les étapes décrites dans l'épisode suivant.	

Reconfigurer le système d'exploitation RHEL pour utiliser le RHUI fourni par AWS : les deux options

Tâche	Description	Compétences requises
Désenregistrez le système d'exploitation de l'abonnement et de la licence Red Hat.	Une fois la migration et le transfert réussis, le système RHEL doit être supprimé de l'abonnement Red Hat afin de ne plus consommer la licence Red Hat et d'éviter une double facturation. Pour supprimer RHEL OS de l'abonnement Red Hat, suivez le processus décrit dans la documentation de gestion des abonnements Red Hat (RHSM). Utilisez la	Linux ou administrateur système

Tâche	Description	Compétences requises
	commande de l'interface de ligne de commande : `subscription-manager unregister` Vous pouvez également désactiver le plugin de gestion des abonnements pour arrêter de vérifier l'état de l'abonnement à chaque appel yum. Pour ce faire, modifiez le fichier de configuration `/etc/yum/pluginconf.d/subscription-manager.conf` et remplacez le paramètre `enabled=1` par `enabled=0`.	

Tâche	Description	Compétences requises
Remplacez l'ancienne configuration de mise à jour (RHUI, réseau Red Hat Satellite, référentiels yum) par le RHUI fourni par AWS.	Vous devez reconfigurer le système RHEL migré pour utiliser les serveurs RHUI fournis par AWS. Cela vous permet d'accéder aux serveurs RHUI au sein des régions AWS sans avoir besoin d'une infrastructure de mise à jour externe. Le changement implique le processus suivant : 1. Sauvegardez la configuration yum existante. 2. Supprimez l'ancienne configuration et les anciens packages RHUI (référentiels yum). 3. Ajoutez la nouvelle configuration RHUI et les nouveaux packages de certificats fournis par AWS. Vous devez les récupérer depuis une autre instance RHEL sur AWS, car ces packages de configuration ne sont disponibles que sur les serveurs RHUI fournis par AWS. Voici les étapes et les commandes détaillées : 1. Sauvegardez la configuration et les certificats yum	Linux ou administrateur système

Tâche	Description	Compétences requises

	existants en copiant tous les `/etc/pki/*` dossiers `/etc/yum*` et les dossiers vers un emplacement de sauvegarde. Par exemple :
	`mkdir yum-backup`
	`cp -ra /etc/yum* /etc/pki ./yum-backup`
	`tar czf yum-backup.tgz ./yum-backup`
	2. Supprimez l'ancienne configuration et les anciens packages RHUI :
	a. Trouvez tous les packages RHUI installés :
	`sudo rpm -qa | grep rhui`
	b. Supprimez les packages suivants :
	`sudo yum remove $(rpm -qa | grep rhui)`
	c. Supprimez le `/etc/yum/vars/releasever` fichier, s'il existe.
	3. Ajoutez le nouveau RHUI et les nouveaux packages de certificats fournis par AWS.	

Tâche	Description	Compétences requises
	Vous devez les récupérer depuis une autre instance RHEL sur AWS. Il existe plusieurs méthodes pour le faire. Par exemple, vous pouvez suivre les instructions fournies dans l'article de la base de connaissances Red Hat : a. Lancez une autre instance RHEL (RHEL-EC2) depuis AWS Marketplace. b. Téléchargez deux packages à partir de cette instance : le dernier package de configuration du client RHUI et les certificats de l'autorité de certification (CA). Par exemple, exécutez cette commande depuis votre bureau : `ssh RHEL-EC2 "sudo yumdownloader ca-certificates rh-amazon-rhui-client"` c. Copiez les packages de l'EC2 instance RHEL vers le nouveau système migré. Par exemple :	

Tâche	Description	Compétences requises
	``` scp RHEL-EC2:rh-amazon-rhui-client* RHEL-EC2:ca-certificates* . ssh <migrated-instance> "mkdir /tmp/amazon" scp rh-amazon-rhui-client* ca-certificates* <migrated-instance>:/tmp/amazon ``` d. Installez les nouveaux packages de configuration RHUI et CA sur l'instance migrée : ``` ssh <migrated-instance> "sudo rpm -Uhv /tmp/amazon/*" ```	
Validez la configuration.	Sur l'instance cible migrée, vérifiez que la nouvelle configuration est correcte : ``` sudo yum clean all sudo yum repolist ```	Linux ou administrateur système

Ressources connexes

- Guide de l'utilisateur du service de migration d'applications AWS (AWS MGN)
- Obtenir un package client AWS RHUI compatible IMDSv2 (article de la base de connaissances Red Hat)
- Modèles de EC2 lancement Amazon (EC2 documentation Amazon)

Migrer une base de données SAP ASE sur site vers Amazon EC2

Créée par Sergey Dmitriev (AWS) et Gergely Cserdi (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données SAP Adaptive Server Enterprise (ASE) d'un hôte sur site vers une instance Amazon Elastic Compute Cloud (Amazon EC2). Le modèle couvre l'utilisation d'AWS Database Migration Service (AWS DMS) ou d'outils natifs de SAP ASE tels que ASE Cockpit, Sybase Central pour ASE et DBA Cockpit pour la migration.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source SAP ASE dans un centre de données sur site

Limitations liées à

- La base de données source doit être inférieure à 64 To

Versions du produit

- SAP ASE versions 15.x et 16.x ou ultérieures

Architecture

Pile technologique source

- Base de données SAP ASE sur site

Pile technologique cible

- Base de données SAP ASE sur une EC2 instance

Architecture de migration de base de données

À l'aide d'AWS DMS :

À l'aide des outils SAP ASE natifs :

Outils

- AWS DMS - AWS Data Migration Service (AWS DMS) prend en charge plusieurs bases de données sources et cibles différentes. Pour plus d'informations, consultez les sections Sources pour la migration des données et Cibles pour la migration des données. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.
- SAP ASE - Les outils natifs incluent ASE Cockpit, Sybase Central pour ASE et DBA Cockpit.

Épopées

Analyser la migration

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.		DBA
Identifiez la version du système d'exploitation cible.		DBA, SysAdmin
Identifiez la configuration matérielle requise pour l'instance de serveur cible en fonction de la liste de compatibilité SAP ASE et des exigences en matière de capacité.		DBA, SysAdmin
Identifiez les exigences relatives au type et à la capacité de stockage.		DBA, SysAdmin

Tâche	Description	Compétences requises
Identifiez les exigences du réseau, y compris la latence et la bande passante.		DBA, SysAdmin
Choisissez le type d'instance, la capacité, les fonctionnalités de stockage et les fonctionn alités réseau appropriés.		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau et à l'hôte pour les bases de données source et cible.		DBA, SysAdmin
Identifiez la liste des utilisate urs du système d'exploitation requis pour l'installation du logiciel SAP ASE.		DBA, SysAdmin
Déterminez la stratégie de sauvegarde.		DBA
Déterminez les exigences de disponibilité.		DBA
Identifiez la stratégie de migration et de transition des applications.		DBA, propriétaire de SysAdmin l'application

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		SysAdmin

Tâche	Description	Compétences requises
Créez des groupes de sécurité et la liste de contrôle d'accès réseau (ACL).		SysAdmin
Configurez et démarrez l' EC2 instance.		SysAdmin

Installez le logiciel

Tâche	Description	Compétences requises
Créez les utilisateurs et les groupes du système d'exploit ation nécessaires au fonctionn ement du logiciel SAP ASE.		DBA, SysAdmin
Téléchargez la version requise du logiciel SAP ASE.		DBA, SysAdmin
Installez la base de données SAP ASE, le logiciel du serveur de sauvegarde et le logiciel du serveur de réplicati on sur l' EC2 instance, puis configurez le serveur.		DBA, SysAdmin

Migrer les données - option 1

Tâche	Description	Compétences requises
Migrez les objets et les données de la base de données à l'aide d'outils SAP ASE natifs ou d'outils tiers.	Consultez la documentation relative à SAP ASE ou à des outils tiers. Il s'agit notamment d'ASE Cockpit, de Sybase	DBA

Tâche	Description	Compétences requises
	Central pour ASE et de DBA Cockpit.	

Migrer les données - option 2

Tâche	Description	Compétences requises
Migrez les données à l'aide d'AWS DMS.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.		DBA, propriétaire de SysAdmin l'application

Découper

Tâche	Description	Compétences requises
Suivez la stratégie de transfert ou de transition des applicati ons.		DBA, propriétaire de SysAdmin l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, SysAdmin

Tâche	Description	Compétences requises
Validez et révisez les documents du projet.		DBA, propriétaire de SysAdmin l'application
Collectez des indicateurs concernant le délai de migration, le pourcentage d'économies réalisées manuellement par rapport aux coûts liés aux outils, etc.		DBA, propriétaire de SysAdmin l'application
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de SysAdmin l'application

Ressources connexes

Références

- Amazon EC2
- AWS DMS
- EC2 Tarification Amazon

Tutoriels et vidéos

- Commencer à utiliser Amazon EC2
- Commencer à utiliser AWS Database Migration Service
- Service de migration de données AWS (vidéo)
- Présentation d'Amazon EC2 - Serveur cloud élastique et hébergement avec AWS (vidéo)

Migrer une base de données Microsoft SQL Server sur site vers Amazon EC2

Créée par Senthil Ramasamy (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Microsoft SQL Server sur site vers Microsoft SQL Server sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Il couvre deux options de migration : utiliser AWS Database Migration Service (AWS DMS) ou utiliser les outils natifs de Microsoft SQL Server tels que la sauvegarde et la restauration, l'assistant de copie de base de données ou la copie et l'attachement de base de données.

Conditions préalables et limitations

Prérequis

- Un AWS compte actif
- Un système d'exploitation pris en charge par Amazon EC2 (pour une liste complète des versions de système d'exploitation prises en charge, consultez Amazon EC2 FAQs)
- Une base de données source Microsoft SQL Server dans un centre de données sur site

Versions du produit

- Pour les bases de données sur site et les bases de données d' EC2 instances Amazon, AWS DMS prend en charge :
  - Versions de SQL Server 2005, 2008, 2008R2, 2012, 2014, 2016, 2017 et 2019
  - Éditions Enterprise, Standard, Workgroup, Developer et Web
- Pour obtenir la dernière liste des versions prises en charge, voir Utilisation d'une base de données Microsoft SQL Server comme cible pour AWS DMS.

Architecture

Pile technologique source

- Base de données Microsoft SQL Server locale

Pile technologique cible

- Base de données Microsoft SQL Server sur une EC2 instance

Architecture cible

Architecture de migration des données

- En utilisant AWS DMS

- Utilisation des outils SQL Server natifs

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer vos données vers et depuis des bases de données commerciales et open source largement utilisées, notamment Oracle, SQL Server, MySQL et PostgreSQL. Vous pouvez l'utiliser AWS DMS pour migrer vos données vers AWS Cloud, entre des instances locales (via une AWS Cloud configuration) ou entre des combinaisons de configurations cloud et locales.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.
- Les outils natifs de Microsoft SQL Server incluent la sauvegarde et la restauration, l'assistant de copie de base de données et la copie et l'attachement de base de données.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.		DBA

Tâche	Description	Compétences requises
Identifiez la version du système d'exploitation cible.		DBA, administrateur système
Identifiez la configuration matérielle requise pour l'instance de serveur cible sur la base de la liste de compatibilité de Microsoft SQL Server et des exigences en matière de capacité.		DBA, administrateur système
Identifiez les exigences de stockage en termes de type et de capacité.		DBA, administrateur système
Identifiez les exigences du réseau, y compris la latence et la bande passante.		DBA, administrateur système
Choisissez le type d' EC2 instance en fonction de la capacité, des fonctionnalités de stockage et des fonctionnalités réseau.		DBA, administrateur système
Identifiez les exigences de sécurité d'accès au réseau et à l'hôte pour les bases de données source et cible.		DBA, administrateur système
Identifiez la liste des utilisateurs requis pour l'installation du logiciel Microsoft SQL Server.		DBA, administrateur système
Déterminez la stratégie de sauvegarde.		DBA

Tâche	Description	Compétences requises
Déterminez les exigences de disponibilité.		DBA
Identifiez la stratégie de migration et de transfert des applications.		DBA, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.		Administrateur de systèmes
Créez des groupes de sécurité et une liste de contrôle d'accès réseau (ACL).		Administrateur de systèmes
Configurez et démarrez une EC2 instance.		Administrateur de systèmes

Installez le logiciel

Tâche	Description	Compétences requises
Créez les utilisateurs et les groupes requis pour le logiciel Microsoft SQL Server.		DBA, administrateur système
Téléchargez le logiciel Microsoft SQL Server.		DBA, administrateur système
Installez le logiciel Microsoft SQL Server sur l' EC2		DBA, administrateur système

Tâche	Description	Compétences requises
instance et configurez le serveur.		

Migrer les données - option 1

Tâche	Description	Compétences requises
Utilisez les outils natifs de Microsoft SQL Server ou des outils tiers pour migrer les objets et les données de la base de données.	Les outils incluent la sauvegarde et la restauration, l'assistant de copie de base de données et la copie et l'attachement de base de données. Pour plus d'informations, consultez le guide Migration des bases de données Microsoft SQL Server vers le AWS Cloud.	DBA

Migrer les données - option 2

Tâche	Description	Compétences requises
Migrez les données à l'aide d'AWS DMS.	Pour plus d'informations sur l'utilisation AWS DMS, consultez les liens de la section Ressources connexes.	DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.	Utilisez AWS Schema Conversion Tool (AWS SCT)	DBA, propriétaire de l'application

Tâche	Description	Compétences requises
	pour analyser et modifier le code SQL intégré au code source de l'application.	

Découper

Tâche	Description	Compétences requises
Suivez la stratégie de changement d'application.		DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez toutes les AWS ressources temporaires.	Les ressources temporaires incluent l'instance de AWS DMS réplication et l' EC2 instance pour AWS SCT.	DBA, administrateur système
Passez en revue et validez les documents du projet.		DBA, propriétaire de l'application, administrateur système
Collectez des indicateurs concernant le délai de migration, le pourcentage d'économies réalisées manuellement par rapport aux coûts liés aux outils, etc.		DBA, propriétaire de l'application, administrateur système
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de l'application, administrateur système

Ressources connexes

Références

- Migration des bases de données Microsoft SQL Server vers AWS Cloud
- Amazon EC2
- Amazon EC2 FAQs
- EC2 Tarification Amazon
- AWS Database Migration Service
- Produits Microsoft sur AWS
- Licence Microsoft sur AWS
- Microsoft SQL Server sur AWS

Tutoriels et vidéos

- Commencer à utiliser Amazon EC2
- Mise en route avec AWS Database Migration Service
- Joindre une EC2 instance Amazon à votre répertoire Simple AD Active Directory
- Joindre une EC2 instance Amazon à votre AWS Managed Microsoft AD Active Directory
- AWS Database Migration Service(vidéo)
- Présentation d'Amazon EC2 — Serveur et hébergement Elastic Cloud avec AWS (vidéo)

Migrer une base de données MySQL sur site vers Amazon EC2

Créée par Lorenzo Mota (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données MySQL sur site vers une base de données MySQL sur une instance Amazon Elastic Compute Cloud EC2 (Amazon). Le modèle décrit l'utilisation de AWS Database Migration Service (AWS DMS) ou d'outils MySQL natifs tels que mysqldump pour la migration. Il se concentre sur la migration complète de la base de données vers une instance de base de données MySQL.

Le modèle est principalement destiné aux architectes DBAs et aux architectes de solutions. Il peut être utilisé dans le cadre de petits ou de grands projets, lors d'une phase de test ou de migration finale. Nous vous recommandons d'exécuter au moins un cycle de test avant d'utiliser ce modèle dans un environnement de production.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source MySQL dans un centre de données sur site

Versions du produit

- MySQL version 5.5 et versions ultérieures
- Un système d'exploitation cible pris en charge par Amazon EC2 ; voir Amazon EC2 FAQs

Architecture

Pile technologique source

- Une base de données MySQL sur site

Pile technologique cible

- Une instance de base de données MySQL sur Amazon EC2

Méthodes de migration de données AWS

- AWS DMS
- Des outils MySQL natifs tels que mysqldump ou des outils tiers tels que Percona XtraBackup

Architecture cible

Le schéma suivant illustre la EC2 mise en œuvre cible d'Amazon après le passage.

Architecture de migration de données AWS

À l'aide d'AWS DMS :

Le schéma suivant illustre le flux de travail de migration des données basé sur l'envoi AWS DMS de modifications complètes et incrémentielles à la base de données MySQL cible jusqu'au passage. La connexion réseau depuis le réseau local vers AWS dépend des exigences du client SQL et n'entre pas dans le cadre de ce modèle.

À l'aide d'autres outils MySQL :

Le schéma suivant illustre le flux de travail de migration des données basé sur l'utilisation des outils MySQL pour générer des fichiers de vidage d'exportation à partir de la base de données locale. Ces fichiers sont déplacés vers Amazon Simple Storage Service (Amazon S3) et importés dans la base de données MySQL cible avant le transfert. La connexion réseau depuis le réseau local vers AWS dépend des exigences du client SQL et n'entre pas dans le cadre de ce modèle.

Remarques :

- En fonction des considérations relatives aux temps d'arrêt et de la taille de la base de données pour le transfert final, vous pouvez utiliser AWS DMS un autre outil de capture des données de modification (CDC) pour minimiser le temps de transition. Lorsque vous utilisez un outil CDC tel que AWS DMS, vous pouvez migrer vers la base de données cible en quelques minutes.
- Une stratégie hors ligne avec mysqldump peut suffire si la taille de la base de données et la latence du réseau permettent une courte période de migration. (Nous vous recommandons d'effectuer des tests pour obtenir une durée approximative.)

- En général, une stratégie du CDC AWS DMS nécessite plus de surveillance et de complexité qu'une option hors ligne.

Outils

AWS services

- AWS Database Migration Service (AWS DMS) prend en charge plusieurs bases de données sources et cibles. Pour plus d'informations sur les bases de données source et cible MySQL prises en charge par AWS DMS, consultez les sections Utilisation d'une base de données compatible MySQL comme source pour AWS DMS et Utilisation d'une base de données compatible MySQL comme cible pour. AWS DMS Si votre base de données source n'est pas prise en charge par AWS DMS, vous devez choisir une autre méthode pour migrer vos données.

Autres outils

- mysqldump est un utilitaire MySQL qui crée un fichier dump à partir d'une base de données MySQL à des fins de sauvegarde ou de migration.
- Percona XtraBackup est un utilitaire open source permettant d'effectuer des sauvegardes non bloquantes sur des bases de données MySQL.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions de base de données.	Validez les versions des bases de données source et cible. Pour plus d'informations sur les versions de MySQL prises en charge par AWS DMS, consultez la section Sources AWS DMS et cibles de la AWS DMS documentation. AWS DMS	DBA

Tâche	Description	Compétences requises
Identifiez le système d'exploitation cible.	Déterminez la version du système d'exploitation cible. Pour obtenir la liste des systèmes d'exploitation cibles pris en charge par Amazon EC2, consultez Amazon EC2 FAQs.	DBA, administrateur système
Identifiez les exigences matérielles.	Déterminez la configuration matérielle requise pour l'instance de serveur cible en fonction de la liste de compatibilité MySQL et des exigences en matière de capacité.	DBA, administrateur système
Identifiez les besoins en matière de stockage.	Déterminez le type et la capacité de stockage de la base de données cible.	DBA, administrateur système
Identifiez les exigences du réseau.	Déterminez les exigences du réseau telles que la latence et la bande passante.	DBA, administrateur système
Choisissez le type d'instance cible.	Choisissez le type d'instance cible en fonction de la capacité, des fonctionnalités de stockage et des fonctionnalités réseau.	DBA, administrateur système
Identifiez les exigences en matière de sécurité.	Déterminez les exigences de sécurité d'accès au réseau ou à l'hôte pour les bases de données source et cible.	DBA, administrateur système

Tâche	Description	Compétences requises
Identifiez les utilisateurs.	Déterminez la liste des utilisateurs du système d'exploitation pour l'installation du logiciel MySQL. Pour plus d'informations, veuillez consulter la documentation MySQL.	DBA, administrateur système
Déterminez une stratégie de sauvegarde.		DBA
Déterminez les exigences de disponibilité.		DBA
Identifiez la stratégie de migration ou de transition des applications.		DBA, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un cloud privé virtuel (VPC) et des sous-réseaux.	Configurez les tables de routage, la passerelle Internet, les passerelles NAT et les sous-réseaux. Pour plus d'informations, consultez les options de configuration VPC dans la documentation Amazon VPC.	Administrateur de systèmes
Créez des groupes de sécurité et des listes de contrôle d'accès au réseau (ACLs).	Configurez les ports (la valeur par défaut pour MySQL est 3306) et les plages CIDR ou	Administrateur de systèmes

Tâche	Description	Compétences requises
	spécifiques IPs en fonction de vos besoins.	
Configurez et démarrez une EC2 instance.	Pour obtenir des instructions, consultez la section Lancer une EC2 instance dans la EC2 documentation Amazon.	Administrateur de systèmes

Installez le logiciel MySQL

Tâche	Description	Compétences requises
Créez des utilisateurs et des groupes.	Créez les utilisateurs et les groupes du système d'exploitation qui ont besoin d'accéder au serveur et à la base de données. Pour de plus amples informations, veuillez consulter Contrôle d'accès et gestion des comptes dans la documentation MySQL.	DBA, administrateur système
Téléchargez MySQL.	Téléchargez le logiciel MySQL. Pour les instructions et les fichiers binaires, consultez la section Installation de MySQL dans la documentation MySQL.	DBA, administrateur système
Installez MySQL sur l' EC2 instance et configurez le serveur.	Connectez-vous à votre EC2 instance et installez le logiciel MySQL. Pour plus d'informations, consultez Connect to your EC2 instance dans la EC2 documentation Amazon.	DBA, administrateur système

Migrer les données — option 1

Tâche	Description	Compétences requises
Migrez les données avec MySQL natif ou des outils tiers.	Cette option utilise des outils MySQL natifs ou des outils tiers pour migrer les objets et les données de base de données. Pour obtenir des instructions, consultez la documentation de mysqldump ou de Percona XtraBackup (pour la migration physique) . Pour plus d'informations sur l'utilisation de ces outils, consultez le billet de AWS blog Options de migration pour MySQL vers Amazon RDS for MySQL ou Amazon Aurora MySQL.	DBA

Migrer les données — option 2

Tâche	Description	Compétences requises
Migrez les données avec AWS DMS.	Pour plus d'informations, consultez la section Vue de haut niveau AWS DMS de la AWS DMS documentation.	DBA

Préparez-vous pour le découpage

Tâche	Description	Compétences requises
Recueillez le nombre d'objets.	Recueillez le nombre d'objets à partir de la base de données	DBA

Tâche	Description	Compétences requises
	source et des nouvelles bases de données cibles. Corrigez les éventuelles anomalies dans la base de données cible.	
Vérifiez les dépendances.	Vérifiez que les dépendances (liens) vers et depuis d'autres bases de données sont toujours valides et fonctionn ent correctement.	DBA
Tester.	S'il s'agit d'un cycle de test, effectuez des tests de requêtes, collectez des métriques et corrigez les éventuels problèmes.	DBA

Découper

Tâche	Description	Compétences requises
Déplacez les clients.	Basculez les clients de l'application vers la nouvelle infrastructure.	DBA, propriétaire de l'applica tion, administrateur système
Fournir un soutien.	Fournir une assistance lors des tests fonctionnels des applications.	DBA

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources.	Arrêtez l'instance AWS DMS de réplication et les autres AWS ressources temporaires.	DBA, administrateur système
Révision et documents de projet.	Passez en revue et validez les documents du projet.	DBA, propriétaire de l'application, administrateur système
Collectez des métriques.	Collectez des indicateurs tels que le temps de migration, le pourcentage de modifications manuelles par rapport aux modifications assistées par des outils et les économies de coûts.	DBA, propriétaire de l'application, administrateur système
Clôturez le projet.	Clôturez le projet de migration et faites part de vos commentaires.	DBA, propriétaire de l'application, administrateur système
Mise hors service de la base de données source.	Mettez hors service la base de données MySQL locale.	DBA, administrateur système

Ressources connexes

Références

- EC2 Documentation Amazon
- AWS DMS documentation
- EC2 Tarification Amazon
- AWS DMS Step-by-Step Procédures pas à pas
- mysqldump
- Percona XtraBackup

Tutoriels et vidéos

- Commencer avec AWS DMS
- Présentation d'Amazon EC2 — Serveur et hébergement Elastic Cloud avec AWS (vidéo)

Réduisez le temps de migration homogène vers SAP en utilisant le service de migration d'applications

Créée par Pavel Rubin (AWS), Diego Valverde (AWS) et Sunil Yadav (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration des charges de travail SAP à l'aide d'AWS Application Migration Service. Le service de migration d'applications facilite les transferts en utilisant la réplication au niveau des blocs pour maintenir des volumes de réplication synchronisés en permanence depuis leurs sources.

Les charges de travail SAP incluent les applications SAP Customer Relationship Management (SAP CRM), SAP Enterprise Resource Planning (ERP) et SAP Business Warehouse (SAP BW).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif avec une connectivité réseau stable entre les serveurs SAP source et le cloud privé virtuel (VPC) de destination sur AWS
- Une base de données source SAP Adaptive Server Enterprise (ASE) pour Linux ou Windows dans un centre de données sur site

Limites

- Le système d'exploitation cible doit être pris en charge par Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez Amazon EC2 FAQs.

Architecture

Pile technologique source

- Une base de données SAP ASE

Pile technologique cible

- Amazon EC2
- Amazon Elastic Block Store (Amazon EBS)

Architecture source et cible

Le schéma suivant montre la migration depuis les serveurs locaux via l'agent de réplication vers le point de terminaison du service de migration des applications. Un point de terminaison Amazon Simple Storage Service (Amazon S3) est utilisé pour accéder aux fichiers d'installation et de configuration. Les sous-réseaux de la zone de transit et des ressources migrées contiennent des EC2 instances, les données étant stockées sur des volumes EBS. Le port TCP 443 est utilisé pour connecter le réseau de machines source au service de migration d'applications et pour connecter les sous-réseaux de la zone de transit aux points de terminaison régionaux du service de migration des applications EC2, Amazon et Amazon S3. Le port TCP 1500 est utilisé pour la réplication des données entre le réseau local et la zone intermédiaire.

Outils

- AWS Application Migration Service vous aide à réhéberger (lift-and-shift) des applications dans le cloud AWS sans modification et avec un temps d'arrêt minimal.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Security Token Service (AWS STS) vous aide à demander des informations d'identification temporaires à privilèges limités pour les utilisateurs.

Épopées

Initialiser le service de migration des applications

Tâche	Description	Compétences requises
Initialisez le service de migration des applications.	Initialisez le service de migration des applications dans la région AWS dans laquelle vous souhaitez	Administrateur AWS

Tâche	Description	Compétences requises
	déployer la base de données SAP ASE. AWS fournit une configuration automatique la première fois que vous accédez à la page du service de migration d'applications dans chaque région.	
Créez manuellement des rôles de service.	(Facultatif) Si vous souhaitez utiliser l'automatisation (par exemple, AWS Control Tower) pour configurer le compte, vous pouvez créer manuellement les six rôles AWS Identity and Access Management (IAM) requis pour l'installation, la réplication et les lancements. Pour obtenir des instructions, consultez la documentation AWS.	Administrateur AWS
Créez un modèle de paramètres de réplication.	Le modèle de paramètres de réplication définit le sous-réseau, le type d'instance, le chiffrement Amazon EBS et le mode de routage des données. Pour obtenir des informations détaillées sur les paramètres, consultez la documentation AWS.	AWS général

Générer des informations d'identification pour l'installation de l'

Tâche	Description	Compétences requises
Créez un nouveau rôle IAM.	Sur la console IAM, accédez à Rôles, puis choisissez Create role. Pour le type d'entité de confiance, choisissez le compte AWS, puis Next.	Administrateur système AWS
Attachez-le AWSApplication MigrationAgentPolicy au rôle IAM.	La `AWSApplicationMigrationAgentPolicy` politique gérée par AWS contient les autorisations nécessaires pour effectuer l'installation de l'agent du service de migration des applications. Après avoir joint la politique, choisissez Next.	Administrateur système AWS
Terminez la création du rôle.	Attribuez un nom convivial, puis choisissez Créer un rôle.	Administrateur système AWS
Générez des informations d'identification temporaires.	Pour générer l'ID de clé d'accès, la clé d'accès secrète et le jeton de session, suivez les instructions de la documentation AWS STS. Ces informations d'identification sont utilisées lors de l'installation de l'agent.	Administrateur système AWS

Installez l'agent du service de migration des applications sur la machine source SAP

Tâche	Description	Compétences requises
Téléchargez le programme d'installation de l'agent sur la machine source SAP.	Téléchargez le programme d'installation de l'agent adapté à votre système d'exploitation source : Windows ou Linux.	Propriétaire de l'application
Installez l'agent de réplication AWS.	Lorsque vous exécutez le fichier d'installation de l'agent sur une machine source, vous êtes d'abord invité à saisir votre clé d'accès, votre clé d'accès secrète, votre jeton de session et la région vers laquelle vous souhaitez effectuer la réplication. Utilisez les informations d'identification temporaires du rôle IAM que vous avez créé précédemment et de la même région que celle que vous avez configurée lors de l'initialisation.	Propriétaire de l'application
Attendez la réplication initiale des données.	Une fois l'agent installé, la machine source apparaît dans l'onglet Machines de la console Application Migration Service.	Propriétaire de l'application

Configurer le modèle de lancement de la machine cible

Tâche	Description	Compétences requises
Mettez à jour le modèle de lancement pour le serveur source.	Chaque serveur source utilise un modèle de EC2 lancement unique qui indique la configuration du EC2 serveur cible. Vous pouvez modifier ce modèle si vous souhaitez personnaliser la EC2 configuration Amazon de votre serveur migré.	AWS général
Définissez la version du modèle de lancement par défaut.	Après avoir apporté les modifications requises au modèle de lancement , spécifiez d'utiliser cette version mise à jour comme modèle de lancement par défaut. Pour plus d'informations, consultez la documentation AWS.	AWS général
Désactivez le dimensionnement correct du type d'instance.	(Facultatif) Le dimensionnement correct du type d'instance fournit des recommandations automatiques sur le type d'instance en fonction de la configuration du serveur SAP source. Nous vous recommandons de désactiver ce paramètre afin de pouvoir spécifier des types d'instances personnalisés dans le modèle de lancement.	AWS général

Réaliser un test

Tâche	Description	Compétences requises
Lancez un test.	Sur la console du service de migration d'applications, sélectionnez un ou plusieurs serveurs, puis sélectionnez Lancer des instances de test sous Test and Cutover.	AWS général, ingénieur en migration, responsable de la migration
Attendez que le processus de conversion et de lancement soit terminé.	Vous pouvez consulter le processus de lancement dans l'onglet Historique des lancements. Une fois que la machine a été lancée avec succès en tant qu' EC2 instance, l'onglet Alertes passe à Launched.	
Vérifiez que le test s'est bien déroulé.	Connectez-vous à l'instance lancée via le protocole RDP (Remote Desktop Protocol) ou SSH (Secure Shell) et effectuez les vérifications d'application appropriées. Par exemple, connectez-vous à l'interface SAP et validez les fonctionnalités.	Ingénieur en migration, propriétaire de l'application
Mettez à jour le cycle de vie de la source.	Si le test est réussi, mettez à jour le cycle de vie de la machine source en indiquant « Prêt pour le passage » dans l'onglet Test and Cutover.	Ingénieur en migration, responsable de la migration

Planifiez et effectuez un transfert vers la cible Amazon EC2

Tâche	Description	Compétences requises
Planifiez une fenêtre de transition.		Responsable du transfert, responsable de la migration, propriétaire de l'application
Lancez un lancement de transition.	Sélectionnez un ou plusieurs serveurs. Dans l'onglet Test and Cutover, sélectionnez Lancer des instances de transition sous Test and Cutover sur la console du service de migration d'applications.	Ingénieur en migration
Attendez que les processus de conversion et de lancement soient terminés.	Vous pouvez consulter le processus de lancement dans l'onglet Historique des lancements. Une fois que la machine a été lancée avec succès en tant qu' EC2 instance, l'onglet Alertes passe à Launched.	
Vérifiez que le transfert s'est effectué correctement.	Connectez-vous à l'instance lancée via RDP ou SSH et effectuez les vérifications d'application appropriées.	Propriétaire de l'application, ingénieur en migration
Mettez à jour le cycle de vie de la source.	Si le transfert est réussi, mettez à jour le cycle de vie de la machine source en sélectionnant Finaliser le transfert dans l'onglet Test et transfert.	Ingénieur en migration

Ressources connexes

Références

- AWS Application Migration Service
- FAQ sur la migration des applications AWS

Vidéo

- Architecture du service de migration d'applications AWS

Réhébergez les charges de travail sur site dans le cloud AWS : liste de contrôle pour la migration

Créée par Srikanth Rangavajhala (AWS)

Récapitulatif

Le réhébergement des charges de travail sur site dans le cloud Amazon Web Services (AWS) implique les phases de migration suivantes : planification, pré-découverte, découverte, création, test et transfert. Ce modèle décrit les phases et les tâches connexes. Les tâches sont décrites de manière détaillée et prennent en charge environ 75 % de toutes les charges de travail des applications. Vous pouvez implémenter ces tâches sur une période de deux à trois semaines dans le cadre d'un cycle de sprint agile.

Vous devez passer en revue et valider ces tâches avec votre équipe de migration et vos consultants. Après l'examen, vous pouvez recueillir les informations, éliminer ou réévaluer les tâches selon les besoins, et modifier d'autres tâches pour prendre en charge au moins 75 % des charges de travail des applications de votre portefeuille. Vous pouvez ensuite utiliser un outil de gestion de projet agile tel qu'Atlassian Jira ou Rally Software pour importer les tâches, les affecter aux ressources et suivre vos activités de migration.

Le modèle suppose que vous utilisez AWS Cloud Migration Factory pour réhéberger vos charges de travail, mais que vous pouvez utiliser l'outil de migration de votre choix.

Amazon Macie peut vous aider à identifier les données sensibles dans vos bases de connaissances, stockées sous forme de sources de données, de modèles de journaux d'invocation et de commandes de commandes dans des compartiments Amazon Simple Storage Service (Amazon S3). Pour plus d'informations, consultez la documentation Macie.

Conditions préalables et limitations

Prérequis

- Outil de gestion de projet pour le suivi des tâches de migration (par exemple, Atlassian Jira ou Rally Software)
- Outil de migration pour réhéberger vos charges de travail sur AWS (par exemple, Cloud Migration Factory)

Architecture

Plateforme source

- Pile source sur site (y compris les technologies, les applications, les bases de données et l'infrastructure)

Plateforme cible

- Stack cible du cloud AWS (y compris les technologies, les applications, les bases de données et l'infrastructure)

Architecture

Le schéma suivant illustre le réhébergement (découverte et migration de serveurs depuis un environnement source sur site vers AWS) à l'aide de Cloud Migration Factory et d'AWS Application Migration Service.

Outils

- Vous pouvez utiliser l'outil de migration et de gestion de projet de votre choix.

Épopées

Phase de planification

Tâche	Description	Compétences requises
Résorber l'arriéré préalable à la découverte.	Organisez la séance de travail préalable à la découverte du backlog avec les responsables des services et les propriéta ires d'applications.	Chef de projet, responsable Agile Scrum
Diriger la séance de travail sur la planification du sprint.	Dans le cadre d'un exercice de cadrage, répartissez les applications que vous	Chef de projet, responsable Agile Scrum

Tâche	Description	Compétences requises
	souhaitez migrer entre des sprints et des vagues.	

Phase préalable à la découverte

Tâche	Description	Compétences requises
Confirmez la connaissance de l'application.	Confirmez et documentez le propriétaire de l'application et sa connaissance de l'applica tion. Déterminez s'il existe un autre point de contact pour les questions techniques.	Spécialiste de la migration (intervieweur)
Déterminez les exigences de conformité des applications.	Vérifiez auprès du propriétaire de l'application que l'applica tion n'est pas tenue de respecter les exigences de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS), de la loi Sarbanes-Oxley (SOX), des informati ons personnelles identifiables (PII) ou d'autres normes. Si des exigences de conformité existent, les équipes doivent terminer leurs contrôles de conformité sur les serveurs qui seront migrés.	Spécialiste de la migration (intervieweur)
Confirmez les exigences relatives à la mise en production.	Vérifiez les exigences relatives à la mise en production de l'application migrée (telles que la date de sortie et la durée	Spécialiste de la migration (intervieweur)

Tâche	Description	Compétences requises
	du temps d'arrêt) auprès du propriétaire de l'application ou du contact technique.	
Obtenez la liste des serveurs.	Obtenez la liste des serveurs associés à l'application ciblée.	Spécialiste de la migration (intervieweur)
Obtenez le diagramme logique qui montre l'état actuel.	Obtenez le diagramme d'état actuel de l'application auprès de l'architecte d'entreprise ou du propriétaire de l'application.	Spécialiste de la migration (intervieweur)
Créez un diagramme logique qui montre l'état cible.	Créez un schéma logique de l'application qui montre l'architecture cible sur AWS. Ce diagramme doit illustrer les serveurs, la connectivité et les facteurs de mappage.	Architecte d'entreprise, propriétaire d'entreprise
Obtenez des informations sur le serveur.	Collectez des informations sur les serveurs associés à l'application, notamment les détails de leur configuration.	Spécialiste de la migration (intervieweur)
Ajoutez les informations du serveur au modèle de découverte.	Ajoutez des informations détaillées sur le serveur au modèle de découverte d'applications (voir ce modèle `mobilize-application-questionnaire.xlsx` en pièce jointe). Ce modèle inclut tous les détails relatifs à la sécurité, à l'infrastructure, au système d'exploitation et au réseau liés aux applications.	Spécialiste de la migration (intervieweur)

Tâche	Description	Compétences requises
Publiez le modèle de découverte d'applications.	Partagez le modèle de découverte d'applications avec le propriétaire de l'application et l'équipe de migration pour un accès et une utilisation communs.	Spécialiste de la migration (intervieweur)

Phase de découverte

Tâche	Description	Compétences requises
Confirmez la liste des serveurs.	Vérifiez la liste des serveurs et l'objectif de chaque serveur auprès du propriétaire de l'application ou du responsable technique.	Spécialiste de la migration
Identifiez et ajoutez des groupes de serveurs.	Identifiez les groupes de serveurs tels que les serveurs Web ou les serveurs d'applications, et ajoutez ces informations au modèle de découverte d'applications. Sélectionnez le niveau de l'application (Web, application, base de données) auquel chaque serveur doit appartenir.	Spécialiste de la migration
Renseignez le modèle de découverte de l'application.	Complétez les détails du modèle de découverte d'applications avec l'aide de l'équipe de migration, de l'équipe d'application et d'AWS.	Spécialiste de la migration

Tâche	Description	Compétences requises
Ajoutez les informations manquantes sur le serveur (équipes du middleware et du système d'exploitation).	Demandez aux équipes du middleware et du système d'exploitation (OS) de revoir le modèle de découverte des applications et d'ajouter les informations manquantes sur le serveur, y compris les informations de base de données.	Spécialiste de la migration
Obtenez les règles relatives au trafic entrant/sortant (équipe réseau).	Demandez à l'équipe réseau de connaître les règles de trafic entrant/sortant pour les serveurs source et de destination. L'équipe réseau doit également ajouter des règles de pare-feu existantes, les exporter vers un format de groupe de sécurité et ajouter des équilibreurs de charge existants au modèle de découverte d'applications.	Spécialiste de la migration
Identifiez le marquage requis.	Déterminez les exigences en matière de balisage pour l'application.	Spécialiste de la migration
Créez les détails de la demande de pare-feu.	Capturez et filtrez les règles de pare-feu requises pour communiquer avec l'application.	Spécialiste de la migration, architecte de solutions, responsable réseau

Tâche	Description	Compétences requises
Mettez à jour le type d' EC2 instance.	Mettez à jour le type d'instance Amazon Elastic Compute Cloud (Amazon EC2) à utiliser dans l'environnement cible, en fonction des exigences en matière d'infrastructure et de serveur.	Spécialiste de la migration, architecte de solutions, responsable réseau
Identifiez le diagramme d'état actuel.	Identifiez ou créez le diagramme qui montre l'état actuel de l'application. Ce diagramme sera utilisé dans la demande de sécurité des informations (InfoSec).	Spécialiste de la migration, architecte de solutions
Finalisez le futur diagramme d'état.	Finalisez le diagramme qui montre l'état futur (cible) de l'application. Ce schéma sera également utilisé dans la InfoSec demande.	Spécialiste de la migration, architecte de solutions
Créez des demandes de service de pare-feu ou de groupe de sécurité.	Créez des demandes de service de pare-feu ou de groupe de sécurité (pour le développement/l'assurance qualité, la pré-production et la production). Si vous utilisez Cloud Migration Factory, incluez les ports spécifiques à la réplication s'ils ne sont pas déjà ouverts.	Spécialiste de la migration, architecte de solutions, responsable réseau

Tâche	Description	Compétences requises
Passez en revue les demandes de pare-feu ou de groupe de sécurité (InfoSec équipe).	Au cours de cette étape, l' InfoSec équipe examine et approuve les demandes de pare-feu ou de groupe de sécurité créées à l'étape précédente.	InfoSec ingénieur, spécialiste de la migration
Mettez en œuvre les demandes de groupe de sécurité du pare-feu (équipe réseau).	Une fois que l' InfoSec équipe a approuvé les demandes de pare-feu, l'équipe réseau met en œuvre les règles de pare-feu entrantes et sortantes requises.	Spécialiste de la migration , architecte de solutions, responsable réseau

Phase de construction (à répéter pour les environnements de développement/assurance qualité, de pré-production et de production)

Tâche	Description	Compétences requises
Importez les données de l'application et du serveur.	1. Vérifiez que vous êtes connecté à votre serveur d'exécution de la migration en tant qu'utilisateur de domaine avec des autorisations d'administrateur local sur les serveurs sources concernés. 2. Utilisez le formulaire de demande de migration pour importer les attributs des serveurs sources concernés . Pour plus d'informations, consultez le guide de	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
	mise en œuvre de Cloud Migration Factory. Si vous n'utilisez pas Cloud Migration Factory, suivez les instructions de configuration de votre outil de migration.	
Vérifiez les conditions requises pour les serveurs source.	Connectez-vous aux serveurs source concernés pour vérifier les conditions requises telles que le port TCP 1500, le port TCP 443, l'espace libre sur le volume racine, la version du .NET Framework et d'autres paramètres. Ils sont nécessaires pour la réplicati on. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud
Créez une demande de service pour installer des agents de réplication.	Créez une demande de service pour installer des agents de réplication sur les serveurs concernés à des fins de développement/d'as surance qualité, de pré-produ ction ou de production.	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Installez les agents de réplication.	Installez les agents de réplication sur les serveurs sources concernés sur les machines de développement/d'assurance qualité, de pré-production ou de production. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud
Appuyez sur les scripts de post-lancement.	Le service de migration d'applications prend en charge les scripts de post-lancement pour vous aider à automatiser les activités au niveau du système d'exploitation, telles que l'installation ou la désinstallation de logiciels après le lancement des instances cibles. Cette étape envoie les scripts de post-lancement aux machines Windows ou Linux, en fonction des serveurs identifiés pour la migration. Pour obtenir des instructions, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Vérifiez l'état de la réplication.	Vérifiez automatiquement l'état de réplication pour les serveurs sources concernés à l'aide du script fourni. Le script se répète toutes les cinq minutes jusqu'à ce que l'état de tous les serveurs sources de la vague donnée passe à Healthy. Pour obtenir des instructions, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud
Créez l'utilisateur administrateur.	Un administrateur local ou un utilisateur sudo sur les machines source peut être nécessaire pour résoudre les problèmes éventuels après le passage de la migration des serveurs source concernés vers AWS. L'équipe de migration utilise cet utilisateur pour se connecter au serveur cible lorsque le serveur d'authentification (par exemple, le serveur DC ou LDAP) n'est pas accessible. Pour obtenir des instructions relatives à cette étape, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Validez le modèle de lancement.	Validez les métadonné es du serveur pour vous assurer qu'elles fonctionnent correctement et qu'elles ne contiennent aucune donnée non valide. Cette étape valide à la fois les métadonnées de test et de transfert. Pour obtenir des instructions, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud

Phase de test (à répéter pour les environnements de développement/assurance qualité, de pré-production et de production)

Tâche	Description	Compétences requises
Créez une demande de service.	Créez une demande de service pour que l'équipe d'infrastructure et les autres équipes effectuent le transfert des applications vers des instances de développement/ assurance qualité, de pré-production ou de production.	Spécialiste de la migration, administrateur cloud
Configurez un équilibreur de charge (facultatif).	Configurez les équilibreurs de charge requis, tels qu'un Application Load Balancer ou un équilibreur de charge F5 avec iRules.	Spécialiste de la migration, administrateur cloud
Lancez des instances à des fins de test.	Lancez toutes les machines cibles pour une vague donnée	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
	dans Application Migration Service en mode test. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	
Vérifiez l'état de l'instance cible.	Vérifiez l'état de l'instance cible en vérifiant le processus de démarrage de tous les serveurs source concernés au cours de la même vague. Le démarrage des instances cibles peut prendre jusqu'à 30 minutes. Vous pouvez vérifier le statut manuellem ent en vous connectant à la EC2 console Amazon, en recherchant le nom du serveur source et en consultant la colonne de vérification du statut. Les vérifications de statut 2/2 passées indiquent que l'instance est saine du point de vue de l'infrastructure.	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Modifiez les entrées DNS.	Modifiez les entrées du système de noms de domaine (DNS). (À utiliser `resolv.conf` ou `host.conf` pour un environnement Microsoft Windows.) Configurez chaque EC2 instance pour qu'elle pointe vers la nouvelle adresse IP de cet hôte. **Note** Assurez-vous qu'il n'existe aucun conflit DNS entre les serveurs sur site et les serveurs du cloud AWS. Cette étape et les suivantes sont facultatives, en fonction de l'environnement dans lequel le serveur est hébergé.	Spécialiste de la migration, administrateur cloud
Testez la connectivité aux hôtes principaux à partir des EC2 instances.	Vérifiez les connexions à l'aide des informations d'identification de domaine des serveurs migrés.	Spécialiste de la migration, administrateur cloud
Mettez à jour l'enregistrement DNS A.	Mettez à jour l'enregistrement DNS A pour chaque hôte afin qu'il pointe vers la nouvelle adresse IP EC2 privée Amazon.	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Mettez à jour l'enregistrement DNS CNAME.	Mettez à jour l'enregistrement DNS CNAME pour le virtuel IPs (noms des équilibreurs de charge) afin qu'il pointe vers le cluster pour les serveurs Web et d'applications.	Spécialiste de la migration, administrateur cloud
Testez l'application dans les environnements applicables.	Connectez-vous à la nouvelle EC2 instance et testez l'application dans les environnements de développement/assurance qualité, de pré-production et de production.	Spécialiste de la migration, administrateur cloud
Marquer comme prêt pour le découpage.	Lorsque le test est terminé, modifiez l'état du serveur source pour indiquer qu'il est prêt pour le passage, afin que les utilisateurs puissent lancer une instance de transfert. Pour obtenir des instructions, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud

Phase de transition

Tâche	Description	Compétences requises
Créez un plan de déploiement de production.	Créez un plan de déploiement de production (y compris un plan de backout).	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Avisez l'équipe des opérations en cas d'indisponibilité.	Informez l'équipe des opérations du calendrier d'indisponibilité des serveurs. Certaines équipes peuvent avoir besoin d'un ticket de demande de modification ou de demande de service (CR/SR) pour cette notification.	Spécialiste de la migration, administrateur cloud
Répliquez les machines de production.	Répliquez les machines de production à l'aide du service de migration d'applications ou d'un autre outil de migration.	Spécialiste de la migration, administrateur cloud
Arrêtez les serveurs sources concernés.	Après avoir vérifié l'état de réplication des serveurs source, vous pouvez arrêter les serveurs sources pour arrêter les transactions entre les applications clientes et les serveurs. Vous pouvez arrêter les serveurs sources dans la fenêtre de transition. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	Administrateur du cloud
Lancez des instances pour le transfert.	Lancez toutes les machines cibles pour une vague donnée dans Application Migration Service en mode cutover. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud

Tâche	Description	Compétences requises
Récupérez l'instance cible IPs.	Récupérez IPs les quatre instances cibles. Si la mise à jour du DNS est un processus manuel dans votre environnement, vous devez obtenir les nouvelles adresses IP pour toutes les instances cibles. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud
Vérifiez les connexions au serveur cible.	Après avoir mis à jour les enregistrements DNS, connectez-vous aux instances cibles avec le nom d'hôte pour vérifier les connexions. Pour plus d'informations, consultez le guide de mise en œuvre de Cloud Migration Factory.	Spécialiste de la migration, administrateur cloud

Ressources connexes

- Comment effectuer la migration
- Guide de mise en œuvre d'AWS Cloud Migration Factory
- Automatiser les migrations de serveurs à grande échelle avec Cloud Migration Factory
- Guide de l'utilisateur du service de migration d'applications AWS
- Programme d’accélération des migrations AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Configurez une infrastructure multi-AZ pour un SQL Server Always On FCI à l'aide d'Amazon FSx

Créée par Manish Garg (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Nishad Mankar (AWS) et RAJNEESH TYAGI (AWS)

Récapitulatif

Si vous devez migrer rapidement un grand nombre d'instances de cluster Microsoft SQL Server Always On Failover (FCIs), ce modèle peut vous aider à réduire le temps de provisionnement. En utilisant l'automatisation et Amazon FSx pour Windows File Server, il réduit les efforts manuels, les erreurs causées par l'homme et le temps nécessaire au déploiement d'un grand nombre de clusters.

Ce modèle configure l'infrastructure de SQL Server FCIs dans un déploiement de zones de disponibilité multiple (multi-AZ) sur Amazon Web Services (AWS). Le provisionnement des services AWS requis pour cette infrastructure est automatisé à l'aide de CloudFormation modèles AWS. L'installation de SQL Server et la création de nœuds de cluster sur une instance Amazon Elastic Compute Cloud (Amazon EC2) sont effectuées à l'aide de PowerShell commandes.

Cette solution utilise un système de fichiers Amazon FSx pour Windows multi-AZ à haute disponibilité comme témoin partagé pour le stockage des fichiers de base de données SQL Server. Le système de FSx fichiers Amazon et les instances EC2 Windows qui hébergent SQL Server sont joints au même domaine AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un utilisateur AWS disposant des autorisations suffisantes pour provisionner des ressources à l'aide de CloudFormation modèles AWS
- AWS Directory Service pour Microsoft Active Directory
- Informations d'identification dans AWS Secrets Manager pour s'authentifier auprès d'AWS Managed Microsoft AD dans une paire clé-valeur :
  - `ADDomainName`: <Domain Name>
  - `ADDomainJoinUserName`: <Domain Username>
  - `ADDomainJoinPassword`: <Domain User Password>
  - `TargetOU`: <Target OU Value>

> **Note**
>
> Vous utiliserez le même nom de clé dans l'automatisation d'AWS Systems Manager pour l'activité de jointure avec AWS Managed Microsoft AD.

- Fichiers multimédia SQL Server pour l'installation de SQL Server et création de comptes de service ou de domaine Windows, qui seront utilisés lors de la création du cluster
- Un cloud privé virtuel (VPC), avec deux sous-réseaux publics dans des zones de disponibilité distinctes, deux sous-réseaux privés dans les zones de disponibilité, une passerelle Internet, des passerelles NAT, des associations de tables de routage et un serveur de saut

Versions du produit

- Windows Server 2012 R2 et Microsoft SQL Server 2016

Architecture

Pile technologique source

- SQL Server sur site avec FCIs utilisation d'un lecteur partagé

Pile technologique cible

- EC2 Instances AWS
- Serveur FSx de fichiers Amazon pour Windows
- Manuel d'utilisation d'AWS Systems Manager Automation
- Configurations réseau (VPC, sous-réseaux, passerelle Internet, passerelles NAT, serveur de saut, groupes de sécurité)
- AWS Secrets Manager
- AWS Managed Microsoft AD
- Amazon EventBridge
- AWS Identity and Access Management (IAM)

Architecture cible

Le schéma suivant montre un compte AWS dans une seule région AWS, avec un VPC comprenant deux zones de disponibilité, deux sous-réseaux publics avec des passerelles NAT, un serveur de saut dans le premier sous-réseau public, deux sous-réseaux privés, chacun avec une EC2 instance pour un nœud SQL Server dans un groupe de sécurité de nœuds, et un système de FSx fichiers Amazon se connectant à chacun des nœuds SQL Server. AWS Directory Service, Amazon EventBridge, AWS Secrets Manager et AWS Systems Manager sont également inclus.

Automatisation et mise à l'échelle

- Vous pouvez utiliser AWS Systems Manager pour rejoindre AWS Managed Microsoft AD et effectuer l'installation de SQL Server.

Outils

Services AWS

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS Directory Service propose plusieurs manières d'utiliser Microsoft Active Directory (AD) avec d'autres services AWS tels qu'Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) pour SQL Server et FSx Amazon pour Windows File Server.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions AWS Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres comptes AWS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- AWS Systems Manager vous aide à gérer vos applications et votre infrastructure exécutées dans le cloud AWS. Il simplifie la gestion des applications et des ressources, réduit le délai de détection

et de résolution des problèmes opérationnels et vous aide à gérer vos ressources AWS en toute sécurité à grande échelle.

Autres outils

- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS. Ce modèle utilise des PowerShell scripts.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub aws-windows-failover-cluster-automation.

Bonnes pratiques

- Les rôles IAM utilisés pour déployer cette solution doivent respecter le principe du moindre privilège. Pour de plus amples informations, veuillez consulter la documentation IAM.
- Suivez les CloudFormation meilleures pratiques d'AWS.

Épopées

Déployer l'infrastructure

Tâche	Description	Compétences requises
Déployez la CloudFormation pile Systems Manager.	1. Connectez-vous à votre compte AWS et ouvrez l'AWS Management Console. 2. Accédez à la CloudFormation console et créez la CloudFormation pile Systems Manager en téléchargeant le `ssm.yaml` modèle. Fournissez des valeurs pour les paramètres suivants :	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	• StateUnJoinAssociationLoggingBucketName— Fournissez un nom pour le compartiment S3 que le modèle créera à des fins de journalisation. • SSMAssociationADUnjoinNom — Donnez un nom à la `AWS::SSM::Association` ressource. • SSMAutomationDocumentName— Entrez un nom pour le runbook Systems Manager Automation. • EventBridgeName— Donnez un nom au bus EventBridge d'événements. 3. Déployez la CloudFormation pile Systems Manager en lançant le `ssm.yaml` CloudFormation modèle. Le modèle créera le manuel d'exécution de Systems Manager Automation qui est lancé lors du lancement d'une nouvelle EC2 instance avec le tag. `ADJoined: FSXADD` Le runbook d'automatisation ajoutera l'instance au	

Tâche	Description	Compétences requises
	répertoire Microsoft AD géré par AWS.	

Tâche	Description	Compétences requises
Déployez la pile d'infrast ructure.	Après le déploiement réussi de la pile Systems Manager, créez la `infra` pile, qui inclut les nœuds d' EC2 instance, les groupes de sécurité, le système de fichiers Amazon FSx pour Windows File Server et le rôle IAM. 1. Accédez à la CloudForm ation console et lancez le `infra-cf.yaml` modèle. Pour déployer cette pile, les paramètres suivants sont requis : • `ActiveDir ectoryId` — ID pour Microsoft AD géré par AWS • `ADDnsIpAd dresses1` — Adresse IP DNS principale de Microsoft AD géré par AWS • `ADDnsIpAd dresses2` — Adresse IP DNS secondaire de Microsoft AD géré par AWS • `FSxSecurityGroupNa me` — Nom du groupe FSx de sécurité Amazon	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	• `FSxWindowsFileSystemName` — Nom du FSx lecteur Amazon • `ImageID`— ID de l'image Windows 2012 R2 de base ou de l'image Amazon Machine (AMI) utilisée pour créer le nœud d'instance SQL Server • `KeyPairName` — Paire clé-valeur à attacher aux nœuds d' EC2 instance pour y accéder • `Node1SecurityGroupName` — Nom du premier groupe de sécurité du nœud • `Node2SecurityGroupName` — Nom du groupe de sécurité du deuxième nœud • `OUSecretName` — Nom du secret contenant les informations Microsoft AD gérées par AWS • `PrivateSubnet1` — ID du premier sous-réseau privé • `PrivateSubnet2` — ID du deuxième sous-réseau privé	

Tâche	Description	Compétences requises
	• `SqlFSxFCIName` — Nom de la balise appliquée aux nœuds principal et secondaire et à Amazon FSx. • `SqlFSxServerNetBIOSName1` — Nom du nœud de l' EC2 instance principale (15 caractères maximum) • `SqlFSxServerNetBIOSName2` — Nom du nœud d' EC2 instance secondaire (15 caractères maximum) • `VPC`— ID VPC • `WorkloadInstanceType` — Type d' EC2 instance Déployez la `infra` pile. La pile créera tous les composants d'infrastructure nécessaires à la configuration de Windows SQL Server FCI. 2. Une fois les nœuds d' EC2 instance lancés, le document Systems Manager Automation sera invoqué pour joindre ces instances à AWS Managed Microsoft AD. Vous pouvez suivre la progression sur la	

Tâche	Description	Compétences requises
	page Automatisation de la console Systems Manager.	

Configurer le système Windows SQL Server Always On (FCI)

Tâche	Description	Compétences requises

Installez les outils Windows.	1. Connectez-vous à l' EC2 instance principale, qui est le nœud 1. Pour installer les fonctionnalités Windows (Active Directory et FCI Tools), exécutez le PowerShell script suivant.
	`Install-WindowsFeature -Name RSAT-AD-Powershell,Failover-Clustering -IncludeManagementTools`
	`Install-WindowsFeature -Name RSAT-Clustering,RSAT-ADDS-Tools,RSAT-AD-Powershell,RSAT-DHCP,RSAT-DNS-Server`
	2. Connectez-vous à l' EC2 instance secondaire, qui est le nœud 2, et exécutez le même script pour activer les fonctionnalités sur le nœud 2.
		AWS DevOps, DevOps ingénieur, DBA

Préinstallez les objets informatiques du cluster dans	Pour préparer l'objet de nom de cluster (CNO) dans les services de domaine Active	AWS DevOps, DBA, ingénieur DevOps

Tâche	Description	Compétences requises
les services de domaine Active Directory.	Directory (AD DS) et préparer un objet d'ordinateur virtuel (VCO) pour un rôle de cluster, suivez les instructions de la documentation de Windows Server.	

Tâche	Description	Compétences requises
Créez le WSFC.	Pour créer le cluster Windows Server Failover Clustering (WSFC), procédez comme suit : 1. Connectez-vous à l' EC2 instance principale, qui est le nœud 1. Pour créer le partage de FSx fichiers Amazon et accorder un accès complet au compte de service AD répertorié, exécutez le code suivant. `Invoke-Command -ComputerName "<FSx Windows Remote PowerShell Endpoint>" -ConfigurationName FSxRemoteAdmin -scriptblock { New-FSxSmbShare -Name "SQLDB" -Path "D:\share" -Description "SQL Databases Share" -ContinuouslyAvailable $true -FolderEnumerationMode AccessBased -EncryptData $true grant-fsxsmbshareaccess -name SQLDB -AccountName "<domain\user>" -accessRight Full }`	AWS DevOps, DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	Cette commande créera également le partage de fichiers disponible en permanence (CA), optimisé pour une utilisation par Microsoft SQL Server. 2. Pour créer le cluster de basculement sur l'instanc e principale (nœud 1), exécutez la commande suivante. `New-Cluster -Name <CNO Name> -Node <Node1 Name>, <Node2 Name> -StaticAddress <Node1 Secondary Private IP>, <Node2 Secondary Private IP>` La commande nécessite les paramètres suivants : • `Name`— Le nom du cluster (CNO) • `Node`— Les noms des nœuds principal et secondaire, respectiv ement • `StaticAddress` — Les adresses IP secondair es des nœuds principal et secondaire, respectiv ement	

Tâche	Description	Compétences requises
	Important Un administrateur de domaine ou un utilisateur normal doit disposer d'une autorisation d'administrateur sur les deux nœuds pour créer le cluster Windows Server Failover Clustering (WSFC). Dans le cas contraire, la commande précédente échouera et renverra le message,`You do not have administrator privilege on servers`. 3. Une fois le cluster créé, exécutez la commande suivante pour joindre le témoin de partage de fichiers. `Set-ClusterQuorum -FileShareWitness \ \<FSx Windows Remote`	

Tâche	Description	Compétences requises
	PowerShell Endpoint>\share\witness	

Tâche	Description	Compétences requises
Installez le cluster de basculement SQL Server.	Une fois le cluster WSFC configuré, installez le cluster SQL Server sur l'instance principale (node1). 1. Dans le lecteur T sur les deux nœuds, créez `tempdb` et `log` dossiers. Les dossiers sont utilisés dans les PowerShell commandes . 2. Après avoir copié les fichiers multimédias de SQL Server pour l'install ation de SQL Server sur les deux nœuds, exécutez la PowerShell commande suivante sur le nœud 1 pour installer SQL Server sur le nœud 1. `D:\setup.exe /Q ` ` /ACTION=InstallF ailoverCluster ` /IACCEPTSQLSERVE RLICENSETERMS ` /FEATURES="SQL,I S,BC,Conn" ` /INSTALLSHAREDDIR="C: \Program Files\Mic rosoft SQL Server” ` /INSTALLSHAREDWO WDIR="C:\Program Files (x86)\Microsoft SQL Server" ` `	AWS DevOps, DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	/RSINSTALLMODE="FilesOnlyMode" ` /INSTANCEID="MSSQLSERVER" ` /INSTANCENAME="MSSQLSERVER" ` /FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` /FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node1>;Cluster Network 1;<subnet mask>" ` /FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` /INSTANCEDIR="C:\Program Files\Microsoft SQL Server" ` /ENU="True" ` /ERRORREPORTING=0 ` /SQMREPORTING=0 ` /SAPWD="<Domain User password>" ` /SQLCOLLATION="SQL_Latin1_General_CP1_CI_AS" ` /SQLSYSADMINACCOUNTS="<domain\username>" ` /SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` /AGTSVCACCOUNT="<domain\username>" /AGTSVCPASSWORD="<Domain User password>" `	

Tâche	Description	Compétences requises
	`/ISSVCACCOUNT="<domain\username>" /ISSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/INSTALLSQLDATADIR="\\<FSX DNS name>\share\Program Files\Microsoft SQL Server" ` `/SQLUSERDBDIR="\\<FSX DNS name>\share\data" ` `/SQLUSERDBLOGDIR="\\<FSX DNS name>\share\log" ` `/SQLTEMPDBDIR="T:\tempdb" ` `/SQLTEMPDBLOGDIR="T:\log" ` `/SQLBACKUPDIR="\\<FSX DNS name>\share\SQLBackup" ` `/SkipRules=Cluster_VerifyForErrors ` `/INDICATEPROGRESS`	

Tâche	Description	Compétences requises
Ajoutez un nœud secondaire au cluster.	Pour ajouter SQL Server au nœud secondaire (nœud 2), exécutez la PowerShell commande suivante. `D:\setup.exe /Q ` `/ACTION=AddNode ` `/IACCEPTSQLSERVERLICENSETERMS ` `/INSTANCENAME="MSSQLSERVER" ` `/FAILOVERCLUSTERGROUP="SQL Server (MSSQLSERVER)" ` `/FAILOVERCLUSTERIPADDRESSES="IPv4;<2nd Sec Private Ip node2>;Cluster Network 2;<subnet mask>" ` `/FAILOVERCLUSTERNETWORKNAME="<Fail over cluster Network Name>" ` `/CONFIRMIPDEPENDENCYCHANGE=1 ` `/SQLSVCACCOUNT="<domain\username>" /SQLSVCPASSWORD="<Domain User password>" ` `/AGTSVCACCOUNT="domain\username>" /AGTSVCPASSWORD="<Domain User password>" ` `/FTSVCACCOUNT="NT Service\MSSQLFDLauncher" ` `/SkipRules=Cluster_VerifyForErrors `	AWS DevOps, DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	`/INDICATEPROGRESS`	
Testez le SQL Server FCI.	1. Sur l'instance Windows de l'un des nœuds, dans Outils d'administration, lancez le Failover Cluster Manager. 2. Accédez à Nodes et vérifiez que le statut du nœud est Status Running. 3. Sélectionnez Rôles, ouvrez le menu contextuel (clic droit) de SQL Server (MSSQLSERVER), puis sélectionnez Déplacer et sélectionner un nœud. 4. Une fois le nœud sélectionné, SQL Server devrait être exécuté sur l'autre nœud.	DBA, ingénieur DevOps

Nettoyage des ressources

Tâche	Description	Compétences requises
Nettoyez les ressources.	Pour nettoyer les ressources, utilisez le processus de suppression de la CloudFormation pile AWS : 1. Ouvrez la CloudFormation console AWS. 2. Sur la page Stacks, sélectionnez la `infra` pile. La pile doit être en cours d'exécution.	AWS DevOps, DBA, ingénieur DevOps

Tâche	Description	Compétences requises
	3. Dans le volet des détails de la pile, choisissez Supprimer. 4. Sélectionnez Supprimer la pile lorsque vous y êtes invité. 5. Répétez les étapes 2 à 4 pour la `ssm` pile. Une fois la suppression des piles terminée, les piles seront dans leur `DELETE_COMPLETE` état actuel. Les piles dans `DELETE_COMPLETE` cet état ne sont pas affichées dans la CloudFormation console par défaut. Pour afficher les piles supprimées, vous devez modifier le filtre de vue des piles comme décrit dans Afficher les piles supprimées sur la console AWS CloudFormation . Si la suppression a échoué, une pile sera dans `DELETE_FAILED` cet état. Pour les solutions, consultez la section Supprimer les échecs de la pile dans la CloudFormation documentation.	

Résolution des problèmes

Problème	Solution
Défaillance CloudFormation du modèle AWS	Si le CloudFormation modèle échoue pendant le déploiement, procédez comme suit : 1. Ouvrez la CloudFormation console AWS. 2. Sur la page Stacks de la CloudFormation console, sélectionnez la pile. 3. Choisissez Events, puis vérifiez l'état de la pile.
Échec de la jointure avec AWS Managed Microsoft AD	Pour résoudre les problèmes de jointure, procédez comme suit : 1. Ouvrez la console Systems Manager. 2. Sélectionnez la région de déploiement. 3. Dans le volet gauche, choisissez Automation et localisez le runbook Automation défaillant. 4. Ouvrez le runbook d'automatisation et vérifiez l'état d'exécution et les étapes d'exécution. 5. Examinez les détails de l'étape qui a échoué pour déterminer l'erreur ou l'échec exact.

Ressources connexes

- Simplifiez vos déploiements de haute disponibilité de Microsoft SQL Server à l'aide d'Amazon FSx pour Windows File Server
- Utilisation FSx d'un serveur de fichiers Windows avec Microsoft SQL Server

Utilisez les requêtes BMC Discovery pour extraire les données de migration afin de planifier la migration

Créée par Ben Taille-Hamblin (AWS), Simon Cunningham (AWS), Emma Baldry (AWS) et Shabnam Khan (AWS)

Récapitulatif

Ce guide fournit des exemples de requêtes et des étapes pour vous aider à extraire des données de votre infrastructure et de vos applications sur site à l'aide de BMC Discovery. Le modèle vous montre comment utiliser les requêtes BMC Discovery pour analyser votre infrastructure et extraire des informations sur les logiciels, les services et les dépendances. Les données extraites sont nécessaires pour les phases d'évaluation et de mobilisation d'une migration à grande échelle vers le cloud Amazon Web Services (AWS). Vous pouvez utiliser ces données pour prendre des décisions critiques concernant les applications à migrer ensemble dans le cadre de votre plan de migration.

Conditions préalables et limitations

Prérequis

- Une licence pour BMC Discovery (anciennement BMC ADDM) ou pour la version logicielle en tant que service (SaaS) de BMC Helix Discovery
- Version sur site ou SaaS de BMC Discovery, installée

> **Note**
>
> Pour les versions locales de BMC Discovery, vous devez installer l'application sur un réseau client avec accès à tous les périphériques réseau et serveurs concernés par une migration entre plusieurs centres de données. L'accès au réseau client doit être fourni conformément aux instructions d'installation de l'application. Si l'analyse des informations de Windows Server est requise, vous devez configurer un périphérique de gestion de proxy Windows sur le réseau.

- Accès au réseau pour permettre à l'application de scanner les appareils entre les centres de données, si vous utilisez BMC Helix Discovery

Versions du produit

- BMC Discovery 22.2 (12,5)

- BMC Discovery 22,1 (12,4)
- BMC Discovery 21,3 (12,3)
- BMC Discovery 21,05 (12,2)
- BMC Discovery 20,08 (12,1)
- BMC Discovery 20,02 (12,0)
- BMC Discovery 11.3
- BMC Discovery 11.2
- BMC Discovery 11.1
- BMC Discovery 11.0
- BMC Atrium Discovery 10.2
- BMC Atrium Discovery 10.1
- BMC Atrium Discovery 10.0

Architecture

Le schéma suivant montre comment les gestionnaires d'actifs peuvent utiliser les requêtes BMC Discovery pour analyser des applications modélisées par BMC dans des environnements SaaS et sur site.

Le diagramme illustre le flux de travail suivant : un gestionnaire d'actifs utilise BMC Discovery ou BMC Helix Discovery pour scanner les instances de base de données et de logiciels exécutées sur des serveurs virtuels hébergés sur plusieurs serveurs physiques. L'outil peut modéliser des applications avec des composants couvrant plusieurs serveurs virtuels et physiques.

Pile technologique

- BMC Discovery
- BMC Helix Discovery

Outils

- BMC Discovery est un outil de découverte de centres de données qui vous permet de découvrir automatiquement votre centre de données.

- BMC Helix Discovery est un système de découverte et de modélisation des dépendances basé sur le SaaS qui vous aide à modéliser dynamiquement vos actifs de données et leurs dépendances.

Bonnes pratiques

Il est recommandé de cartographier les données d'application, de dépendance et d'infrastructure lors de la migration vers le cloud. Le mappage vous aide à comprendre la complexité de votre environnement actuel et les dépendances entre les différents composants.

Les informations sur les actifs fournies par ces requêtes sont importantes pour plusieurs raisons :

1. Planification : la compréhension des dépendances entre les composants vous aide à planifier le processus de migration de manière plus efficace. Par exemple, il se peut que vous deviez d'abord migrer certains composants afin de garantir que d'autres puissent être migrés avec succès.
2. Évaluation des risques — La cartographie des dépendances entre les composants peut vous aider à identifier les risques ou problèmes potentiels pouvant survenir au cours du processus de migration. Par exemple, vous découvrirez peut-être que certains composants reposent sur des technologies obsolètes ou non prises en charge susceptibles de provoquer des problèmes dans le cloud.
3. Architecture cloud — La cartographie des données de votre application et de votre infrastructure peut également vous aider à concevoir une architecture cloud adaptée aux besoins de votre organisation. Par exemple, vous devrez peut-être concevoir une architecture multiniveau pour répondre aux exigences de haute disponibilité ou d'évolutivité.

Dans l'ensemble, le mappage des données relatives aux applications, aux dépendances et à l'infrastructure constitue une étape cruciale du processus de migration vers le cloud. L'exercice de cartographie peut vous aider à mieux comprendre votre environnement actuel, à identifier les problèmes ou risques potentiels et à concevoir une architecture cloud adaptée.

Épopées

Identifier et évaluer les outils de découverte

Tâche	Description	Compétences requises
Identifiez les propriétaires de l'ITSM.	Identifiez les responsables de la gestion des services	Responsable de la migration

Tâche	Description	Compétences requises
	informatiques (ITSM) (généralement en contactant les équipes de support opérationnel).	
Vérifiez CMDB.	Identifiez le nombre de bases de données de gestion de configuration (CMDBs) contenant des informations sur les actifs, puis identifiez les sources de ces informations.	Responsable de la migration
Identifiez les outils de découverte et vérifiez l'utilisation de BMC Discovery.	Si votre entreprise utilise BMC Discovery pour envoyer des données relatives à votre environnement à l'outil CMDB, vérifiez l'étendue et la couverture de ses analyses. Par exemple, vérifiez si BMC Discovery analyse tous les centres de données et si les serveurs d'accès sont situés dans des zones périmétriques.	Responsable de la migration
Vérifiez le niveau de modélisation des applications.	Vérifiez si les applications sont modélisées dans BMC Discovery. Si ce n'est pas le cas, recommandez l'utilisation de l'outil BMC Discovery pour modéliser les instances logicielles en cours d'exécution fournissant une application et un service métier.	Ingénieur en migration, responsable de la migration

Extraire les données d'infrastructure

Tâche	Description	Compétences requises
Extrayez les données sur des serveurs physiques et virtuels.	Pour extraire des données sur les serveurs physiques et virtuels analysés par BMC Discovery, utilisez Query Builder pour exécuter la requête suivante : `search Host show key as 'Serverid', virtual, name as 'HOSTNAME', os_type as 'osName', os_version as 'OS Version', num_logical_processors as 'Logical Processor Counts', cores_per_processor as 'Cores per Processor', logical_ram as 'Logical RAM', #Consumer:StorageUse:Provider:DiskDrive.size as 'Size'` **Note** Vous pouvez utiliser les données extraites pour déterminer les tailles d'instance appropriées pour la migration.	Ingénieur en migration, responsable de la migration
Extrayez des données sur des applications modélisées.	Si vos applications sont modélisées dans BMC	Propriétaire de l'application BMC Discovery

Tâche	Description	Compétences requises
	Discovery, vous pouvez extraire des données concernant les serveurs qui exécutent le logiciel d'application. Pour obtenir les noms des serveurs, utilisez le Générateur de requêtes pour exécuter la requête suivante : `search SoftwareInstance show key as 'ApplicationID', #RunningSoftware:HostedSoftware:Host:Host.key as 'ReferenceID', type, name` **Note** Les applications sont modélisées dans BMC Discovery par un ensemble d'instances logicielles en cours d'exécution. L'application dépend de tous les serveurs qui exécutent le logiciel d'application.	

Tâche	Description	Compétences requises
Extraire des données dans des bases de données.	Pour obtenir la liste de toutes les bases de données scannées et des serveurs sur lesquels ces bases de données sont exécutées , utilisez le Générateur de requêtes pour exécuter la requête suivante : `search Database show key as 'Key', name, type as 'Source Engine Type', #Detail:Detail:ElementWithDetail:SoftwareInstance.name as 'Software Instance', #Detail:Detail:ElementWithDetail:SoftwareInstance.product_version as 'Product Version', #Detail:Detail:ElementWithDetail:SoftwareInstance.edition as 'Edition', #Detail:Detail:ElementWithDetail:SoftwareInstance.#RunningSoftware:HostedSoftware:Host:Host.key as 'ServerID'`	Propriétaire de l'application

Tâche	Description	Compétences requises
Extrayez les données relatives à la communication avec le serveur.	Pour obtenir des informations sur toutes les communications réseau entre les serveurs collectées par BMC Discovery à partir des journaux de communications réseau historiques, utilisez Query Builder pour exécuter la requête suivante : `search Host TRAVERSE InferredElement:Inference:Associate:DiscoveryAccess TRAVERSE DiscoveryAccess:DiscoveryAccessResult:DiscoveryResult:NetworkConnectionList TRAVERSE List:List:Member:DiscoveredNetworkConnection PROCESS WITH networkConnectionInfo`	Propriétaire de l'application BMC Discovery

Tâche	Description	Compétences requises
Extrayez les données relatives à la découverte d'applications.	Pour obtenir des informations sur les dépendances des applications, utilisez le Générateur de requêtes pour exécuter la requête suivante : `search SoftwareInstance show key as 'SRC App ID', #Dependant:Dependency:DependedUpon:SoftwareInstance.key as 'DEST App ID'`	Propriétaire de l'application BMC Discovery
Extrayez des données sur les services aux entreprises.	Pour extraire des données sur les services commerciaux fournis par les hôtes, utilisez le Générateur de requêtes pour exécuter la requête suivante : `search Host show name, #Host:HostedSoftware:AggregateSoftware:BusinessService.name as 'Name'`	Propriétaire de l'application BMC Discovery

Résolution des problèmes

Problème	Solution
Une requête ne s'exécute pas ou contient des colonnes non remplies.	Passez en revue les enregistrements des actifs dans BMC Discovery et déterminez les champs dont vous avez besoin. Remplacez ensuite ces champs dans la requête à l'aide du Générateur de requêtes.

Problème	Solution
Les détails d'un actif dépendant ne sont pas renseignés.	Cela est probablement dû aux autorisations d'accès ou à la connectivité réseau. L'outil de découverte peut ne pas disposer des autorisations nécessaires pour accéder à certains actifs, en particulier s'ils se trouvent sur différents réseaux ou dans différents environnements. Nous vous recommandons de travailler en étroite collaboration avec des experts en matière de découverte afin de vous assurer que tous les actifs pertinents sont identifiés.

Ressources connexes

Références

- Droits de licence BMC Discovery (documentation BMC)
- Fonctionnalités et composants de BMC Discovery (documentation BMC)
- Guide de l'utilisateur de BMC Discovery (documentation BMC)
- Recherche de données (sur BMC Discovery) (documentation BMC)
- Découverte et analyse du portefeuille pour la migration (AWS Prescriptive Guidance)

Tutoriels et vidéos

- BMC Discovery : Webinaire - Meilleures pratiques en matière de requêtes de reporting (partie 1) (YouTube)

Déménager

Rubriques

- Migrer une base de données Amazon RDS for Oracle vers Compte AWS une autre Région AWS et AWS DMS l'utiliser pour une réplication continue
- Migrer VMware le SDDC vers le VMware cloud sur AWS à l'aide de HCX VMware
- Migrer une instance de base de données Amazon RDS vers un autre VPC ou un autre compte
- Migrer une instance de base de données Amazon RDS pour Oracle vers un autre VPC
- Migrer un cluster Amazon Redshift vers une région AWS en Chine
- Transportez des bases de données PostgreSQL entre deux instances de base de données Amazon RDS à l'aide de pg_transport

Migrer une base de données Amazon RDS for Oracle vers Compte AWS une autre Région AWS et AWS DMS l'utiliser pour une réplication continue

Créée par Durga Prasad Cheepuri (AWS) et Eduardo Valentim (AWS)

Récapitulatif

> **Warning**
>
> Les utilisateurs IAM disposent d’informations d’identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu’elles ne sont plus nécessaires.

Ce modèle explique les étapes de migration d'une base de données source Amazon Relational Database Service (Amazon RDS) pour Oracle vers un autre et. Compte AWS Région AWS Le modèle utilise un instantané de base de données pour un chargement complet de données unique et active AWS Database Migration Service (AWS DMS) pour une réplication continue.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS contenant la base de données source Amazon RDS for Oracle, qui a été chiffrée à l'aide d'une clé autre que AWS Key Management Service default (AWS KMS)
- Un actif Compte AWS dans une base de données Région AWS différente de la base de données source, à utiliser pour la base de données Amazon RDS for Oracle cible
- Cloud privé virtuel (VPC) reliant la source à la cible VPCs
- Connaissance de l'utilisation d'une base de données Oracle comme source pour AWS DMS
- Connaissance de l'utilisation d'une base de données Oracle comme cible pour AWS DMS

Versions du produit

- Versions Oracle 11g (versions 11.2.0.3.v1 et ultérieures) et jusqu'à 12.2, et 18c. Pour obtenir la dernière liste des versions et éditions prises en charge, consultez les sections Utilisation d'une

base de données Oracle comme source AWS DMS et Utilisation d'une base de données Oracle comme cible AWS DMS dans la AWS documentation. Pour les versions d'Oracle prises en charge par Amazon RDS, consultez Oracle sur Amazon RDS.

Architecture

Stacks technologiques sources et cibles

- Instance de base de données Amazon RDS pour Oracle

Architecture de réplication continue

Outils

Outils utilisés pour le chargement complet des données en une seule fois

- Amazon Relational Database Service (Amazon RDS) crée un instantané du volume de stockage de votre instance de base de données, en sauvegardant l'intégralité de l'instance de base de données et pas uniquement les bases de données individuelles. Lorsque vous créez un snapshot DB, vous devez identifier quelle instance de base de données vous allez sauvegarder, puis nommer votre snapshot DB afin de pouvoir effectuer une restauration à partir de ce dernier ultérieurement. Le temps nécessaire à la création d'un instantané varie en fonction de la taille de vos bases de données. Étant donné que l'instantané inclut l'intégralité du volume de stockage, la taille des fichiers, comme les fichiers temporaires, a également une incidence sur le temps nécessaire à la création de l'instantané. Pour plus d'informations sur l'utilisation des instantanés de base de données, consultez la section Création d'un instantané de base de données dans la documentation Amazon RDS.
- AWS Key Management Service (AWS KMS) crée une clé pour le chiffrement Amazon RDS. Lorsque vous créez une instance de base de données chiffrée, vous pouvez également fournir l'identifiant de AWS KMSclé de votre clé de chiffrement. Si vous ne spécifiez aucun identifiant de AWS KMSclé, Amazon RDS utilise votre clé de chiffrement par défaut pour votre nouvelle instance de base de données. AWS KMScrée votre clé de chiffrement par défaut pour votre Compte AWS. Vous disposez Compte AWS d'une clé de chiffrement par défaut différente pour chacune d'entre elles Région AWS. Pour ce modèle, l'instance de base de données Amazon RDS doit être chiffrée à l'aide d'une clé autre que celle par défaut AWS KMS. Pour plus d'informations sur l'utilisation

des AWS KMSclés pour le chiffrement Amazon RDS, consultez la section Chiffrer les ressources Amazon RDS dans la documentation Amazon RDS.

Outils utilisés pour la réplication continue

- AWS Database Migration Service (AWS DMS) est utilisé pour répliquer les modifications en cours et pour synchroniser les bases de données source et cible. Pour plus d'informations sur l'utilisation AWS DMS pour une réplication continue, consultez la section Utilisation d'une instance de AWS DMS réplication dans la AWS DMS documentation.

Épopées

Configurez votre source Compte AWS

Tâche	Description	Compétences requises
Préparez l'instance de base de données Oracle source.	Laissez l'instance de base de données Amazon RDS for Oracle s'exécuter en mode ARCHIVELOG et définissez la période de rétention. Pour plus de détails, voir Utilisation d'une base de données Oracle AWS gérée en tant que source pour AWS DMS.	DBA
Définissez une journalisation supplémentaire pour l'instanc e de base de données Oracle source.	Définissez une journalisation supplémentaire au niveau de la base de données et au niveau de la table pour l'instance de base de données Amazon RDS for Oracle. Pour plus de détails, voir Utilisation d'une base de données Oracle AWS gérée en tant que source pour AWS DMS.	DBA

Tâche	Description	Compétences requises
Mettez à jour la politique AWS KMS clé dans le compte source.	Mettez à jour la politique AWS KMS clé dans la source Compte AWS pour permettre à la cible Compte AWS d'utiliser la AWS KMS clé Amazon RDS cryptée. Pour plus de détails, consultez la AWS KMS documentation.	SysAdmin
Créez un instantané manuel de base de données Amazon RDS de l'instance de base de données source.		Utilisateur AWS IAM
Partagez l'instantané Amazon RDS chiffré manuel avec la cible Compte AWS.	Pour plus de détails, consultez la section Partage d'un instantané de base de données.	Utilisateur AWS IAM

Configurez votre cible Compte AWS

Tâche	Description	Compétences requises
Joignez une politique.	Dans la cible Compte AWS, attachez une politique AWS Identity and Access Management (IAM) à l'utilisateur IAM racine, afin de lui permettre de copier un instantané de base de données chiffré à l'aide de la clé partagée. AWS KMS	SysAdmin

Tâche	Description	Compétences requises
Passez à la source Région AWS.		Utilisateur AWS IAM
Copiez le cliché partagé.	Dans la console Amazon RDS, dans le volet Snapshots , choisissez Shared with Me, puis sélectionnez l'instantané partagé. Copiez l'instantané sur le même emplacement Région AWS que la base de données source en utilisant le Amazon Resource Name (ARN) pour la AWS KMS clé utilisée par la base de données source. Pour plus de détails, consultez la section Copier un instantané de base de données.	Utilisateur AWS IAM
Passez à la cible Région AWS et créez une nouvelle AWS KMS clé.		Utilisateur AWS IAM
Copiez le cliché.	Passez à la source Région AWS. Sur la console Amazon RDS, dans le volet Snapshots , choisissez Owned by Me, puis sélectionnez l'instant ané copié. Copiez le cliché sur la cible Région AWS en utilisant la AWS KMS clé de la nouvelle cible Région AWS.	Utilisateur AWS IAM

Tâche	Description	Compétences requises
Restaurez l'instantané.	Passez à la cible Région AWS. Sur la console Amazon RDS, dans le volet Snapshots , choisissez Owned by Me. Sélectionnez le snapshot copié et restaurez-le sur une instance de base de données Amazon RDS for Oracle. Pour plus de détails, consultez la section Restauration à partir d'un instantané de base de données.	Utilisateur AWS IAM

Préparez votre base de données source pour une réplication continue

Tâche	Description	Compétences requises
Créez un utilisateur Oracle doté des autorisations appropriées.	Créez un utilisateur Oracle doté des privilèges requis pour Oracle en tant que source pour AWS DMS. Pour plus de détails, consultez la AWS DMS documentation.	DBA
Configurez la base de données source pour Oracle LogMiner ou Oracle Binary Reader.		DBA

Préparez votre base de données cible pour une réplication continue

Tâche	Description	Compétences requises
Créez un utilisateur Oracle doté des autorisations appropriées.	Créez un utilisateur Oracle doté des privilèges requis pour Oracle en tant que cible pour AWS DMS. Pour plus de détails, consultez la AWS DMS documentation.	DBA

Création de AWS DMS composants

Tâche	Description	Compétences requises
Créez une instance de réplication dans la cible Région AWS.	Créez une instance de réplication dans le VPC de la cible. Région AWS Pour plus de détails, consultez la AWS DMS documentation.	Utilisateur AWS IAM
Créez des points de terminais on source et cible avec le chiffrement requis et testez les connexions.	Pour plus de détails, consultez la AWS DMS documentation.	DBA
Créez des tâches de réplicati on.	1. Pour le type de migration , choisissez la réplication continue. 2. Pour le point de départ de la capture des données de modification (CDC), utilisez le numéro de modification du système Oracle (SCN) lorsque le snapshot Amazon RDS a été pris pour le chargemen	Utilisateur IAM

Tâche	Description	Compétences requises
	t complet, ou l'horodatage lorsque le chargement complet a été effectué. 3. Pour`TargetTablePrepMode`, choisissez DO_NOTHING. Si la tâche comporte de grandes tables de données d'objets binaires (LOB), choisissez le mode LOB limité et définissez la taille LOB maximale sur la taille maximale des données LOB de la table. 4. Activez la journalisation 5. Regroupez les tables liées par des clés en une seule tâche. Si certaines tables contiennent une grande quantité de données LOB et que la table n'a aucune relation avec les autres tables, créez-lui une tâche distincte avec les paramètres LOB décrits précédemment. Pour plus de détails, consultez la AWS DMS documentation.	
Démarrez les tâches et surveillez-les.	Pour plus de détails, consultez la AWS DMS documentation.	Utilisateur AWS IAM

Tâche	Description	Compétences requises
Activez la validation de la tâche si nécessaire.	Notez que l'activation de la validation a un impact sur les performances de la réplication. Pour plus de détails, consultez la AWS DMS documentation.	Utilisateur AWS IAM

Ressources connexes

- Modification d'une politique clé
- Création d'un instantané manuel de base de données Amazon RDS
- Partage d'un instantané manuel de base de données Amazon RDS
- Copier un instantané
- Restauration à partir d'un instantané de base de données Amazon RDS
- Commencer avec AWS DMS
- Utilisation d'une base de données Oracle comme source pour AWS DMS
- Utilisation d'une base de données Oracle comme cible pour AWS DMS
- AWS DMS configuration à l'aide du peering VPC
- Comment partager des instantanés de base de données Amazon RDS manuels ou des instantanés de cluster de bases de données avec une autre personne ? Compte AWS (article du centre de connaissances AWS)

Migrer VMware le SDDC vers le VMware cloud sur AWS à l'aide de HCX VMware

Créée par Deepak Kumar (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

Ce modèle décrit l'utilisation de l'extension VMware Hybrid Cloud (HCX) pour migrer vos machines virtuelles sur site (VMs) et vos applications vers le VMware cloud sur Amazon Web Services (AWS). La migration utilise un logiciel de centre VMware de données défini par logiciel (SDDC) d'entreprise sur le cloud AWS pour fournir un accès optimisé aux services AWS.

VMware Cloud on AWS intègre des produits de calcul, de stockage et de virtualisation du réseau (vSphere, vSAN et VMware NSX) à la gestion des serveurs VMware vCenter, qui est optimisée pour fonctionner sur une infrastructure AWS dédiée, élastique et bare metal. L'infrastructure qui en résulte nécessite peu de maintenance, est simplifiée et hyperconvergée.

Grâce à ce service, les équipes informatiques peuvent gérer leurs ressources basées sur le cloud à l'aide VMware d'outils familiers. Pour plus d'informations, consultez VMware Cloud on AWS sur le VMware site Web.

VMware HCX prend en charge trois types de migrations vers le cloud :

- Hybridité (extension du centre de données) : extension d'un VMware SDDC sur site existant à AWS afin de fournir une extension de l'encombrement, une capacité à la demande, un environnement de test/développement et des bureaux virtuels.
- Évacuation du cloud (actualisation de l'infrastructure à l'échelle du centre de données) : consolidation des centres de données et migration complète vers le cloud AWS (y compris la gestion de la colocation des centres de données ou de la fin du bail).
- Migration spécifique aux applications : migration d'applications individuelles vers le cloud AWS pour répondre à des besoins commerciaux spécifiques.

Conditions préalables et limitations

Prérequis

- Ouvrez un compte AWS (obligatoire pour la création d'un SDDC VMware dans le cloud).
- Ouvrez un VMware compte Mon compte. Inscrivez-vous sur https://my.vmware.com/web/vmware/ et remplissez tous les champs.
- Vérifiez la version de vCenter et des hôtes, puis collectez le nombre de. VMs Si possible, demandez une RVToolsexportation pour afficher des informations sur vos environnements virtuels. Nous recommandons la version 6.0 ou ultérieure de vCenter.
- Vous devez déployer des commutateurs virtuels distribués si vous souhaitez étendre les réseaux de centres de données (L2), tester vMotion à l'aide de HCX ou analyser la dépendance des applications à l'aide de vRealize Network Insight.
- Choisissez un réseau de sous-réseau de gestion actuel sur site non conflictuel pour créer le SDDC on Cloud on AWS. VMware
- Validez les exigences du HCX en consultant les prérequis fournis dans le guide de l'utilisateur du VMware HCX.
- Identifiez et regroupez VMs en fonction des vagues de migration. Vérifiez VMs que vous pouvez l'utiliser pour les tests.
- Collectez toutes les données relatives à la consommation de bande passante, à la compression WAN et à la vitesse de transfert des données.

Remarques

- Pas besoin de VMware NSX-V ou NSX-T sur site.
- Aucun coût supplémentaire pour HCX (il est inclus dans VMware Cloud on AWS).

Architecture

Le schéma suivant montre la solution HCX basée sur des services à composants multiples. Chaque composant prend en charge une fonction spécifique dans la solution HCX. Pour plus d'informations sur chaque composant HCX, consultez le billet de blog Migration des charges de travail vers le cloud VMware sur AWS avec Hybrid Cloud Extension (HCX).

Pile technologique source

- Sur site VMs et applications gérées par vSphere VMware

Pile technologique cible

- VMware Cloud sur AWS

Outils

- VMware HCX — VMware HCX est un outil que vous pouvez utiliser pour migrer vos applications et charges de travail entre des centres de données et des environnements cloud. Il est inclus dans VMware Cloud on AWS.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Choisissez une stratégie de migration.	Décidez si vous souhaitez étendre votre centre de données (hybridité), déplacer tous vos centres de données (évacuation du cloud) ou transférer des applications spécifiques vers AWS.	SysAdmin, propriétaire de l'application
Validez les exigences HCX.	Pour obtenir des informations sur la migration, consultez le guide de l'utilisateur VMware HCX.	SysAdmin, propriétaire de l'application

Migrer vers VMware le cloud sur AWS

Tâche	Description	Compétences requises
Migrez vos VMs applications informatiques.	Pour plus d'informations, consultez la section Migration hybride avec VMware HCX	SysAdmin, propriétaire de l'application

Tâche	Description	Compétences requises
	dans la VMware documentation.	

Ressources connexes

- VMware Cloud sur AWS : mise en route
- Migration hybride avec VMware HCX
- VMware Guide de l'utilisateur HCX
- VMware Tarification du cloud sur AWS
- VMware Feuille de route pour le cloud sur AWS

Migrer une instance de base de données Amazon RDS vers un autre VPC ou un autre compte

Créée par Dhrubajyoti Mukherjee (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une instance de base de données Amazon Relational Database Service (Amazon RDS) d'un cloud privé virtuel (VPC) vers un autre dans le même compte AWS, ou d'un compte AWS vers un autre compte AWS.

Ce modèle est utile si vous souhaitez migrer vos instances de base de données Amazon RDS vers un autre VPC ou un autre compte pour des raisons de séparation ou de sécurité (par exemple, lorsque vous souhaitez placer votre pile d'applications et votre base de données dans VPCs un autre emplacement).

La migration d'une instance de base de données vers un autre compte AWS implique des étapes telles que la prise d'un instantané manuel, son partage et sa restauration sur le compte cible. Ce processus peut prendre beaucoup de temps, en fonction des modifications apportées à la base de données et des taux de transactions. Cela entraîne également des interruptions de service de la base de données. Planifiez donc la migration à l'avance. Envisagez une stratégie de déploiement bleu/vert pour minimiser les temps d'arrêt. Vous pouvez également évaluer AWS Data Migration Service (AWS DMS) afin de minimiser les temps d'arrêt liés au changement. Toutefois, ce modèle ne couvre pas cette option. Pour en savoir plus, consultez la documentation AWS DMS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorisations AWS Identity and Access Management (IAM) requises pour le VPC, les sous-réseaux et la console Amazon RDS

Limites

- Les modifications apportées à un VPC entraînent le redémarrage de la base de données, ce qui entraîne des interruptions d'application. Nous vous recommandons de migrer pendant les périodes de pointe peu élevées.
- Limitations lors de la migration d'Amazon RDS vers un autre VPC :

  - L'instance de base de données que vous migrez doit être une instance unique sans veille. Il ne doit pas être membre d'un cluster.
  - Amazon RDS ne doit pas se trouver dans plusieurs zones de disponibilité.
  - Amazon RDS ne doit pas disposer de répliques de lecture.
  - Le groupe de sous-réseaux créé dans le VPC cible doit comporter des sous-réseaux provenant de la zone de disponibilité où s'exécute la base de données source.
- Limitations lors de la migration d'Amazon RDS vers un autre compte AWS :
  - Le partage d'instantanés chiffrés avec la clé de service par défaut pour Amazon RDS n'est actuellement pas pris en charge.

Architecture

Migration vers un VPC dans le même compte AWS

Le schéma suivant montre le flux de travail de migration d'une instance de base de données Amazon RDS vers un autre VPC dans le même compte AWS.

Les étapes sont les suivantes. Consultez la section Epics pour obtenir des instructions détaillées.

1. Créez un groupe de sous-réseaux de base de données dans le VPC cible. Un groupe de sous-réseaux de base de données est un ensemble de sous-réseaux que vous pouvez utiliser pour spécifier un VPC spécifique lorsque vous créez des instances de base de données.
2. Configurez l'instance de base de données Amazon RDS dans le VPC source pour utiliser le nouveau groupe de sous-réseaux de base de données.
3. Appliquez les modifications pour migrer la base de données Amazon RDS vers le VPC cible.

Migration vers un autre compte AWS

Le schéma suivant montre le flux de travail de migration d'une instance de base de données Amazon RDS vers un autre compte AWS.

Les étapes sont les suivantes. Consultez la section Epics pour obtenir des instructions détaillées.

1. Accédez à l'instance de base de données Amazon RDS dans le compte AWS source.
2. Créez un instantané Amazon RDS dans le compte AWS source.

3. Partagez l'instantané Amazon RDS avec le compte AWS cible.
4. Accédez à l'instantané Amazon RDS dans le compte AWS cible.
5. Créez une instance de base de données Amazon RDS dans le compte AWS cible.

Outils

Services AWS

- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Bonnes pratiques

- Si l'indisponibilité de la base de données est un problème lors de la migration d'une instance de base de données Amazon RDS vers un autre compte, nous vous recommandons d'utiliser AWS DMS. Ce service assure la réplication des données, ce qui entraîne une interruption de service de moins de cinq minutes.

Épopées

Migrer vers un autre VPC dans le même compte AWS

Tâche	Description	Compétences requises
Créez un nouveau VPC.	Sur la console Amazon VPC, créez un nouveau VPC et des sous-réseaux avec les propriétés et les plages d'adresses IP souhaitées. Pour obtenir des instructi ons détaillées, consultez la documentation Amazon VPC.	Administrateur

Tâche	Description	Compétences requises
Créez un groupe de sous-réseaux de base de données.	Sur la console Amazon RDS : 1. Choisissez Groupes de sous-réseaux, puis Créer un groupe de sous-réseaux de base de données. 2. Entrez le nom, la description et l'ID du VPC du groupe de sous-réseaux. 3. Ajoutez les sous-réseaux qui appartiennent au groupe de sous-réseaux. Ajoutez des sous-réseaux pour couvrir au moins deux zones de disponibilité. 4. Choisissez Créer. Pour plus d'informations, consultez la documentation Amazon RDS.	Administrateur

Tâche	Description	Compétences requises
Modifiez l'instance de base de données Amazon RDS pour utiliser le nouveau groupe de sous-réseaux.	Sur la console Amazon RDS : 1. Dans le volet de navigation, choisissez Databases, puis choisissez l'instance de base de données Amazon RDS à migrer. 2. Dans la section Connectivité, choisissez le groupe de sous-réseaux associé au VPC cible. 3. Dans la section Modifications du calendrier, choisissez Appliquer immédiatement. Lorsque la migration vers le VPC cible est terminée, le groupe de sécurité par défaut du VPC cible est attribué à l'instance de base de données Amazon RDS. Vous pouvez configurer un nouveau groupe de sécurité pour ce VPC avec les règles entrantes et sortantes requises pour votre instance de base de données. Vous pouvez également utiliser l'interface de ligne de commande AWS (AWS CLI) pour effectuer la migration vers le VPC cible en fournissant explicitement le nouvel ID	Administrateur

Tâche	Description	Compétences requises
	de groupe de sécurité VPC. Par exemple : `aws rds modify-db-instance \ --db-instance-identifier testrds \ --db-subnet-group-name new-vpc-subnet-group \ --vpc-security-group-ids sg-idxxxx \ --apply-immediately`	

Migrer vers un autre compte AWS

Tâche	Description	Compétences requises
Créez un nouveau VPC et un nouveau groupe de sous-réseaux dans le compte AWS cible.	1. Sur la console Amazon VPC, créez un nouveau VPC avec les propriétés et les plages d'adresses IP souhaitées. Pour obtenir des instructions détaillées, consultez la documentation Amazon VPC. 2. Créez des sous-réseaux pour le nouveau VPC en suivant les instructions de la documentation Amazon VPC. 3. Sur la console Amazon RDS, créez des groupes de sous-réseaux de base	Administrateur

Tâche	Description	Compétences requises
	de données. Pour obtenir des instructions, consultez la documentation Amazon RDS.	
Partagez un instantané manuel de la base de données et partagez-le avec le compte cible.	1. Prenez un instantané manuel de la base de données source en suivant les instructions de la documentation Amazon RDS. 2. Partagez l'instantané avec le compte AWS cible en fournissant l'ID du compte cible. Pour obtenir des instructions, consultez l'article Re:Post sur le partage d'instantanés de base de données avec d'autres comptes.	Administrateur
Lancez une nouvelle instance de base de données Amazon RDS.	Lancez une nouvelle instance de base de données Amazon RDS à partir de l'instantané partagé dans le compte AWS cible. Pour obtenir des instructions, consultez la documentation Amazon RDS.	Administrateur

Ressources connexes

- Documentation Amazon VPC
- Documentation Amazon RDS
- Comment modifier le VPC d'une instance de base de données RDS ? (AWS Re:Publier un article)

- Comment transférer la propriété des ressources Amazon RDS vers un autre compte AWS ? (AWS Re:Publier un article)
- Comment partager des instantanés de base de données Amazon RDS manuels ou des instantanés de cluster de bases de données Aurora avec un autre compte AWS ? (AWS Re:Publier un article)
- Documentation AWS DMS

Migrer une instance de base de données Amazon RDS pour Oracle vers un autre VPC

Créée par Pinesh Singal (AWS)

Récapitulatif

Ce modèle de migration fournit des step-by-step conseils pour migrer une instance de base de données (DB) Amazon Relational Database Service (Amazon RDS) pour Oracle d'un cloud privé virtuel (VPC) vers un autre VPC dans le même compte Amazon Web Services (AWS). Par exemple, vous pouvez utiliser ce modèle si votre entreprise exige que la base de données et le serveur d'applications Amazon Elastic Compute Cloud (Amazon EC2) se trouvent dans le même VPC.

Le schéma décrit une stratégie de migration en ligne avec pratiquement aucun temps d'arrêt pour une base de données source Oracle de plusieurs téraoctets comportant un grand nombre de transactions.

Pour déplacer une instance de base de données Amazon RDS pour Oracle vers un autre VPC, vous devez modifier le groupe de sous-réseaux Amazon RDS. Ce groupe de sous-réseaux doit être préconfiguré avec le nouveau VPC et les sous-réseaux requis. Pendant le passage du VPC d'un réseau à un autre, l'instance Amazon RDS redémarre, de sorte que la base de données ne sera pas accessible pendant le transfert.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Deux VPCs avec des sous-réseaux privés
- Une instance de base de données Amazon RDS pour Oracle (opérationnelle), configurée avec des groupes de sécurité entrants et sortants

Limites

- Une instance de base de données qui couvre plusieurs zones de disponibilité (multi-AZ) n'est pas prise en charge. Ce modèle permet toutefois de contourner cette limitation.
- L'instance de base de données ne peut pas être migrée lorsqu'une réplique en lecture est activée.
- Le groupe de sous-réseaux du nouveau VPC doit se trouver dans la même zone de disponibilité que la base de données.

- La migration doit avoir lieu pendant la période de maintenance planifiée ou pendant les périodes de faible trafic, car le déplacement de la base de données vers un autre VPC entraîne le redémarrage de la base de données, ce qui entraîne des interruptions d'application pendant quelques minutes.

Versions du produit

- Instance de base de données Amazon RDS for Oracle, 12.1.0.2 et versions ultérieures

Architecture

Pile technologique source

- Une instance de base de données Amazon RDS for Oracle 12.1.0.2.v22 dans un VPC
- Un VPC configuré dans une table de routage séparée
- Groupes de sous-réseaux Amazon RDS configurés dans un VPC
- Groupes d'options Amazon RDS (si nécessaire)

Pile technologique cible

- Instance de base de données Amazon RDS for Oracle avec version 12.1.0.2.v22 dans un autre VPC
- Amazon VPC configuré sur une route séparée
- Groupes de sous-réseaux Amazon RDS configurés dans le nouveau VPC
- Groupes d'options Amazon RDS (si nécessaire)

Architecture source et cible

Le schéma suivant montre comment utiliser la console pour déplacer la base de données Amazon RDS for Oracle d'un sous-réseau privé d'un VPC vers un sous-réseau privé d'un autre VPC.

1. Utilisez la console pour modifier l'instance de base de données Amazon RDS for Oracle source.
2. Dans le VPC cible, modifiez le groupe de sous-réseaux et modifiez le groupe d'options s'il est utilisé.

Outils

- Amazon RDS — Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud AWS. Il fournit une capacité redimensionnable et rentable pour une base de données relationnelle et gère les tâches d'administration de base de données courantes. Ce modèle utilise Amazon RDS for Oracle.

Épopées

Modifier la configuration de la base de données Amazon RDS for Oracle dans le VPC existant

Tâche	Description	Compétences requises
Créez un groupe de sous-réseaux.	Configurez un groupe de sous-réseaux dans Amazon RDS.	AWS général
Créez un groupe d'options.	(Facultatif) Configurez un groupe d'options dans Amazon RDS.	AWS général
Modifiez l'instance de base de données Amazon RDS for Oracle.	Modifiez la base de données avec le groupe de sous-réseaux et le groupe d'options.	AWS, DBA en général
Mettez à jour la base de données Oracle, si nécessaire.	Pour migrer la base de données source Amazon RDS for Oracle, apportez les modifications suivantes : • Supprimez les répliques lues, si elles existent. • Désactivez la fonction Multi-AZ, si elle est activée.	AWS général

Configuration de la base de données Amazon RDS for Oracle dans le VPC cible

Tâche	Description	Compétences requises
Créez un groupe de sous-réseaux.	Dans Amazon RDS, configurez un groupe de sous-réseaux à l'aide du sous-réseau du nouveau VPC et de la zone de disponibilité de la base de données.	AWS général
Créez un groupe d'options.	(Facultatif) Configurez un groupe d'options dans Amazon RDS.	AWS général
Modifiez la base de données Amazon RDS for Oracle.	Modifiez la base de données avec le nouveau groupe de sous-réseaux et le nouveau groupe d'options du nouveau VPC. Vous pouvez appliquer ces modifications immédiatement ou dans une fenêtre de maintenance. La modification peut prendre plusieurs minutes. Au cours de la modification, vous verrez les changements de statut suivants : • moving-to-vpc • C onfiguring-enhanced-monitoring • Modification • Disponible	AWS, DBA en général

Tâche	Description	Compétences requises
	La modification associera le groupe de sécurité par défaut du nouveau VPC. Associez un nouveau groupe de sécurité selon les besoins d'Amazon RDS for Oracle.	
Mettez à jour la base de données Amazon RDS for Oracle, si nécessaire.	Après avoir migré vers la base de données Amazon RDS for Oracle cible dans le nouveau VPC, apportez les modificat ions suivantes, si nécessaire : • Activez les répliques de lecture, si elles existent dans la base de données source. • Activez la fonctionnalité Multi-AZ, si elle était activée dans la base de données source.	AWS général
Testez la connectivité des applications.	Effectuez un test de connectiv ité de base de données depuis n'importe quelle applicati on. Vérifiez que la base de données Amazon RDS for Oracle modifiée dans le nouveau VPC est connectée et est accessible depuis l'application.	Propriétaire de l'application

Ressources connexes

- Documentation Amazon VPC

- VPCs et sous-réseaux
- Utilisation d'une instance de base de données dans un VPC
- Documentation Amazon RDS
- Oracle sur Amazon RDS
- Console Amazon RDS
- Comment puis-je remplacer le VPC par une instance de base de données Amazon RDS ?

Migrer un cluster Amazon Redshift vers une région AWS en Chine

Créée par Jing Yan (AWS)

Récapitulatif

Ce modèle fournit une step-by-step approche pour migrer un cluster Amazon Redshift vers une région AWS en Chine depuis une autre région AWS.

Ce modèle utilise des commandes SQL pour recréer tous les objets de base de données, et utilise la commande UNLOAD pour déplacer ces données d'Amazon Redshift vers un bucket Amazon Simple Storage Service (Amazon S3) dans la région source. Les données sont ensuite migrées vers un compartiment S3 dans la région AWS en Chine. La commande COPY est utilisée pour charger des données depuis le compartiment S3 et les transférer vers le cluster Amazon Redshift cible.

Amazon Redshift ne prend actuellement pas en charge les fonctionnalités interrégionales telles que la copie d'instantanés vers les régions AWS en Chine. Ce modèle fournit un moyen de contourner cette limitation. Vous pouvez également inverser les étapes de ce modèle pour migrer des données d'une région AWS en Chine vers une autre région AWS.

Conditions préalables et limitations

Prérequis

- Comptes AWS actifs à la fois dans une région chinoise et dans une région AWS hors de Chine
- Clusters Amazon Redshift existants dans une région chinoise et une région AWS en dehors de la Chine

Limites

- Il s'agit d'une migration hors ligne, ce qui signifie que le cluster Amazon Redshift source ne peut pas effectuer d'opérations d'écriture pendant la migration.

Architecture

Pile technologique source

- Cluster Amazon Redshift dans une région AWS en dehors de la Chine

Pile technologique cible

- Cluster Amazon Redshift dans une région AWS en Chine

Architecture cible

Outils

Outils

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre évolutivité, disponibilité des données, sécurité et performances. Vous pouvez utiliser Amazon S3 pour stocker les données d'Amazon Redshift, et vous pouvez copier les données d'un compartiment S3 vers Amazon Redshift.
- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données entièrement géré de plusieurs pétaoctets dans le cloud.
- psql — psql est une interface basée sur un terminal pour PostgreSQL.

Épopées

Préparation à la migration dans la région source

Tâche	Description	Compétences requises
Lancez et configurez une EC2 instance dans la région source.	Connectez-vous à l'AWS Management Console et ouvrez la console Amazon Elastic Compute Cloud (Amazon EC2). Votre région actuelle est affichée dans la barre de navigation en haut de l'écran. Cette région ne peut pas être une région AWS en Chine. Dans le tableau de bord de la EC2 console Amazon, choisisse z « Launch instance », puis créez et configurez une EC2	DBA, Développeur

Tâche	Description	Compétences requises
	instance. Important : Assurez-vous que vos groupes EC2 de sécurité pour les règles entrantes autorisent un accès illimité au port TCP 22 depuis votre machine source. Pour obtenir des instructions sur le lancement et la configuration d'une EC2 instance, consultez la section « Ressources associées ».	
Installez l'outil psql.	Téléchargez et installez PostgreSQL. Amazon Redshift ne fournit pas l'outil psql, il est installé avec PostgreSQL. Pour plus d'informations sur l'utilisation de psql et l'installation des outils PostgreSQL, consultez la section « Ressources associées ».	DBA

Tâche	Description	Compétences requises
Enregistrez les détails du cluster Amazon Redshift.	Ouvrez la console Amazon Redshift et choisissez « Clusters » dans le volet de navigation. Choisissez ensuite le nom du cluster Amazon Redshift dans la liste. Dans l'onglet « Propriétés », dans la section « Configurations de base de données », enregistrez le « Nom de la base de données » et le « Port ». Ouvrez la section « Détails de la connexion » et enregistrez le « point de terminaison », au <port><databasename>format « point de terminaison :/». Important : assurez-vous que vos groupes de sécurité Amazon Redshift pour les règles entrantes autorisent un accès illimité au port TCP 5439 depuis votre instance. EC2	DBA

Tâche	Description	Compétences requises
Connectez psql au cluster Amazon Redshift.	<databasename><por t>À l'invite de commande, spécifiez les informations de connexion en exécutant la commande « psql -h <endpoint>-U <userid>-d - p ». À l'invite de mot de passe psql, entrez le mot de passe de l'<userid>utilisateur « ». Vous êtes ensuite connecté au cluster Amazon Redshift et pouvez saisir des commandes de manière interactive.	DBA
Créez un compartiment S3.	Ouvrez la console Amazon S3 et créez un compartim ent S3 pour contenir les fichiers exportés depuis Amazon Redshift. Pour obtenir des instructions sur la création d'un compartim ent S3, consultez la section « Ressources associées ».	Administrateur de bases de données, AWS en général

Tâche	Description	Compétences requises
Créez une politique IAM qui prend en charge le déchargement des données.	Ouvrez la console AWS Identity and Access Management (IAM) et choisissez « Policies ». Choisissez « Créer une politique », puis choisissez l'onglet « JSON ». Copiez et collez la politique IAM pour le déchargement des données depuis la section « Informations supplémentaires ». Important : remplacez « s3_bucket_name » par le nom de votre compartiment S3. Choisissez « Réviser la politique », puis entrez le nom et la description de la politique. Choisissez « Créer une politique ».	DBA

Tâche	Description	Compétences requises
Créez un rôle IAM pour autoriser l'opération UNLOAD pour Amazon Redshift.	Ouvrez la console IAM et choisissez « Rôles ». Choisissez « Créer un rôle », puis « Service AWS » dans « Sélectionner le type d'entité de confiance ». Choisissez « Redshift » pour le service, choisisse z « Redshift — Personnal isable », puis « Suivant ». Choisissez la politique de « Déchargement » que vous avez créée précédemment, puis choisissez « Suivant ». Entrez un « Nom du rôle », puis choisissez « Créer un rôle ».	DBA
Associez le rôle IAM au cluster Amazon Redshift.	Ouvrez la console Amazon Redshift et choisissez « Gérer les rôles IAM ». Choisissez « Rôles disponibles » dans le menu déroulant et choisisse z le rôle que vous avez créé précédemment. Choisisse z « Appliquer les modificat ions ». Lorsque le « statut » du rôle IAM dans la section « Gérer les rôles IAM » indique « Synchronisé », vous pouvez exécuter la commande UNLOAD.	DBA

Tâche	Description	Compétences requises
Arrêtez les opérations d'écriture sur le cluster Amazon Redshift.	N'oubliez pas d'arrêter toutes les opérations d'écriture sur le cluster Amazon Redshift source jusqu'à ce que la migration soit terminée.	DBA

Préparer la migration dans la région cible

Tâche	Description	Compétences requises
Lancez et configurez une EC2 instance dans la région cible.	Connectez-vous à la console de gestion AWS pour une région de Chine, Pékin ou Ningxia. Dans la EC2 console Amazon, choisissez « Launch instance », puis créez et configurez une EC2 instance. Important : assurez-vous que vos groupes EC2 de sécurité Amazon pour les règles entrantes autorisent un accès illimité au port TCP 22 depuis votre machine source. Pour plus d'instructions sur le lancement et la configuration d'une EC2 instance, consultez la section « Ressources associées ».	DBA
Enregistrez les détails du cluster Amazon Redshift.	Ouvrez la console Amazon Redshift et choisissez « Clusters » dans le volet de navigation. Choisissez ensuite le nom du cluster Amazon	DBA

Tâche	Description	Compétences requises
	Redshift dans la liste. Dans l'onglet « Propriétés », dans la section « Configurations de base de données », enregistrez le « Nom de la base de données » et le « Port ». Ouvrez la section « Détails de la connexion » et enregistrez le « point de terminaison », au <port><databasename>format « point de terminaison :/». Important : assurez-vous que vos groupes de sécurité Amazon Redshift pour les règles entrantes autorisent un accès illimité au port TCP 5439 depuis votre instance. EC2	
Connectez psql au cluster Amazon Redshift.	<databasename><port>À l'invite de commande, spécifiez les informations de connexion en exécutant la commande « psql -h <endpoint>-U <userid>-d -p ». À l'invite de mot de passe psql, entrez le mot de passe de l'<userid>utilisateur « ». Vous êtes ensuite connecté au cluster Amazon Redshift et pouvez saisir des commandes de manière interactive.	DBA

Tâche	Description	Compétences requises
Créez un compartiment S3.	Ouvrez la console Amazon S3 et créez un compartiment S3 pour contenir les fichiers exportés depuis Amazon Redshift. Pour obtenir de l'aide sur ce sujet et sur d'autres articles, consultez la section « Ressources connexes ».	DBA
Créez une politique IAM qui prend en charge la copie de données.	Ouvrez la console IAM et choisissez « Politiques ». Choisissez « Créer une politique », puis choisissez l'onglet « JSON ». Copiez et collez la politique IAM pour copier des données depuis la section « Informations supplémentaires ». Important : remplacez « s3_bucket _name » par le nom de votre compartiment S3. Choisissez « Réviser la politique », entrez le nom et la description de la politique. Choisissez « Créer une politique ».	DBA

Tâche	Description	Compétences requises
Créez un rôle IAM pour autoriser l'opération COPY pour Amazon Redshift.	Ouvrez la console IAM et choisissez « Rôles ». Choisissez « Créer un rôle », puis « Service AWS » dans « Sélectionner le type d'entité de confiance ». Choisissez « Redshift » pour le service, choisissez « Redshift — Personnalisable », puis « Suivant ». Choisissez la politique « Copier » que vous avez créée précédemment, puis choisissez « Suivant ». Entrez un « Nom du rôle », puis choisissez « Créer un rôle ».	DBA
Associez le rôle IAM au cluster Amazon Redshift.	Ouvrez la console Amazon Redshift et choisissez « Gérer les rôles IAM ». Choisissez « Rôles disponibles » dans le menu déroulant et choisisse z le rôle que vous avez créé précédemment. Choisisse z « Appliquer les modificat ions ». Lorsque le « statut » du rôle IAM dans la section « Gérer les rôles IAM » indique « Synchronisé », vous pouvez exécuter la commande « COPIER ».	DBA

Vérifiez les données source et les informations sur les objets avant de commencer la migration

Tâche	Description	Compétences requises
Vérifiez les lignes des tables Amazon Redshift source.	Utilisez les scripts de la section « Informations supplémentaires » pour vérifier et enregistrer le nombre de lignes dans les tables Amazon Redshift sources. N'oubliez pas de répartir les données de manière égale pour les scripts UNLOAD et COPY. Cela améliorera l'efficac ité du déchargement et du chargement des données, car la quantité de données couverte par chaque script sera équilibrée.	DBA
Vérifiez le nombre d'objets de base de données dans le cluster Amazon Redshift source.	Utilisez les scripts de la section « Informations supplémentaires » pour vérifier et enregistrer le nombre de bases de données, d'utilisateurs, de schémas, de tables, de vues et de fonctions définies par l'utilisateur (UDFs) dans votre cluster Amazon Redshift source.	DBA
Vérifiez les résultats des instructions SQL avant la migration.	Certaines instructions SQL pour la validation des données doivent être triées en fonction de la situation réelle de l'entreprise et des données.	DBA

Tâche	Description	Compétences requises
	Cela permet de vérifier les données importées afin de garantir leur cohérence et leur affichage correct.	

Migrer les données et les objets vers la région cible

Tâche	Description	Compétences requises
Générez des scripts DDL Amazon Redshift.	Générez des scripts DDL (Data Definition Language) en utilisant les liens de la section « Instructions SQL pour interroger Amazon Redshift » dans la section « Informations supplémen taires ». Ces scripts DDL doivent inclure les requêtes « créer un utilisateur », « créer un schéma », « privilèges sur le schéma pour l'utilisateur », « créer une table/une vue », « privilèges sur des objets pour l'utilisateur » et « créer une fonction ».	DBA
Créez des objets dans le cluster Amazon Redshift pour la région cible.	Exécutez les scripts DDL à l'aide de l'interface de ligne de commande AWS (AWS CLI) dans la région AWS en Chine. Ces scripts créeront des objets dans le cluster Amazon Redshift pour la région cible.	DBA

Tâche	Description	Compétences requises
Déchargez les données sources du cluster Amazon Redshift dans le compartiment S3.	Exécutez la commande UNLOAD pour décharger les données du cluster Amazon Redshift de la région source vers le compartiment S3.	DBA, Développeur
Transférez les données du compartiment source de la région S3 vers le compartim ent de la région S3 cible.	Transférez les données de votre compartiment de région S3 source vers le compartim ent S3 cible. La commande « $ aws s3 sync » ne pouvant pas être utilisée, veillez à suivre le processus décrit dans l'article « Transférer les données Amazon S3 des régions AWS vers les régions AWS en Chine » de la section « Ressources associées ».	Developer
Chargez les données dans le cluster Amazon Redshift cible.	Dans l'outil psql de votre région cible, exécutez la commande COPY pour charger les données du compartiment S3 vers le cluster Amazon Redshift cible.	DBA

Vérifiez les données dans les régions source et cible après la migration

Tâche	Description	Compétences requises
Vérifiez et comparez le nombre de lignes dans les tables source et cible.	Vérifiez et comparez le nombre de lignes du tableau dans les régions source et	DBA

Tâche	Description	Compétences requises
	cible pour vous assurer que toutes sont migrées.	
Vérifiez et comparez le nombre d'objets de base de données source et cible.	Vérifiez et comparez tous les objets de base de données dans les régions source et cible pour vous assurer qu'ils sont tous migrés.	DBA
Vérifiez et comparez les résultats des scripts SQL dans les régions source et cible.	Exécutez les scripts SQL préparés avant la migration . Vérifiez et comparez les données pour vous assurer que les résultats SQL sont corrects.	DBA
Réinitialisez les mots de passe de tous les utilisateurs du cluster Amazon Redshift cible.	Une fois la migration terminée et toutes les données vérifiées , vous devez réinitialiser tous les mots de passe utilisate ur pour le cluster Amazon Redshift dans la région AWS en Chine.	DBA

Ressources connexes

- Transfert de données Amazon S3 des régions AWS vers les régions AWS en Chine
- Création d'un compartiment S3
- Réinitialisation d'un mot de passe utilisateur Amazon Redshift
- documentation psql

Informations supplémentaires

Politique IAM pour le déchargement des données

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Politique IAM pour la copie de données

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::s3_bucket_name"]
    },
    {
      "Effect": "Allow",
      "Action": ["s3:GetObject"],
      "Resource": ["arn:aws:s3:::s3_bucket_name/*"]
    }
  ]
}
```

Instructions SQL pour interroger Amazon Redshift

```
##Database

select * from pg_database where datdba>1;

##User
```

```
select * from pg_user where usesysid>1;

##Schema

SELECT n.nspname AS "Name",

  pg_catalog.pg_get_userbyid(n.nspowner) AS "Owner"

FROM pg_catalog.pg_namespace n

WHERE n.nspname !~ '^pg_' AND n.nspname <> 'information_schema'

ORDER BY 1;

##Table

select count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema');

select schemaname,count(*) from pg_tables where schemaname not in
 ('pg_catalog','information_schema') group by schemaname order by 1;

##View

SELECT

    n.nspname AS schemaname,c.relname AS
 viewname,pg_catalog.pg_get_userbyid(c.relowner) as "Owner"

FROM

    pg_catalog.pg_class AS c

INNER JOIN

    pg_catalog.pg_namespace AS n

    ON c.relnamespace = n.oid

WHERE relkind = 'v' and n.nspname not in ('information_schema','pg_catalog');

##UDF

SELECT
```

```
   n.nspname AS schemaname,

   p.proname AS proname,

   pg_catalog.pg_get_userbyid(p.proowner) as "Owner"

FROM pg_proc p

LEFT JOIN pg_namespace n on n.oid = p.pronamespace

WHERE p.proowner != 1;
```

Scripts SQL pour générer des instructions DDL

- Script Get_Schema_Priv_by_user
- Générer un script TBL_DDL
- Generate_View_DDL
- Generate_User_Grant_Revoke_DDL
- Générer un UDF_DDL

Transportez des bases de données PostgreSQL entre deux instances de base de données Amazon RDS à l'aide de pg_transport

Créée par Raunak Rishabh (AWS) et Jitender Kumar (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration de bases de données extrêmement volumineuses entre deux instances de base de données Amazon Relational Database Service (Amazon RDS) pour PostgreSQL à l'aide de l'extension pg_transport. Cette extension offre un mécanisme physique de transport permettant de déplacer chaque base de données. En diffusant les fichiers de base de données avec un traitement minimal, il fournit une méthode extrêmement rapide pour migrer des bases de données volumineuses entre des instances de base de données avec un temps d'arrêt minimal. Cette extension utilise un modèle d'extraction dans lequel l'instance de base de données cible importe la base de données depuis l'instance de base de données source.

Conditions préalables et limitations

Prérequis

- Les deux instances de base de données doivent exécuter la même version majeure de PostgreSQL.
- La base de données ne doit pas exister sur la cible. Dans le cas contraire, le transport échoue.
- Aucune extension autre que pg_transport ne doit être activée dans la base de données source.
- Tous les objets de la base de données source doivent se trouver dans le tablespace pg_default par défaut.
- Le groupe de sécurité de l'instance de base de données source doit autoriser le trafic provenant de l'instance de base de données cible.
- Installez un client PostgreSQL tel que psql PgAdminou pour fonctionner avec l'instance de base de données Amazon RDS PostgreSQL. Vous pouvez installer le client dans votre système local ou utiliser une instance Amazon Elastic Compute Cloud (Amazon EC2). Dans ce modèle, nous utilisons psql sur une EC2 instance.

Limites

- Vous ne pouvez pas transporter de bases de données entre différentes versions majeures d'Amazon RDS for PostgreSQL.

- Les privilèges d'accès et la propriété de la base de données source ne sont pas transférés vers la base de données cible.
- Vous ne pouvez pas transporter de bases de données sur des répliques en lecture ou sur des instances parentes de répliques en lecture.
- Vous ne pouvez pas utiliser les types de données reg dans les tables de base de données que vous prévoyez de transporter avec cette méthode.
- Vous pouvez exécuter jusqu'à 32 transports au total (y compris les importations et les exportations) en même temps sur une instance de base de données.
- Vous ne pouvez pas renommer ou inclure/exclure des tables. Tout est migré tel quel.

Prudence

- Effectuez des sauvegardes avant de supprimer l'extension, car la suppression de l'extension supprime également les objets dépendants et certaines données essentielles au fonctionnement de la base de données.
- Tenez compte de la classe d'instance et des processus exécutés sur d'autres bases de données de l'instance source lorsque vous déterminez le nombre de travailleurs et les `work_mem` valeurs de pg_transport.
- Lorsque le transport démarre, toutes les connexions à la base de données source sont interrompues et la base de données passe en mode lecture seule.

> **Note**
>
> Lorsque le transport est exécuté sur une base de données, il n'affecte pas les autres bases de données du même serveur.

Versions du produit

- Amazon RDS pour PostgreSQL 10.10 et versions ultérieures, et Amazon RDS pour PostgreSQL 11.5 et versions ultérieures. Pour obtenir les informations les plus récentes sur les versions, consultez Transporter des bases de données PostgreSQL entre des instances de base de données dans la documentation Amazon RDS.

Architecture

Outils

- pg_transport fournit un mécanisme de transport physique pour déplacer chaque base de données. En diffusant les fichiers de base de données avec un minimum de traitement, le transport physique déplace les données beaucoup plus rapidement que les processus traditionnels de vidage et de chargement et nécessite un minimum de temps d'arrêt. Les bases de données transportables PostgreSQL utilisent un modèle d'extraction dans lequel l'instance de base de données de destination importe la base de données à partir de l'instance de base de données source. Vous installez cette extension sur vos instances de base de données lorsque vous préparez les environnements source et cible, comme expliqué dans ce modèle.
- psql vous permet de vous connecter à vos instances de base de données PostgreSQL et de les utiliser. Pour installer psql sur votre système, consultez la page des téléchargements de PostgreSQL.

Épopées

Création du groupe de paramètres cible

Tâche	Description	Compétences requises
Créez un groupe de paramètres pour le système cible.	Spécifiez un nom de groupe qui l'identifie en tant que groupe de paramètres cible ; par exemple,`pgtarget-param-group` . Pour obtenir des instructions, consultez la documentation Amazon RDS.	DBA
Modifiez les paramètres du groupe de paramètres.	Définissez les paramètres suivants : 1. Ajoutez `pg_transport` au `shared_pr`	DBA

Tâche	Description	Compétences requises
	`eload_libraries` paramètre. `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Définissez le paramètre `pg_transport.num_workers` . Choisissez le nombre de travailleurs avec lesquels vous souhaitez effectuer le transport. La valeur que vous définissez détermine le nombre de `transport.send_file` travailleurs qui seront créés dans la source. 3. Augmentez la valeur de `max_worker_processes` jusqu'à plus de trois fois la valeur de`pg_transport.num_workers` . Par exemple, si vous définissez la valeur `pg_transport.num_workers` de 4, la `max_worker_processes` valeur doit être d'au moins 13. En cas d'échec, pg_transport recommande une valeur minimale. 4. `pg_transport.timing` Réglé sur 1. Ce	

Tâche	Description	Compétences requises
	paramètre permet de signaler les informations temporelles pendant le transport. 5. Définissez le paramètre `pg_transport.work_mem` . Ce paramètre indique la mémoire maximale à allouer à chaque travailleur. La valeur par défaut est de 128 Mo. Pour plus d'informations sur ces paramètres, consultez la documentation Amazon RDS.	

Création du groupe de paramètres source

Tâche	Description	Compétences requises
Créez un groupe de paramètres pour le système source.	Spécifiez un nom de groupe qui l'identifie en tant que groupe de paramètres source ; par exemple,`pgsource-param-group` . Pour obtenir des instructions, consultez la documentation Amazon RDS.	DBA
Modifiez les paramètres du groupe de paramètres.	Définissez les paramètres suivants :	DBA

Tâche	Description	Compétences requises
	1. Ajoutez `pg_transport` au `shared_preload_libraries` paramètre. `shared_preload_libraries = pg_stat_statements, pg_transport` 2. Définissez le paramètre `pg_transport.num_workers`. La valeur de ce paramètre définie dans la cible détermine le nombre de `transport.send_file` travailleurs à utiliser. Si une importation est en cours d'exécution sur cette instance, augmentez cette valeur, mais tenez compte du nombre de travailleurs déjà en cours d'exécution. 3. Augmentez la valeur de `max_worker_processes` jusqu'à plus de trois fois la valeur de `pg_transport.num_workers` sur la cible. Par exemple, si vous définissez la valeur `pg_transport.num_workers` de 4 sur la cible, la `max_worker_processes` valeur	

Tâche	Description	Compétences requises
	sur la source doit être d'au moins 13. En cas d'échec, pg_transport recommande une valeur minimale. 4. Définissez le paramètre `pg_transport.work_mem` . Ce paramètre indique la mémoire maximale à allouer à chaque travailleur. La valeur par défaut est de 128 Mo. Pour plus d'informations sur ces paramètres, consultez la documentation Amazon RDS.	

Préparer l'environnement cible

Tâche	Description	Compétences requises
Créez une nouvelle instance de base de données Amazon RDS for PostgreSQL vers laquelle transporter votre base de données source.	Déterminez la classe d'instance et la version de PostgreSQL en fonction des besoins de votre entreprise.	DBA, administrateur système, architecte de base de données
Modifiez le groupe de sécurité de la cible pour autoriser les connexions sur le port de l'instance de base de données depuis l' EC2 instance.	Par défaut, le port de l'instance PostgreSQL est 5432. Si vous utilisez un autre port, les connexions à ce port doivent être ouvertes pour l' EC2 instance.	DBA, administrateur système

Tâche	Description	Compétences requises
Modifiez l'instance et attribuez le nouveau groupe de paramètres cible.	Par exemple, `pgtarget-param-group` .	DBA
Redémarrez l'instance de base de données Amazon RDS cible.	Les paramètres `shared_preload_libraries` et `max_worker_processes` sont des paramètres statiques qui nécessitent un redémarrage de l'instance.	DBA, administrateur système
Connectez-vous à la base de données depuis l' EC2 instance à l'aide de psql.	Utilisez la commande : `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Créez l'extension pg_transport.	Exécutez la requête suivante en tant qu'utilisateur ayant le `rds_superuser` rôle : `create extension pg_transport;`	DBA

Préparation de l'environnement source

Tâche	Description	Compétences requises
Modifiez le groupe de sécurité de la source pour autoriser les connexions sur le port de l'instance de base de données depuis l' EC2 instance	Par défaut, le port de l'instance PostgreSQL est 5432. Si vous utilisez un autre port, les connexions à ce port doivent être ouvertes pour l' EC2 instance.	DBA, administrateur système

Tâche	Description	Compétences requises
Amazon et l'instance de base de données cible		
Modifiez l'instance et assignez le nouveau groupe de paramètres source.	Par exemple, `pgsource-param-group` .	DBA
Redémarrez l'instance de base de données Amazon RDS source.	Les paramètres `shared_preload_libraries` et `max_worker_processes` sont des paramètres statiques qui nécessitent un redémarrage de l'instance.	DBA
Connectez-vous à la base de données depuis l' EC2 instance à l'aide de psql.	Utilisez la commande : `psql -h <rds_end_point> -p PORT -U username -d database -W`	DBA
Créez l'extension pg_transport et supprimez toutes les autres extensions des bases de données à transporter.	Le transport échouera si des extensions autres que pg_transport sont installées sur la base de données source. Cette commande doit être exécutée par un utilisateur doté du `rds_superuser` rôle.	DBA

Effectuer le transport

Tâche	Description	Compétences requises
Effectuez un essai à sec.	Utilisez la `transport.import_from_server`	DBA

Tâche	Description	Compétences requises
	fonction pour effectuer d'abord un essai à sec : `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', 'true');` Le dernier paramètre de cette fonction (défini sur`true`) définit le cycle à sec. Cette fonction affiche toutes les erreurs que vous pourriez rencontrer lors de l'exécution du transport principal. Résolvez les erreurs avant d'exécuter le transport principal.	

Tâche	Description	Compétences requises
Si le dry run est réussi, lancez le transport de la base de données.	Exécutez la `transport.import_from_server` fonction pour effectuer le transport. Il se connecte à la source et importe les données. `SELECT transport.import_from_server( 'source-db-instance-endpoint', source-db-instance-port, 'source-db-instance-user', 'source-user-password', 'source-database-name', 'destination-user-password', false);` Le dernier paramètre de cette fonction (défini sur`false`) indique qu'il ne s'agit pas d'un essai à sec.	DBA

Tâche	Description	Compétences requises
Effectuez les étapes après le transport.	Une fois le transport de la base de données terminé : • Validez les données dans l'environnement cible. • Ajoutez tous les rôles et autorisations à la cible. • Activez toutes les extensions requises dans la cible et dans la source, si nécessaire. • Annulez la valeur du `max_worker_processes` paramètre.	DBA

Ressources connexes

- Documentation Amazon RDS
- documentation de pg_transport
- Migration de bases de données à l'aide de bases de données transportables RDS PostgreSQL (article de blog)
- Téléchargements de PostgreSQL
- utilitaire psql
- Création d'un groupe de paramètres DB
- Modifier les paramètres d'un groupe de paramètres de base de données
- Téléchargements de PostgreSQL

Recréation de plateforme

Rubriques

- Exporter une base de données Microsoft SQL Server vers Amazon S3 à l'aide d'AWS DMS
- Migrez les charges de travail de création, de formation et de déploiement de ML vers Amazon à SageMaker l'aide des outils de développement AWS
- Migrer OpenText TeamSite les charges de travail vers le cloud AWS
- Migrer les valeurs Oracle CLOB vers des lignes individuelles dans PostgreSQL sur AWS
- Migrez une base de données Oracle sur site vers Amazon RDS for Oracle en utilisant directement Oracle Data Pump Import via un lien de base de données
- Migrer Oracle E-Business Suite vers Amazon RDS Custom
- Migrer Oracle PeopleSoft vers Amazon RDS Custom
- Migrer la fonctionnalité Oracle ROWID vers PostgreSQL sur AWS
- Migrer les codes d'erreur de la base de données Oracle vers une base de données compatible avec Amazon Aurora PostgreSQL
- Migrer les charges de travail Redis vers Redis Enterprise Cloud sur AWS
- Migrez SAP ASE sur Amazon EC2 vers Amazon Aurora PostgreSQL compatible avec AWS SCT et AWS DMS
- Migrer les certificats SSL Windows vers un Application Load Balancer à l'aide d'ACM
- Migrer une file d'attente de messagerie de Microsoft Azure Service Bus vers Amazon SQS
- Migrer une base de données relationnelle vers MongoDB Atlas sur AWS
- Migrer un environnement MongoDB auto-hébergé vers MongoDB Atlas sur AWS
- Migrer une EnterpriseOne base de données Oracle JD Edwards vers AWS à l'aide d'Oracle Data Pump et d'AWS DMS
- Migrer une PeopleSoft base de données Oracle vers AWS à l'aide d'AWS DMS
- Migrer une base de données MySQL sur site vers Amazon RDS for MySQL
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server
- Migrez les données de Microsoft Azure Blob vers Amazon S3 à l'aide de Rclone
- Migrer du serveur Couchbase vers Couchbase Capella sur AWS
- Migrer d'un serveur WebSphere d'applications IBM vers Apache Tomcat sur Amazon EC2
- Migrez d'IBM WebSphere Application Server vers Apache Tomcat sur Amazon EC2 avec Auto Scaling

- Migrer une application .NET de Microsoft Azure App Service vers AWS Elastic Beanstalk
- Migrer d'Oracle WebLogic vers Apache Tomcat (ToMee) sur Amazon ECS
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for Oracle à l'aide d'AWS DMS
- Migrer une base de données Oracle sur site vers Amazon OpenSearch Service à l'aide de Logstash
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'Oracle Data Pump
- Migrez de PostgreSQL sur EC2 Amazon vers Amazon RDS pour PostgreSQL à l'aide de pglogical
- Migrer une base de données PostgreSQL locale vers Aurora PostgreSQL
- Migrer une base de données Microsoft SQL Server sur site vers Microsoft SQL Server sur Amazon EC2 exécutant Linux
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de serveurs liés
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de méthodes de sauvegarde et de restauration natives
- Migrer une base de données Microsoft SQL Server vers Aurora MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données MariaDB sur site vers Amazon RDS for MariaDB à l'aide d'outils natifs
- Migrer une base de données MySQL sur site vers Aurora MySQL
- Migrez des bases de données MySQL sur site vers Aurora MySQL à l'aide de Percona, XtraBackup Amazon EFS et Amazon S3
- Migrez des applications Java sur site vers AWS à l'aide d'AWS App2Container
- Migrer des systèmes de fichiers partagés dans le cadre d'une migration AWS de grande envergure
- Migrer une base de données Oracle vers Amazon RDS for Oracle à l'aide d'adaptateurs de GoldenGate fichiers plats Oracle
- Modifier les applications Python et Perl pour prendre en charge la migration de bases de données de Microsoft SQL Server vers Amazon Aurora PostgreSQL Compatible Edition
- Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS

Exporter une base de données Microsoft SQL Server vers Amazon S3 à l'aide d'AWS DMS

Créée par Sweta Krishna (AWS)

Récapitulatif

Organisations ont souvent besoin de copier des bases de données vers Amazon Simple Storage Service (Amazon S3) à des fins de migration, de sauvegarde et de restauration, d'archivage des données et d'analyse des données. Ce modèle décrit comment exporter une base de données Microsoft SQL Server vers Amazon S3. La base de données source peut être hébergée sur site ou sur Amazon Elastic Compute Cloud (Amazon EC2) ou Amazon Relational Database Service (Amazon RDS) pour Microsoft SQL Server sur le cloud Amazon Web Services (AWS).

Les données sont exportées à l'aide d'AWS Database Migration Service (AWS DMS). Par défaut, AWS DMS écrit les données de capture des données de chargement complet et de modification (CDC) au format .csv (valeurs séparées par des virgules). Pour un stockage plus compact et des options de requête plus rapides, ce modèle utilise l'option de format Apache Parquet (.parquet).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Rôle AWS Identity and Access Management (IAM) pour le compte avec accès en écriture, suppression et balisage au compartiment S3 cible, et AWS DMS (`dms.amazonaws.com`) ajouté en tant qu'entité de confiance à ce rôle IAM
- Une base de données Microsoft SQL Server sur site (ou Microsoft SQL Server sur une EC2 instance ou une base de données Amazon RDS for SQL Server)
- Connectivité réseau entre le cloud privé virtuel (VPC) sur AWS et le réseau sur site fourni par AWS Direct Connect ou un réseau privé virtuel (VPN)

Limites

- Un compartiment S3 compatible VPC (VPC de passerelle) n'est actuellement pas pris en charge dans les versions d'AWS DMS antérieures à 3.4.7.
- Les modifications apportées à la structure de la table source lors du chargement complet ne sont pas prises en charge.

- Le mode LOB (Full Large Binary Object) d'AWS DMS n'est pas pris en charge.

Versions du produit

- Microsoft SQL Server versions 2005 ou ultérieures pour les éditions Enterprise, Standard, Workgroup et Developer.
- Support pour Microsoft SQL Server version 2019 en tant que source est disponible dans les versions 3.3.2 et ultérieures d'AWS DMS.

Architecture

Pile technologique source

- Une base de données Microsoft SQL Server sur site (ou Microsoft SQL Server sur une EC2 instance ou une base de données Amazon RDS for SQL Server)

Pile technologique cible

- AWS Direct Connect
- AWS DMS
- Amazon S3

Architecture cible

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- AWS Direct Connect relie votre réseau interne à un emplacement Direct Connect via un câble Ethernet à fibre optique standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les services AWS publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Épopées

Préparer la migration

Tâche	Description	Compétences requises
Validez la version de la base de données.	Validez la version de la base de données source et assurez-vous qu'elle est prise en charge par AWS DMS. Pour plus d'informations sur les versions de base de données SQL Server prises en charge, consultez la section Utilisation d'une base de données Microsoft SQL Server comme source pour AWS DMS.	DBA
Créez un VPC et un groupe de sécurité.	Dans votre compte AWS, créez un VPC et un groupe de sécurité. Pour plus d'informations, consultez la documentation Amazon VPC.	Administrateur système
Créez un utilisateur pour la tâche AWS DMS.	Créez un utilisateur AWS DMS dans la base de données source et accordez-lui les autorisations READ. Cet utilisateur sera utilisé par AWS DMS.	DBA
Testez la connectivité à la base de données.	Testez la connectivité à l'instance de base de données SQL Server auprès de l'utilisateur AWS DMS.	DBA

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez le compartiment S3 cible. Ce compartiment contiendra les données de la table migrée.	Administrateur de systèmes
Créez une politique et un rôle IAM.	1. Pour créer une politique IAM avec des autorisations de compartiment, utilisez le code de la section Informations supplémentaires. 2. Créez le rôle pour AWS DMS et associez la politique au rôle.	Administrateur de systèmes

Migrer les données à l'aide d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication AWS DMS.	Connectez-vous à l'AWS Management Console, puis ouvrez la console AWS DMS. Dans le volet de navigation, choisissez Instances de réplication, puis Créer une instance de réplication. Pour obtenir des instructions, consultez l'étape 1 de la documentation AWS DMS.	DBA
Créez des points de terminaison source et cible.	Créez des points de terminaison source et cible. Testez la connexion entre l'instance de réplication et les points de terminaison source et cible.	DBA

Tâche	Description	Compétences requises
	Pour obtenir des instructions, consultez l'étape 2 de la documentation AWS DMS.	
Créez une tâche de réplication.	Créez une tâche de réplication et sélectionnez le chargement complet ou le chargement complet avec capture des données de modification (CDC) pour migrer les données de SQL Server vers le compartiment S3. Pour obtenir des instructions, consultez l'étape 3 de la documentation AWS DMS.	DBA
Démarrez la réplication des données.	Lancez la tâche de réplication et surveillez les journaux pour détecter toute erreur.	DBA

Valider les données

Tâche	Description	Compétences requises
Validez les données migrées.	Sur la console, accédez à votre compartiment S3 cible. Ouvrez le sous-dossier portant le même nom que la base de données source. Vérifiez que le dossier contient toutes les tables migrées depuis la base de données source.	DBA

Nettoyage des ressources

Tâche	Description	Compétences requises
Arrêtez et supprimez les ressources AWS temporaires.	Arrêtez les ressources AWS temporaires que vous avez créées pour la migration des données, telles que l'instanc e de réplication AWS DMS, et supprimez-les après avoir validé l'exportation.	DBA

Ressources connexes

- Guide de l'utilisateur d'AWS Database Migration Service
- Utilisation d'une base de données Microsoft SQL Server comme source pour AWS DMS
- Utilisation d'Amazon S3 comme cible pour AWS Database Migration Service
- Utilisation d'un compartiment S3 comme cible AWS DMS (AWS Re:POST)

Informations supplémentaires

Utilisez le code suivant pour ajouter une politique IAM avec des autorisations de compartiment S3 pour le rôle AWS DMS. Remplacez `bucketname` par le nom de votre compartiment.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "s3:PutObject",
                 "s3:DeleteObject"
             ],
             "Resource": [
                 "arn:aws:s3:::bucketname*"
             ]
         },
         {
```

```
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::bucketname*"
            ]
        }
    ]
}
```

Migrez les charges de travail de création, de formation et de déploiement de ML vers Amazon à SageMaker l'aide des outils de développement AWS

Créée par Mustafa Waheed (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle fournit des conseils pour la migration d'une application d'apprentissage automatique (ML) sur site exécutée sur des serveurs Unix ou Linux à former et à déployer sur AWS à l'aide d'Amazon. SageMaker Ce déploiement utilise un pipeline d'intégration continue et de déploiement continu (CI/CD). Le modèle de migration est déployé à l'aide d'une CloudFormation pile AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif utilisant AWS Landing Zone
- Interface de ligne de commande (AWS CLI) (AWS CLI) installée et configurée sur votre serveur Unix ou Linux
- Un référentiel de code source ML provisionné dans AWS CodeCommit

Limites

- Seuls 300 pipelines individuels peuvent être déployés dans une région AWS.
- Ce modèle est destiné aux charges de travail ML supervisées avec train-and-deploy du code en Python.

Versions du produit

- Docker version 19.03.5, build 633a0ea, avec Python 3.6x

Architecture

Pile technologique source

- Instance de calcul Linux sur site avec des données sur le système de fichiers local ou dans une base de données relationnelle

Architecture source

Pile technologique cible

- AWS a été CodePipeline déployé avec Amazon S3 pour le stockage des données et Amazon DynamoDB comme magasin de métadonnées pour le suivi ou la journalisation des cycles de pipeline

Architecture cible

Architecture de migration des applications

- Package Python natif et CodeCommit référentiel AWS (et un client SQL, pour les ensembles de données sur site sur une instance de base de données)

Outils

- Python3
- Git
- AWS CLI — L'AWS CLI déploie la CloudFormation pile AWS et déplace les données vers le compartiment S3. Le compartiment S3 mène à son tour à la cible.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez le code source et les ensembles de données.		Spécialiste des données
Identifiez les types et tailles d'instances cibles de création, de formation et de déploiement.		Ingénieur de données, data scientist
Créez une liste de capacités et des exigences de capacité.		
Identifiez les exigences du réseau.		DBA, administrateur système
Identifiez les exigences de sécurité d'accès au réseau ou à l'hôte pour les applications source et cible.		Ingénieur de données, ingénieur ML, administrateur système
Déterminez la stratégie de sauvegarde.		Ingénieur ML, administrateur système
Déterminez les exigences de disponibilité.		Ingénieur ML, administrateur système
Identifiez la stratégie de migration ou de transition des applications.		Data scientist, ingénieur ML

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)		Ingénieur ML, administrateur système
Créez des groupes de sécurité.		Ingénieur ML, administrateur système
Configurez un compartiment Amazon S3 et des branches de CodeCommit référentiel AWS pour le code ML.		Ingénieur ML

Téléchargez les données et le code

Tâche	Description	Compétences requises
Utilisez des outils MySQL natifs ou des outils tiers pour migrer, former, valider et tester des ensembles de données vers un compartiment S3 provisionné.	Cela est nécessaire pour le déploiement d'AWS CloudFormation Stack.	Ingénieur de données, ingénieur ML
Package du train ML et du code d'hébergement sous forme de packages Python et transfert vers le référenti el provisionné dans AWS CodeCommit ou GitHub.	Vous avez besoin du nom de branche du référentiel pour déployer le CloudFormation modèle AWS à des fins de migration.	Data scientist, ingénieur ML

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration de la charge de travail ML.		Propriétaire de l'application, ingénieur ML
Déployez la CloudFormation pile AWS.	Utilisez la CLI AWS pour créer la pile déclarée dans le modèle YAML fourni avec cette solution.	Data scientist, ingénieur ML

Découper

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		Propriétaire de l'application, data scientist, ingénieur ML

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.	Arrêtez toutes les ressources personnalisées du CloudFormation modèle AWS (par exemple, les fonctions AWS Lambda qui ne sont pas utilisées).	Data scientist, ingénieur ML
Passez en revue et validez les documents du projet.		Propriétaire de l'application, data scientist

Tâche	Description	Compétences requises
Validez les résultats et les métriques d'évaluation du modèle ML avec les opérateurs.	Assurez-vous que les performances du modèle correspondent aux attentes des utilisateurs de l'application et sont comparables à celles de l'état sur site.	Propriétaire de l'application, data scientist
Clôturez le projet et faites part de vos commentaires.		Propriétaire de l'application, ingénieur ML

Ressources connexes

- AWSCodePipeline
- AWS CodeCommit
- AWSCodeBuild
- AmazonSageMaker
- Amazon S3
- Amazon DynamoDB
- AWS Lambda

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer OpenText TeamSite les charges de travail vers le cloud AWS

Créée par Battulga Purevragchaa (AWS), Michael Stewart et Carlos Marruenda Molina

Récapitulatif

> **Warning**
>
> Ce scénario nécessite que les utilisateurs IAM disposent d'un accès programmatique et d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisat ions lorsqu'elles ne sont plus nécessaires. Les clés d'accès peuvent être mises à jour si nécessaire. Pour plus d'informations, consultez la section Mise à jour des clés d'accès dans le guide de l'utilisateur IAM.

De nombreuses instances OpenText d'Experience Platform sont hébergées sur site ou sur des solutions d'hébergement traditionnelles avec une capacité fixe et des modèles de coûts hérités. La migration de vos charges de travail OpenText Experience Platform vers le cloud Amazon Web Services (AWS) apporte des fonctionnalités et de la valeur supplémentaires en augmentant l'agilité de votre entreprise et les opportunités d'intégration, en plus de réduire votre coût de propriété global.

Ce modèle fournit des étapes et un modèle pour migrer les OpenText TeamSitecharges de travail vers le cloud AWS. Le modèle vous aide à comprendre comment définir le périmètre et le budget de vos projets de migration en fournissant une section Epics détaillée qui vous guide tout au long du processus de OpenText TeamSite migration.

Ce modèle a été développé par AWS et TBSCG, un partenaire AWS, et accompagne le guide Migrating OpenText TeamSite and Media Management workloads to the AWS Cloud sur le site Web AWS Prescriptive Guidance.

Conditions préalables et limitations

Prérequis

- Au moins un compte AWS actif
- OpenText Charge de travail hébergée dans un centre de données sur site ou chez un autre fournisseur de cloud

- OpenText Licences actives

Le processus de migration nécessite également les rôles et responsabilités décrits dans le tableau suivant.

Rôle	Responsabilités
Sponsor	Parrainage interne
Responsable de livraison	Livraison de la migration
Architecte de solutions	Définition de l'architecture actuelle et de la nouvelle architecture
DevOps ingénieur	DevOps activités
Testeur QA	Tests au niveau du système
Propriétaire du produit	Hiérarchisation des tâches en fonction des exigences de l'entreprise
TeamSite auteurs	Test d'acceptation par les utilisateurs (UAT) de migration
TeamSite administrateur	Migration UAT
OpenText plomb	OpenText spécialiste des produits
OpenText développeur	OpenText spécialiste des produits
Spécialiste de la tarification	AWS et les OpenText licences
Sécurité informatique	Base de référence de sécurité informatique
Développeur d'intégration tiers	Retravailler les intégrations existantes
Développeur front-end	Apporter des modifications au code frontal migré
Administrateur de base de données	Configuration de base de données

Limites

- Assurez-vous de la compatibilité avec vos systèmes d'exploitation cibles (OSs). Vous pouvez utiliser la matrice de compatibilité figurant dans les notes de version du OpenText produit que vous migrez.

Architecture

Pile technologique source

- OpenText solutions d'expérience client hébergées sur site ou chez un autre fournisseur de cloud :
  - OpenText TeamSite
  - OpenText LiveSite
  - OpenText Gestion des médias
  - OpenText MediaBin

Pile technologique cible

- Une plateforme d'expérience OpenText client hébergée sur le cloud AWS et qui utilise les services AWS suivants :
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon Elastic Container Service (Amazon ECS)
  - Amazon OpenSearch Service
  - Elastic Load Balancing
  - AWS Lambda
  - Amazon API Gateway
  - Amazon Relational Database Service (Amazon RDS)
  - Amazon Elastic Block Store (Amazon EBS)
  - Amazon Simple Storage Service (Amazon S3)

Architecture cible

Outils

- AWS Database Migration Service (AWS DMS) est un service cloud qui facilite la migration de bases de données relationnelles, d'entrepôts de données, de bases de données NoSQL et d'autres types de magasins de données.
- AWS Application Migration Service automatise la conversion de vos serveurs sources pour qu'ils s'exécutent de manière native sur AWS. Il simplifie également la modernisation des applications grâce à des options d’optimisation intégrées et personnalisées.

Épopées

Découverte et évaluation

Tâche	Description	Compétences requises
Organisez des ateliers sur les exigences en matière de découverte.	Organisez des ateliers avec les équipes commerciales et techniques pour découvrir le paysage actuel, recueillir les exigences et valider la stratégie de migration. En fonction de la complexité et de l'ampleur de votre migration, votre organisation peut avoir besoin de plusieurs ateliers. Durée : deux semaines	Sponsor (facultatif), responsable de livraison, architecte de solutions, OpenText responsable, responsable du produit
Analysez les exigences en matière de solution et de migration.	Analysez et documentez les exigences commerciales, fonctionnelles et techniques qui influencent la conception de la solution planifiée et le processus de migration. Durée : Une semaine	Architecte de solutions, OpenText responsable, responsable du produit

Tâche	Description	Compétences requises
Documentez votre OpenText architecture existante.	Documentez votre OpenText architecture existante, y compris les composant s principaux et toutes les applications et services associés. Durée : Une semaine	Architecte de solutions, OpenText responsable, responsable du produit
Définissez l'architecture AWS prévue.	Définissez votre architect ure AWS prévue en fonction des composants identifiés, des exigences et en utilisant la matrice de OpenText compatibilité. Vous trouverez la matrice de OpenText compatibilité dans les notes de publication de votre OpenText TeamSite version. Durée : Une semaine	Architecte de solutions, OpenText responsable, responsable du produit, sécurité informatique
Évaluez la taille de votre architecture AWS prévue.	Les exigences de taille varient selon les composants architecturaux en fonction de la charge de travail et d'autres exigences non fonctionnelles. Durée : Deux jours	Architecte de solutions, OpenText responsable
Calculez le TCO.	Calculez le coût total de possession (TCO) de la solution que vous proposez. Durée : Deux jours	Architecte de solutions, spécialiste de la tarification

Tâche	Description	Compétences requises
Définissez la stratégie de migration pour chaque composant.	Définissez et documentez laquelle des sept stratégie s de migration courantes (7 R) utiliser pour chaque composant principal ou supplémentaire devant être migré vers le cloud AWS. Durée : Une semaine	Architecte de solutions, OpenText responsable, responsable du produit
Définissez le processus de migration des composants.	Définissez le processus de migration détaillé pour chacun des composants de votre charge de travail. Durée : Une semaine	Architecte de solutions, OpenText responsable, responsable du produit, sécurité informatique
Définissez le processus de migration global et ses dépendances.	Créez un processus et un calendrier de migration globaux qui incluent les détails de migration pour les composants, les dépendances et la continuité des activités. Durée : Trois jours	Architecte de solutions, OpenText responsable, responsable du produit, sécurité informatique

Activités de sécurité et de conformité

Tâche	Description	Compétences requises
Créez des politiques de sécurité.	Configurez les politiques de sécurité gérées par le client dans vos comptes AWS. Cela devrait inclure la complexit é et la rotation des mots de passe, en plus de la désactiva	Architecte de solutions

Tâche	Description	Compétences requises
	tion automatique des comptes inutilisés. Pour plus d'informations sur les politiques gérées par le client, consultez la section Politiques gérées par le client dans la documentation AWS Identity and Access Management (IAM).	
Créez des utilisateurs IAM.	Créez les utilisateurs IAM qui ont besoin d'accéder à la console de gestion AWS, à l'interface de ligne de commande AWS (AWS CLI) et au kit SDK AWS. Pour plus d'informations sur la création d'utilisateurs IAM, consultez la section Création d'un utilisateur IAM dans votre compte AWS dans la documentation IAM.	Architecte de solutions
Créez des groupes IAM.	Créez les groupes d'utilisateurs IAM requis (par exemple, des groupes d'administrateurs ou de développeurs) et ajoutez-y des utilisateurs IAM. Pour plus d'informations sur les groupes d'utilisateurs IAM, consultez la section Groupes d'utilisateurs IAM dans la documentation IAM.	Architecte de solutions

Tâche	Description	Compétences requises
Joignez des politiques de sécurité.	Associez des politiques de sécurité aux groupes ou aux rôles IAM. Pour plus d'informations à ce sujet, consultez la section Attacher une politique à un groupe d'utilisateurs IAM dans la documentation IAM.	Architecte de solutions
Activez la facturation détaillée.	Pour plus d'informations sur la facturation, consultez la section Surveillance de votre utilisation et de vos coûts dans la documentation AWS Billing and Cost Management.	Architecte de solutions
Vérifiez les coordonnées de vos comptes.	Assurez-vous que les coordonnées de vos comptes sont à jour et qu'elles correspondent à plusieurs personnes au sein de votre organisation. Pour plus d'informations, consultez la section Gestion d'un compte AWS dans la documentation AWS Billing and Cost Management.	Architecte de solutions, Product Owner

Tâche	Description	Compétences requises
Ajoutez les coordonnées de sécurité.	Configurez vos informations de contact avec vos coordonnées de sécurité. Pour plus d'informations à ce sujet, consultez la section Gestion d'un compte AWS dans la documentation AWS Billing and Cost Management.	Architecte de solutions, sécurité informatique
Configurez les rôles IAM pour les EC2 instances.	Configurez les rôles IAM pour les EC2 instances. Pour plus d'informations à ce sujet, consultez les rôles IAM pour Amazon EC2 dans la EC2 documentation Amazon.	Architecte de solutions
Configurez l'accès à AWS Support.	Associez une politique IAM aux utilisateurs IAM qui ont besoin d'accéder à AWS Support for Support Center et de créer des dossiers de support. Pour plus d'informations à ce sujet, consultez la section Autorisations d'accès pour AWS Support dans la documentation d'AWS Support.	Architecte de solutions

Tâche	Description	Compétences requises
Activer CloudTrail.	Activez automatiquement AWS CloudTrail dans toutes vos régions AWS. Pour plus d'informations à ce sujet, consultez la section Utilisation `create-trail` dans la CloudTrail documentation AWS.	Architecte de solutions
Activez la validation du fichier CloudTrail journal.	Activez la validation des fichiers CloudTrail journaux. Pour plus d'informations à ce sujet, consultez la section Activation de la validation de l'intégrité des fichiers journaux CloudTrail dans la CloudTrail documentation AWS.	Architecte de solutions
Limitez l'accès à tous les compartiments S3 contenant des CloudTrail journaux.	Appliquez une politique de compartiment limitant l'accès aux compartiments S3 contenant des fichiers CloudTrail journaux. Pour plus d'informations à ce sujet, consultez la politique relative aux compartiments Amazon S3 CloudTrail dans la CloudTrail documentation AWS.	Architecte de solutions

Tâche	Description	Compétences requises
Intégrer CloudTrail aux CloudWatch journaux	Intégrez les traces générées CloudTrail par Amazon CloudWatch Logs. Pour plus d'informations à ce sujet, consultez la section Envoi d'événements aux CloudWatch journaux dans la CloudTrail documentation AWS.	Architecte de solutions
Activez AWS Config dans toutes les régions requises.	Activez automatiquement AWS Config dans toutes les régions requises. Vous pouvez configurer AWS Config à l'aide de l'AWS CLI. Pour plus d'informations, consultez la section Configuration d'AWS Config avec l'interface de ligne de commande AWS dans la documentation AWS Config.	Architecte de solutions
Activez la journalisation de l'accès au compartiment S3.	Automatisez la journalisation des accès aux compartiments S3 avec CloudTrail. Pour plus d'informations à ce sujet, consultez la section Activation de la journalisation des CloudTrail événements pour les buckets et les objets S3 dans la documentation Amazon S3.	Architecte de solutions

Tâche	Description	Compétences requises
Configurez les politiques clés d'AWS KMS pour CloudTrail.	Automatisez la configuration des politiques clés d'AWS Key Management Service (AWS KMS) pour CloudTrail. Pour plus d'informations à ce sujet, consultez la section Configurer les politiques clés d'AWS KMS CloudTrail dans la CloudTrail documentation AWS.	Architecte de solutions
Chiffrez CloudTrail les journaux au repos.	Configurez le chiffrement des CloudTrail journaux côté serveur à l'aide des clés gérées par le client détenues dans AWS KMS. Pour plus d'informations à ce sujet, consultez la section Chiffrement des fichiers CloudTrail journaux avec des clés gérées par AWS KMS (SSE-KMS) dans la documentation AWS. CloudTrail	Architecte de solutions
Faites pivoter automatiq uement les touches KMS.	Configurez la rotation des clés AWS KMS. Pour plus d'informations à ce sujet, consultez Comment activer et désactiver la rotation automatique des clés dans la documentation AWS KMS.	Architecte de solutions

Tâche	Description	Compétences requises
Configurez CloudWatch les alarmes.	Configurez les CloudWatch alarmes Amazon déclenché es par des événements spécifiques. Par exemple, les demandes APIs ou l'utilisa tion non autorisées du compte root. Pour plus d'informations à ce sujet, consultez Comment recevoir des notifications lorsque les clés d'accès root de votre compte AWS sont utilisées sur le blog de sécurité AWS.	Architecte de solutions
Configurez les groupes de sécurité.	Configurez les groupes de sécurité pour vous assurer que le trafic entrant non restreint n'est pas autorisé sur les ports 22 et 3389.	Architecte de solutions
Activez la journalisation des flux VPC.	Capturez le trafic IP rejeté vers et depuis les interfaces réseau de votre cloud privé virtuel (VPC) et configurez-le CloudWatch pour le capturer. Pour plus d'informations à ce sujet, consultez la section Création d'un journal de flux dans la documentation Amazon VPC.	Architecte de solutions

Tâche	Description	Compétences requises
Modifiez le groupe de sécurité par défaut pour restreindre l'ensemble du trafic.	Modifiez le groupe de sécurité par défaut de chaque VPC afin que le trafic soit refusé par défaut et que l'accès soit explicitement accordé via vos groupes de sécurité. Pour plus d'informations à ce sujet, consultez la section Groupes de sécurité pour votre VPC dans la documentation Amazon VPC.	Architecte de solutions
Configurez les tables de routage entre les VPCs.	Configurez les tables de routage pour l'appairage VPC avec le moins d'accès nécessaire. Pour plus d'informations à ce sujet, consultez la section Mise à jour de vos tables de routage pour une connexion d'appairage VPC dans la documentation Amazon VPC.	Architecte de solutions

Activités de configuration pour la nouvelle infrastructure AWS

Tâche	Description	Compétences requises
Provisionnez l'infrastructure AWS.	Créez les comptes et les ressources AWS. Durée : deux semaines	DevOps ingénieur, architecte de solutions
Configurez DevOps des outils et des processus.	Configurez DevOps des outils et des procédures, tels	DevOps ingénieur, architecte de solutions

Tâche	Description	Compétences requises
	que des pipelines d'intégra tion continue et de livraison continue (CI/CD) et des cadres de test automatisés.	
Automatisez la migration des composants principaux.	Utilisez des modèles ou des scripts existants pour automatiser l'installation et la configuration des OpenText produits TeamSite, notamment LiveSite, OpenDeploy et MediaBin. Durée : Une semaine	DevOps ingénieur, architect e de solutions, OpenText responsable
Automatisez la migration de composants supplémentaires.	Analysez et automatisez la migration d'applications supplémentaires intégrées aux composants OpenText principaux (par exemple, des bases de données supplémen taires, des composants de communication, de surveilla nce ou de cache). Durée : deux semaines	DevOps ingénieur, architect e de solutions, OpenText responsable
Adaptez les composants de base.	Apportez les modifications nécessaires aux personnal isations des composants OpenText principaux (par exemple, les intégrations).	Architecte de solutions, OpenText responsable, OpenText développeur, développeur d'intégration tiers, développeur front-end

Tâche	Description	Compétences requises
Implémenter et configurer des services supplémentaires.	Fournissez, configurez et implémentez tous les nouveaux services AWS, tels que les fonctions AWS Lambda ou Amazon API Gateway.	DevOps ingénieur, Architecte de solutions, Développeur d'intégration tiers, Développeur front-end
Migrez ou refactorisez d'autres composants.	Migrez des composants supplémentaires, y compris toute refactorisation requise. Cela inclut les applications externes telles que les portails de reporting personnalisés ou les couches d'intégration d'API existantes.	DevOps ingénieur, Architecte de solutions, Développeur d'intégration tiers, Développeur front-end
Effectuer la migration dans un environnement de développement.	Activités de migration automatisées pour l'environnement de développement, notamment le provisionnement du système, la migration des données, la migration des applications, l'installation et la configuration.	DevOps ingénieur
Effectuez la migration dans l'environnement de production.	Activités de migration automatisées pour l'environnement de production, notamment le provisionnement du système, la migration des données, la migration des applications, l'installation et la configuration.	DevOps ingénieur

Activités de mise en réseau

Tâche	Description	Compétences requises
Définissez des blocs CIDR pour chaque VPC.	Définissez le bloc CIDR (Classless Inter-Domain Routing) (plage d'adresses IP et masque) pour chaque VPC autre que celui par défaut. Durée : Moins d'une semaine	DevOps ingénieur, architecte de solutions
Définissez des sous-réseaux et des zones de disponibilité.	Définissez les sous-réseaux et les zones de disponibilité utilisés dans chaque VPC autre que celui par défaut. Durée : Moins d'une semaine	DevOps ingénieur, architecte de solutions
Définissez les groupes de sécurité.	Définissez des groupes de sécurité et des règles de groupes de sécurité pour contrôler la sécurité des ressources AWS. Durée : Moins d'une semaine	DevOps ingénieur, architecte de solutions
Définissez le réseau ACLs.	Définissez les listes de contrôle d'accès réseau (ACLs) pour contrôler la sécurité aux limites des sous-réseaux. Durée : Moins d'une semaine	DevOps ingénieur, architecte de solutions

Migrer des bases de

Tâche	Description	Compétences requises
Préparez les bases de données sources.	Utilisez AWS DMS pour préparer chaque base de données source en vue d'une réplication continue vers le cloud AWS.	DevOps ingénieur, architecte de solutions
Créez les bases de données pour les composants OpenText principaux.	Créez les bases de données requises par Opentext TeamSite LiveSite, et les MediaBin composants. Assurez-vous que les utilisateurs et les droits d'accès sont correctement configurés conformément à la documentation OpenText d'installation.	Architecte de solutions, OpenText responsable, OpenText développeur
Copiez les données des serveurs de base de données source.	Automatisez le processus de copie des données pour les composants OpenText principaux du serveur de base de données source vers le serveur de base de données cible.	Architecte de solutions, OpenText responsable, OpenText développeur
Synchronisez les données des serveurs de base de données.	Automatisez le processus de synchronisation régulière des données entre les bases de données source et les bases de données cibles.	OpenText développeur

Activités de migration de contenu

Tâche	Description	Compétences requises
Copiez les magasins de OpenText TeamSite contenu.	Automatisez le processus de copie des magasins de contenu OpenText TeamSite du serveur source vers le OpenText TeamSite serveur cible.	Architecte de solutions, OpenText responsable, OpenText développeur
Cartographiez les utilisateurs et les groupes.	Mappage interne entre l' OpenText TeamSite utilisateur interne IDs et le système cible IDs.	OpenText plomb
Synchronisez les magasins de OpenText TeamSite contenu.	Automatisez le processus de synchronisation régulière des magasins de contenu source et cible. Ceci est mis en œuvre dans le cadre du processus de migration et d'assurance qualité.	OpenText développeur
Copiez les données des serveurs Web.	Automatisez le processus de copie des données des serveurs Web sources vers les serveurs Web cibles.	Architecte de solutions, OpenText responsable, OpenText développeur
Synchronisez les données du serveur Web.	Automatisez le processus de synchronisation régulière des données du serveur Web source et cible.	OpenText développeur
Copiez les données du système de fichiers du serveur Web.	Automatisez le processus de copie de contenu et d'autres ressources Web depuis le système de fichiers du serveur	Architecte de solutions, OpenText responsable, OpenText développeur

Tâche	Description	Compétences requises
	Web source vers les serveurs Web cibles.	
Synchronisez les systèmes de fichiers du serveur Web.	Automatisez le processus de synchronisation régulière du contenu et des autres ressources Web entre le système de fichiers du serveur Web source et les serveurs Web cibles.	OpenText développeur
Générez des flux et des index.	Automatisez le processus d'exécution de tous les processus qui génèrent des flux ou d'autres index (par exemple, la recherche sur le Web) qui utilisent OpenText TeamSite le contenu du serveur Web comme source de données.	Architecte de solutions, OpenText responsable, OpenText développeur
Synchronisez la génération des flux et des index.	Automatisez le processus de régénération régulière des flux et des index après les synchronisations de données.	OpenText développeur

Activités de test et d'assurance qualité

Tâche	Description	Compétences requises
Effectuez l'assurance qualité sur la migration.	Testez l'environnement, les applications et les services AWS cibles pour vous assurer que les processus de migration automatisés	DevOps ingénieur, OpenText responsable, testeur QA

Tâche	Description	Compétences requises
	sont correctement conçus et configurés.	
Procéder à des tests de performance.	Testez les performances en termes de réactivité et de stabilité sous une charge de travail particulière. Étudiez, mesurez, validez ou vérifiez d'autres attributs de qualité du système de destination, tels que l'évolutivité et la fiabilité. Pour que ce test soit utile, vous devez disposer d'un environnement de test de la même taille que votre environnement de production. Durée : Entre une et deux semaines	DevOps ingénieur, OpenText responsable

Tâche	Description	Compétences requises
Tests de sécurité.	Analyse des vulnérabilités et tests de pénétration pour révéler les failles potentielles des mécanismes de sécurité d'une application qui protègent les données et maintiennent les fonctionnalités selon les besoins. Pour que ce test soit utile, vous devez disposer d'un environnement de test équivalent à votre environne ment de production en termes de réseau et de sécurité. Durée : Entre une et deux semaines	DevOps ingénieur, OpenText responsable

Activités d'intégration opérationnelle

Tâche	Description	Compétences requises
Vérifiez l'état de préparation opérationnelle.	Découvrez comment vous effectuez actuellement les opérations informatiques et comment vous allez opérer dans le cloud AWS. Vous pouvez atteindre ce résultat commercial en définissant un modèle d'exploitation dans le cloud. Durée : Une semaine	DevOps ingénieur, OpenText responsable, responsable de la prestation de services

Tâche	Description	Compétences requises
Investissez dans l'automat isation des opérations.	Investissez dans l'automat isation pour mettre en place un modèle d'exploitation AWS.	DevOps ingénieur, OpenText responsable, responsable de la prestation de services
Intégrez les opérations.	Continuez à utiliser les outils informatiques actuels et étendez-les grâce à l'intégra tion au cloud AWS.	DevOps ingénieur, OpenText responsable, responsable de la prestation de services

Activités liées à la transition

Tâche	Description	Compétences requises
Changez de DNS.	Basculez manuellement le système de noms de domaine (DNS) des hôtes existants vers des hôtes basés dans le cloud AWS. Durée : Une heure	DevOps ingénieur, OpenText responsable
Testez la reprise après sinistre.	Testez la reprise après sinistre, la restauration des sauvegardes et exécutez vos tests automatisés. Durée : Un jour	DevOps ingénieur, OpenText responsable, testeur QA
Validez la surveillance et les analyses.	Vérifiez que la surveillance et les analyses fonctionnent. Durée : deux heures	DevOps ingénieur, OpenText responsable
Éteignez l'ancien environne ment et demandez l'arrêt du serveur.	Durée : Trois jours	DevOps ingénieur, OpenText responsable

Ressources connexes

- Politiques gérées par le client
- Création d'un utilisateur IAM dans votre compte AWS
- Groupes d'utilisateurs IAM
- Associer une politique à un groupe d'utilisateurs IAM
- Surveillance de votre utilisation et de vos coûts
- Gérer un compte AWS
- Rôles IAM pour Amazon EC2
- Autorisations d'accès pour AWS Support
- Utilisation de create-trail
- Activation de la validation de l'intégrité des fichiers journaux pour CloudTrail
- Politique relative aux compartiments Amazon S3 pour CloudTrail
- Envoyer des événements à CloudWatch Logs
- Configuration d'AWS Config avec l'interface de ligne de commande AWS
- Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3
- Configurer les politiques clés d'AWS KMS pour CloudTrail
- Chiffrement des fichiers CloudTrail journaux à l'aide des clés gérées par AWS KMS (SSE-KMS)
- Comment activer et désactiver la rotation automatique des touches
- Comment recevoir des notifications lorsque les clés d'accès root de votre compte AWS sont utilisées
- Création d'un journal de flux
- Groupes de sécurité pour votre VPC
- Mise à jour de vos tables de routage pour une connexion d'appairage VPC

Migrer les valeurs Oracle CLOB vers des lignes individuelles dans PostgreSQL sur AWS

Créée par Sai Krishna Namburu (AWS) et Sindhusha Paturu (AWS)

Récapitulatif

Ce modèle décrit comment diviser les valeurs CLOB (Character Large Object) Oracle en lignes individuelles dans Amazon Aurora PostgreSQL Compatible Edition et Amazon Relational Database Service (Amazon RDS) pour PostgreSQL. PostgreSQL ne prend pas en charge le type de données CLOB.

Les tables comportant des partitions par intervalles sont identifiées dans la base de données Oracle source, et le nom de la table, le type de partition, l'intervalle de la partition et les autres métadonnées sont capturés et chargés dans la base de données cible. Vous pouvez charger des données CLOB d'une taille inférieure à 1 Go dans les tables cibles sous forme de texte à l'aide d'AWS Database Migration Service (AWS DMS), ou vous pouvez exporter les données au format CSV, les charger dans un bucket Amazon Simple Storage Service (Amazon S3) et les migrer vers votre base de données PostgreSQL cible.

Après la migration, vous pouvez utiliser le code PostgreSQL personnalisé fourni avec ce modèle pour diviser les données CLOB en lignes individuelles en fonction du nouvel identifiant de caractère de ligne `CHR(10)` () et remplir la table cible.

Conditions préalables et limitations

Prérequis

- Table de base de données Oracle comportant des partitions d'intervalles et des enregistrements contenant des données de type CLOB.
- Une base de données compatible avec Aurora PostgreSQL ou Amazon RDS for PostgreSQL dotée d'une structure de table similaire à celle de la table source (mêmes colonnes et types de données).

Limites

- La valeur CLOB ne peut pas dépasser 1 Go.
- Chaque ligne de la table cible doit avoir un nouvel identifiant de caractère de ligne.

Versions du produit

- Oracle 12c
- Aurora Postgres 11.6

Architecture

Le schéma suivant montre une table Oracle source contenant des données CLOB et la table PostgreSQL équivalente dans la version 11.6 compatible avec Aurora PostgreSQL.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.
- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

Vous pouvez utiliser les outils clients suivants pour vous connecter, accéder et gérer vos bases de données compatibles Aurora PostgreSQL et Amazon RDS for PostgreSQL. (Ces outils ne sont pas utilisés dans ce modèle.)

- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.
- DBeaverest un outil de base de données open source destiné aux développeurs et aux administrateurs de bases de données. Vous pouvez utiliser cet outil pour manipuler, surveiller, analyser, administrer et migrer vos données.

Bonnes pratiques

Pour connaître les meilleures pratiques relatives à la migration de votre base de données d'Oracle vers PostgreSQL, consultez le billet de blog AWS intitulé Meilleures pratiques pour la migration d'une base de données Oracle vers Amazon RDS PostgreSQL ou Amazon Aurora PostgreSQL : considérations relatives au processus de migration et à l'infrastructure.

Pour connaître les meilleures pratiques de configuration de la tâche AWS DMS pour la migration d'objets binaires volumineux, consultez la section Migration d'objets binaires volumineux (LOBs) dans la documentation AWS DMS.

Épopées

Identifier les données CLOB

Tâche	Description	Compétences requises
Analysez les données CLOB.	Dans la base de données Oracle source, analysez les données CLOB pour voir si elles contiennent des en-têtes de colonne, afin de déterminer la méthode de chargement des données dans la table cible. Pour analyser les données d'entrée, utilisez la requête suivante. `SELECT * FROM clobdata_or;`	Developer
Chargez les données CLOB dans la base de données cible.	Migrez la table contenant des données CLOB vers une table intermédiaire (intermédiaire) dans la base de données cible Aurora ou Amazon RDS. Vous pouvez utiliser AWS DMS ou	Ingénieur de migration, DBA

Tâche	Description	Compétences requises
	télécharger les données sous forme de fichier CSV dans un compartiment Amazon S3. Pour plus d'informations sur l'utilisation d'AWS DMS pour cette tâche, consultez les sections Utilisation d'une base de données Oracle comme source et Utilisation d'une base de données PostgreSQL comme cible dans la documentation AWS DMS. Pour plus d'informations sur l'utilisation d'Amazon S3 pour cette tâche, consultez la section Utilisation d'Amazon S3 comme cible dans la documentation AWS DMS.	

Tâche	Description	Compétences requises

Validez la table PostgreSQL cible.	Validez les données cibles, y compris les en-têtes, par rapport aux données source en utilisant les requêtes suivantes dans la base de données cible.
	`SELECT * FROM clobdata_pg;`
	`SELECT * FROM clobdatatarget;`
	Comparez les résultats aux résultats des requêtes de la base de données source (dès la première étape).
		Developer

Divisez les données CLOB en lignes distinctes.	Exécutez le code PostgreSQL personnalisé fourni dans la section Informations supplémentaires pour diviser les données CLOB et les insérer dans des lignes distinctes dans la table PostgreSQL cible.	Developer

Validez les données.

Tâche	Description	Compétences requises
Validez les données de la table cible.	Validez les données insérées dans la table cible à l'aide des requêtes suivantes.	Developer

Tâche	Description	Compétences requises
	`SELECT * FROM clobdata_pg;` `SELECT * FROM clobdatatarget;`	

Ressources connexes

- Type de données CLOB (documentation Oracle)
- Types de données (documentation PostgreSQL)

Informations supplémentaires

Fonction PostgreSQL pour diviser les données CLOB

```
do
$$
declare
totalstr varchar;
str1 varchar;
str2 varchar;
pos1 integer := 1;
pos2 integer ;
len integer;


begin
        select rawdata||chr(10) into totalstr from clobdata_pg;
        len :=  length(totalstr) ;
        raise notice 'Total length : %',len;
        raise notice 'totalstr : %',totalstr;
        raise notice 'Before while loop';


        while pos1 < len  loop


                select position (chr(10) in totalstr) into pos2;
```

```
                 raise notice '1st position of new line : %',pos2;


                str1 := substring (totalstr,pos1,pos2-1);
                raise notice 'str1 : %',str1;


                   insert into clobdatatarget(data) values (str1);
                   totalstr := substring(totalstr,pos2+1,len);
                   raise notice 'new totalstr :%',totalstr;
                len :=  length(totalstr) ;


        end loop;
end
$$
LANGUAGE 'plpgsql' ;
```

Exemples d'entrée et de sortie

Vous pouvez utiliser les exemples suivants pour tester le code PostgreSQL avant de migrer vos données.

Créez une base de données Oracle avec trois lignes de saisie.

```
CREATE TABLE clobdata_or (
id INTEGER GENERATED ALWAYS AS IDENTITY,
rawdata clob  );


insert into clobdata_or(rawdata) values (to_clob('test line 1') || chr(10) ||
 to_clob('test line 2') || chr(10) || to_clob('test line 3') || chr(10));
COMMIT;


SELECT * FROM clobdata_or;
```

Cela affiche le résultat suivant.

id	données brutes
1	ligne de test 1 ligne de test 2 ligne de test 3

Chargez les données sources dans une table intermédiaire PostgreSQL `clobdata_pg` () pour les traiter.

```
SELECT * FROM clobdata_pg;

CREATE TEMP TABLE clobdatatarget (id1 SERIAL,data VARCHAR );

<Run the code in the additional information section.>

SELECT * FROM clobdatatarget;
```

Cela affiche le résultat suivant.

id1	data
1	ligne de test 1
2	ligne de test 2
3	ligne de test 3

Migrez une base de données Oracle sur site vers Amazon RDS for Oracle en utilisant directement Oracle Data Pump Import via un lien de base de données

Créée par Rizwan Wangde (AWS)

Récapitulatif

De nombreux modèles couvrent la migration de bases de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle à l'aide d'Oracle Data Pump, un utilitaire Oracle natif qui constitue le moyen préféré pour migrer de grandes charges de travail Oracle. Ces modèles impliquent généralement l'exportation de schémas ou de tables d'application dans des fichiers de vidage, le transfert des fichiers de vidage vers un répertoire de base de données sur Amazon RDS for Oracle, puis l'importation des schémas d'application et des données à partir des fichiers de vidage.

Avec cette approche, une migration peut prendre plus de temps en fonction de la taille des données et du temps nécessaire pour transférer les fichiers de vidage vers l'instance Amazon RDS. En outre, les fichiers de vidage se trouvent sur le volume Amazon Elastic Block Store (Amazon EBS) de l'instance Amazon RDS, qui doit être suffisamment grand pour contenir la base de données et les fichiers de vidage. Lorsque les fichiers de vidage sont supprimés après l'importation, l'espace vide ne peut pas être récupéré. Vous continuez donc à payer pour l'espace inutilisé.

Ce modèle atténue ces problèmes en effectuant une importation directe sur l'instance Amazon RDS à l'aide de l'API Oracle Data Pump (`DBMS_DATAPUMP`) via un lien de base de données. Le modèle lance un pipeline d'exportation et d'importation simultané entre les bases de données source et cible. Ce modèle ne nécessite pas de dimensionner un volume EBS pour les fichiers de vidage car aucun fichier de vidage n'est créé ou stocké sur le volume. Cette approche permet d'économiser le coût mensuel de l'espace disque inutilisé.

Conditions préalables et limitations

Prérequis

- Un compte Amazon Web Services (AWS) actif.
- Un cloud privé virtuel (VPC) configuré avec des sous-réseaux privés répartis sur au moins deux zones de disponibilité, afin de fournir l'infrastructure réseau pour l'instance Amazon RDS.
- Une base de données Oracle dans un centre de données sur site ou autogérée sur Amazon Elastic Compute Cloud (Amazon EC2).

- Une instance Amazon RDS pour Oracle existante dans une seule zone de disponibilité. L'utilisation d'une seule zone de disponibilité améliore les performances d'écriture lors de la migration. Un déploiement multi-AZ peut être activé 24 à 48 heures avant le passage au relais.

  Cette solution peut également utiliser Amazon RDS Custom for Oracle comme cible.
- AWS Direct Connect (recommandé pour les bases de données de grande taille).
- Les règles de connectivité réseau et de pare-feu sur site sont configurées pour autoriser une connexion entrante entre l'instance Amazon RDS et la base de données Oracle sur site.

Limites

- La limite de taille de base de données sur Amazon RDS for Oracle est de 64 tebioctets (TiB) en décembre 2022.
- La taille maximale d'un seul fichier sur une instance de base de données Amazon RDS for Oracle est de 16 TiB. Il est important de le savoir car vous devrez peut-être répartir les tables sur plusieurs tablespaces.

Versions du produit

- Base de données source : Oracle Database version 10g version 1 et versions ultérieures.
- Base de données cible : pour obtenir la dernière liste des versions et éditions prises en charge sur Amazon RDS, consultez Amazon RDS for Oracle dans la documentation AWS.

Architecture

Pile technologique source

- Base de données Oracle autogérée sur site ou dans le cloud

Pile technologique cible

- Amazon RDS pour Oracle ou Amazon RDS Custom pour Oracle

Architecture cible

Le schéma suivant montre l'architecture permettant de migrer d'une base de données Oracle sur site vers Amazon RDS for Oracle dans un environnement mono-AZ. Les flèches indiquent le flux de données dans l'architecture. Le schéma ne montre pas quel composant initie la connexion.

1. L'instance Amazon RDS for Oracle se connecte à la base de données Oracle source sur site pour effectuer une migration complète via le lien de base de données.
2. AWS Database Migration Service (AWS DMS) se connecte à la base de données Oracle source sur site pour effectuer une réplication continue à l'aide de la capture des données de modification (CDC).
3. Les modifications du CDC sont appliquées à la base de données Amazon RDS for Oracle.

Outils

Services AWS

- AWS Database Migration Service (AWS DMS) vous aide à migrer les banques de données vers AWS Cloud ou entre des combinaisons de configurations cloud et sur site. Ce modèle utilise le CDC et le paramètre Répliquer les données uniquement change.
- AWS Direct Connectrelie votre réseau interne à un AWS Direct Connect emplacement via un câble à fibre optique Ethernet standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement destinées au public Services AWS tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- Amazon Relational Database Service vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.

Autres outils

- Oracle Data Pump vous aide à déplacer des données et des métadonnées d'une base de données à une autre à grande vitesse.
- Les outils clients tels qu'Oracle Instant Client ou SQL Developer sont utilisés pour connecter et exécuter des requêtes SQL sur la base de données.

Bonnes pratiques

Bien qu'il AWS Direct Connect utilise des connexions réseau privées dédiées entre le réseau local AWS, envisagez les options suivantes pour renforcer la sécurité et le chiffrement des données en transit :

- Un réseau privé virtuel (VPN) utilisant AWS Site-to-Site VPN ou une connexion IPsec VPN entre le réseau local et le AWS réseau
- Chiffrement réseau natif de la base de données Oracle configuré sur la base de données Oracle locale
- Chiffrement à l'aide de TLS

Épopées

Préparation de la base de données Oracle source sur site

Tâche	Description	Compétences requises
Configurez la connectivité réseau entre la base de données cible et la base de données source.	Configurez le réseau et le pare-feu sur site pour autoriser la connexion entrante entre l'instance Amazon RDS cible et la base de données Oracle source sur site.	Administrateur réseau, ingénieur en sécurité

Créez un utilisateur de base de données doté des privilège s appropriés.	Créez un utilisateur de base de données dans la base de données Oracle source locale avec les privilèges nécessair es pour migrer les données entre la source et la cible à l'aide d'Oracle Data Pump :
	`GRANT CONNECT to <migration_user>;`
	`GRANT DATAPUMP_EXP_FULL_DATABASE to <migration_user>;`
		DBA

Tâche	Description	Compétences requises
	`GRANT SELECT ANY TABLE to <migration_user>;`	

Préparez la base de données source sur site pour la migration AWS DMS CDC.	(Facultatif) Préparez la base de données Oracle source sur site pour la migration AWS DMS CDC une fois le chargement complet d'Oracle Data Pump terminé :
	1. Configurez les privilège s supplémentaires requis pour gérer FLASHBACK lors de la migration d'Oracle Data Pump :
	`GRANT FLASHBACK ANY TABLE to <migratio n_user>;`
	`GRANT FLASHBACK ARCHIVE ADMINISTER to <migration_user>;`
	2. Pour configurer les privilège s de compte utilisateur requis sur une source Oracle autogérée pour AWS DMS, consultez la AWS DMS documentation.
	3. Pour préparer une base de données source autogérée Oracle à l'usage du CDC AWS DMS, consultez la AWS DMS documentation.
		DBA

Tâche	Description	Compétences requises
Installez et configurez SQL Developer.	Installez et configurez SQL Developer pour connecter et exécuter des requêtes SQL sur les bases de données source et cible.	DBA, ingénieur en migration
Générez un script pour créer les tablespaces.	Utilisez l'exemple de requête SQL suivant pour générer le script dans la base de données source : `SELECT 'CREATE TABLESPACE ' tablespace_name ' DATAFILE SIZE 1G AUTOEXTEND ON MAXSIZE UNLIMITED;' from dba_tablespaces where tablespace_name not in ('SYSTEM', 'SYSAUX','TEMP','UNDOTBS1') order by 1;` Le script sera appliqué à la base de données cible.	DBA

Tâche	Description	Compétences requises
Générez un script pour créer des utilisateurs, des profils, des rôles et des privilèges.	Pour générer un script permettant de créer les utilisateurs, les profils, les rôles et les privilèges de la base de données, utilisez les scripts du document de support Oracle How to Extract DDL for User including Privileges and Roles Using dbms_metadata.get_ddl (Doc ID 2739952.1) (compte Oracle requis). Le script sera appliqué à la base de données cible.	DBA

Préparez l'instance Amazon RDS for Oracle cible

Tâche	Description	Compétences requises
Créez un lien de base de données vers la base de données source et vérifiez la connectivité.	Pour créer un lien de base de données vers la base de données source locale, vous pouvez utiliser l'exemple de commande suivant : `CREATE DATABASE LINK link2src CONNECT TO <migration_user_account> IDENTIFIED BY <password> USING '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=<dns`	DBA

Tâche	Description	Compétences requises
	or ip address of remote db>) (PORT=<listener port>))(CONNECT_DATA=(SID=<remote SID>)))'; Pour vérifier la connectivité, exécutez la commande SQL suivante : select * from dual@link2src; La connectivité est réussie si la réponse l'estX.	
Exécutez les scripts pour préparer l'instance cible.	Exécutez les scripts générés précédemment pour préparer l'instance Amazon RDS for Oracle cible : 1. Espaces de table 2. Profils 3. Rôles Cela permet de garantir que la migration d'Oracle Data Pump peut créer les schémas et leurs objets.	DBA, ingénieur en migration

Effectuez une migration complète en utilisant Oracle Data Pump Import via un lien de base de données

Tâche	Description	Compétences requises
Migrez les schémas requis.	Pour migrer les schémas requis de la base de données source sur site vers l'instanc e Amazon RDS cible, utilisez le code de la section Informati ons supplémentaires : • Pour migrer un schéma unique, exécutez le code 1 dans la section Informations supplémentaires. • Pour migrer plusieurs schémas, exécutez le code 2 dans la section Informati ons supplémentaires. Pour optimiser les performan ces de la migration, vous pouvez ajuster le nombre de processus parallèles en exécutant la commande suivante : `DBMS_DATAPUMP.SET_ PARALLEL (handle => v_hdnl, degree => 4);`	DBA
Collectez des statistiques de schéma pour améliorer les performances.	La commande Gather Schema Statistics renvoie les statistiq ues de l'optimiseur de requêtes Oracle collectée s pour les objets de base	DBA

Tâche	Description	Compétences requises
	de données. À l'aide de ces informations, l'optimiseur peut sélectionner le meilleur plan d'exécution pour toute requête portant sur les objets suivants : `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');`	

Effectuez une migration à charge complète et une réplication CDC à l'aide d'Oracle Data Pump et AWS DMS

Tâche	Description	Compétences requises
Capturez le SCN sur la base de données Oracle locale source.	Capturez le numéro de modification du système (SCN) sur la base de données Oracle locale source. Vous utiliserez le SCN pour l'importation complète et comme point de départ pour la réplication CDC. Pour générer le SCN actuel sur la base de données source, exécutez l'instruction SQL suivante : `SELECT current_scn FROM V$DATABASE;`	DBA

Tâche	Description	Compétences requises
Effectuez la migration complète des schémas.	Pour migrer les schémas requis (`FULL LOAD`) de la base de données source sur site vers l'instance Amazon RDS cible, procédez comme suit : • Pour migrer un schéma unique, exécutez le code 3 depuis la section Informations supplémentaires. • Pour migrer plusieurs schémas, exécutez le code 4 dans la section Informations supplémentaires. Dans le code, remplacez `<CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>` par le SCN que vous avez capturé dans la base de données source : `DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value => <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>);` Pour optimiser les performances de la migration, vous pouvez ajuster le nombre de processus parallèles :	DBA

Tâche	Description	Compétences requises
	`DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);`	
Désactivez les déclencheurs dans les schémas migrés.	Avant de commencer la tâche AWS DMS réservée aux CDC, désactivez-les `TRIGGERS` sous les schémas migrés.	DBA
Collectez des statistiques de schéma pour améliorer les performances.	La commande Gather Schema Statistics renvoie les statistiques de l'optimiseur de requêtes Oracle collectées pour les objets de base de données : `EXECUTE DBMS_STATS.GATHER_SCHEMA_STATS(ownname => '<schema_name>');` À l'aide de ces informations, l'optimiseur peut sélectionner le meilleur plan d'exécution pour toute requête portant sur ces objets.	DBA

Tâche	Description	Compétences requises
AWS DMS À utiliser pour effectuer une réplication continue de la source vers la cible.	AWS DMS À utiliser pour effectuer une réplication continue de la base de données Oracle source vers l'instance Amazon RDS for Oracle cible. Pour plus d'informations, consultez la section Création de tâches pour une réplication continue à l'aide AWS DMS et le billet de blog How to work with native CDC support in AWS DMS.	DBA, ingénieur en migration

Passez à Amazon RDS for Oracle

Tâche	Description	Compétences requises
Activez Multi-AZ sur l'instance 48 heures avant le passage.	S'il s'agit d'une instance de production, nous recommandons d'activer le déploiement multi-AZ sur l'instance Amazon RDS afin de bénéficier des avantages de la haute disponibilité (HA) et de la reprise après sinistre (DR).	DBA, ingénieur en migration
Arrêtez la tâche AWS DMS uniquement sur le CDC (si le CDC était activé).	1. Assurez-vous que la latence source et la latence cible sur les CloudWatch métriques Amazon de la AWS DMS tâche indiquent 0 seconde.	DBA

Tâche	Description	Compétences requises
	2. Arrêtez la tâche AWS DMS uniquement sur le CDC.	
Activez les déclencheurs.	Activez celle `TRIGGERS` que vous avez désactivée avant la création de la tâche CDC.	DBA

Ressources connexes

AWS

- Préparation d'une base de données source autogérée Oracle pour le CDC à l'aide de AWS DMS
- Création de tâches pour une réplication continue à l'aide de AWS DMS
- Déploiements multi-AZ pour une haute disponibilité
- Comment travailler avec le support natif du CDC dans AWS DMS (article de blog)

Documentation Oracle

- POMPE DE DONNÉES DBMS

Informations supplémentaires

Code 1 : migration à chargement complet uniquement, schéma d'application unique

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')'); --
 To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
```

```
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Code 2 : migration à chargement complet uniquement, schémas d'applications multiples

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Code 3 : migration à chargement complet avant une tâche uniquement pour le CDC, schéma d'application unique

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN(operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE( handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER(v_hdnl,'SCHEMA_EXPR','IN (''<schema_name>'')');  --
 To migrate one selected schema
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
```

```
/
```

Code 4 : Migration à chargement complet avant une tâche uniquement sur le CDC, plusieurs schémas d'application

```
DECLARE
    v_hdnl NUMBER;
BEGIN
    v_hdnl := DBMS_DATAPUMP.OPEN (operation => 'IMPORT', job_mode  => 'SCHEMA',
 remote_link => '<DB LINK Name to Source Database>', job_name  => null);
    DBMS_DATAPUMP.ADD_FILE (handle => v_hdnl, filename  => 'import_01.log',  directory
 => 'DATA_PUMP_DIR', filetype  => dbms_datapump.ku$_file_type_log_file);
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'SCHEMA_LIST',
 '''<SCHEMA_1>'',''<SCHEMA_2>'', ''<SCHEMA_3>'''); -- To migrate multiple schemas
    DBMS_DATAPUMP.METADATA_FILTER (v_hdnl, 'EXCLUDE_PATH_EXPR','IN (''STATISTICS'')');
 -- To prevent gathering Statistics during the import
    DBMS_DATAPUMP.SET_PARAMETER (handle => v_hdnl, name => 'FLASHBACK_SCN', value =>
 <CURRENT_SCN_VALUE_IN_SOURCE_DATABASE>); -- SCN required for AWS DMS CDC only task.
    DBMS_DATAPUMP.SET_PARALLEL (handle => v_hdnl, degree => 4);  -- Number of parallel
 processes performing export and import
    DBMS_DATAPUMP.START_JOB(v_hdnl);
END;
/
```

Scénario dans lequel une approche de migration mixte peut mieux fonctionner

Dans de rares cas où la base de données source contient des tables comportant des millions de lignes et des colonnes LOBSEGMENT de très grande taille, ce modèle ralentira la migration. Oracle effectue la migration LOBSEGMENTs sur le lien réseau un par un. Il extrait une seule ligne (ainsi que les données de la colonne LOB) de la table source et insère la ligne dans la table cible, en répétant le processus jusqu'à ce que toutes les lignes soient migrées. Oracle Data Pump via le lien de base de données ne prend pas en charge les mécanismes de chargement groupé ou de chargement par chemin direct pour LOBSEGMENTs.

Dans ce cas, nous recommandons ce qui suit :

- Ignorez les tables identifiées lors de la migration d'Oracle Data Pump en ajoutant le filtre de métadonnées suivant :

```
dbms_datapump.metadata_filter(handle =>h1, name=>'NAME_EXPR', value => 'NOT IN
 (''TABLE_1'',''TABLE_2'')');
```

- Utilisez une AWS DMS tâche (migration à charge complète, avec réplication CDC si nécessaire) pour migrer les tables identifiées. AWS DMS extraira plusieurs lignes de la base de données Oracle source et les insérera par lots dans l'instance Amazon RDS cible, ce qui améliore les performances.

Migrer Oracle E-Business Suite vers Amazon RDS Custom

Créée par Simon Cunningham (AWS), Jaydeep Nandy (AWS), Nitin Saxena (AWS) et Vishnu Vinnakota (AWS)

Récapitulatif

Oracle E-Business Suite est une solution de planification des ressources d'entreprise (ERP) permettant d'automatiser les processus à l'échelle de l'entreprise tels que les finances, les ressources humaines, les chaînes d'approvisionnement et la fabrication. Il possède une architecture à trois niveaux : client, application et base de données. Auparavant, vous deviez exécuter votre base de données Oracle E-Business Suite sur une instance Amazon Elastic Compute Cloud EC2 (Amazon) autogérée, mais vous pouvez désormais bénéficier d'Amazon Relational Database Service (Amazon RDS) Custom.

Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents. Il automatise les tâches et les opérations d'administration des bases de données tout en vous permettant, en tant qu'administrateur de base de données, d'accéder à votre environnement de base de données et de votre système d'exploitation et de les personnaliser. Lorsque vous migrez votre base de données Oracle vers Amazon RDS Custom, Amazon Web Services (AWS) prend en charge les tâches les plus lourdes, telles que les tâches de sauvegarde et garantit la haute disponibilité, tandis que vous pouvez vous concentrer sur la maintenance de l'application et des fonctionnalités de votre suite Oracle E-Business. Pour connaître les principaux facteurs à prendre en compte lors d'une migration, consultez les stratégies de migration des bases de données Oracle dans AWS Prescriptive Guidance.

Ce modèle se concentre sur les étapes de migration d'une base de données Oracle autonome sur Amazon EC2 vers Amazon RDS Custom en utilisant une sauvegarde Oracle Recovery Manager (RMAN) et un système de fichiers partagé Amazon Elastic File System (Amazon EFS) entre l'instance EC2 et Amazon RDS Custom. Le modèle utilise une sauvegarde complète RMAN (parfois appelée sauvegarde de niveau 0). Pour des raisons de simplicité, il utilise une sauvegarde à froid dans laquelle l'application est arrêtée et la base de données est montée et non ouverte. (Vous pouvez également utiliser Oracle Data Guard ou la duplication RMAN pour la sauvegarde. Toutefois, ce modèle ne couvre pas ces options.)

Pour plus d'informations sur l'architecture d'Oracle E-Business Suite sur AWS pour une haute disponibilité et une reprise après sinistre, consultez le modèle Configurer une architecture HA/DR

pour Oracle E-Business Suite sur Amazon RDS Custom avec une base de données de secours active.

> **Note**
>
> Ce modèle fournit des liens vers les notes de support Oracle. Vous avez besoin d'un compte Oracle Support pour accéder à ces documents.

Conditions préalables et limitations

Prérequis

- Une base de données source Oracle version 12.1.0.2 ou 19c (minimum 19.3) exécutée sur Amazon EC2 avec Oracle Linux 7 ou Red Hat Enterprise Linux (RHEL) version 7.x. Ce modèle suppose que le nom de la base de données source est `VIS` et que le nom de la base de données conteneur supplémentaire pour Oracle 19c l'est`VISCDB`, mais vous pouvez utiliser d'autres noms.

  > **Note**
  >
  > Vous pouvez également utiliser ce modèle avec les bases de données source Oracle locales, à condition de disposer de la connectivité réseau appropriée entre le réseau local et Amazon Virtual Private Cloud (Amazon VPC).

- Une application Oracle E-Business Suite version 12.2.x (instance de vision). Cette procédure a été testée sur la version 12.2.11.
- Un seul niveau d'application Oracle E-Business Suite. Toutefois, vous pouvez adapter ce modèle pour qu'il fonctionne avec plusieurs niveaux d'application.
- Pour Oracle 12.1.0.2, Amazon RDS Custom est configuré avec au moins 16 Go d'espace de swap. Dans le cas contraire, le CD 12c Examples affiche un avertissement. (Oracle 19c ne nécessite pas le CD d'exemples, comme indiqué plus loin dans ce document.)

Effectuez les étapes suivantes avant de commencer votre migration :

1. Sur la console Amazon RDS, créez une instance de base de données Amazon RDS personnalisée pour Oracle avec le nom de la base de données `VIS` (ou le nom de votre base de données source). Pour obtenir des instructions, consultez Working with Amazon RDS Custom dans la documentation AWS et le billet de blog Amazon RDS Custom for Oracle — New Control

Capabilities in Database Environment. Cela garantit que le nom de la base de données est le même que celui de la base de données source. (Si ce champ est laissé vide, le nom de l' EC2 instance et de la base de données sera défini sur`ORCL`.) Assurez-vous de créer votre version de moteur personnalisée (CEV) avec au minimum les correctifs qui ont été appliqués à la source. Pour plus d'informations, consultez la section Préparation à la création d'un CEV dans la documentation Amazon RDS.

Remarque pour Oracle 19c : Actuellement, pour Oracle 19c, le nom de la base de données de conteneurs Amazon RDS peut être personnalisé. L'argument par défaut est `RDSCDB`. Assurez-vous de créer l'instance Oracle personnalisée RDS avec le même ID système (SID) que sur l' EC2 instance source. Par exemple, dans ce modèle, le SID Oracle 19c est supposé se trouver `VISCDB` sur l'instance source. Par conséquent, le SID Oracle 19c cible sur Amazon RDS Custom doit également l'être. `VISCDB`

2. Configurez l'instance de base de données personnalisée Amazon RDS avec suffisamment de stockage, de vCPU et de mémoire pour correspondre à la base de données source EC2 Amazon. Pour ce faire, vous pouvez faire correspondre les types d' EC2 instances Amazon en fonction du vCPU et de la mémoire.
3. Créez un système de fichiers Amazon EFS et installez-le sur les instances personnalisées Amazon EC2 et Amazon RDS. Pour obtenir des instructions, consultez le billet de blog sur l'intégration d'Amazon RDS Custom pour Oracle à Amazon EFS. Ce modèle suppose que vous avez monté le volume Amazon EFS à la fois `/RMAN` sur les instances de base de données personnalisées Amazon RDS source EC2 et cible, et que la connectivité réseau est possible entre la source et la cible. Vous pouvez également utiliser la même méthode en utilisant Amazon FSx ou n'importe quel lecteur partagé.

Hypothèses

Ce modèle suppose que votre application et votre base de données utilisent des noms d'hôte logiques, ce qui réduit le nombre d'étapes de migration. Vous pouvez ajuster ces étapes pour utiliser des noms d'hôtes physiques, mais les noms d'hôtes logiques réduisent la complexité du processus de migration. Pour plus d'informations sur les avantages liés à l'utilisation de noms d'hôtes logiques, consultez les notes d'assistance suivantes :

- Pour 12c, note de support Oracle 2246690.1
- Pour 19c, note de support Oracle 2617788.1

Ce modèle ne couvre pas le scénario de mise à niveau d'Oracle 12c vers 19c et se concentre sur la migration de la même version de la base de données Oracle exécutée sur Amazon vers EC2 Amazon RDS Custom for Oracle.

Amazon RDS Custom pour Oracle prend en charge la personnalisation d'Oracle Home. (Oracle Home stocke les fichiers binaires Oracle.) Vous pouvez remplacer le chemin par défaut par un chemin que vous spécifiez, tel que `/d01/oracle/VIS/19c`. `/rdsdbbin/oracle` Pour des raisons de simplicité, les instructions de ce modèle utilisent le chemin par défaut `/rdsdbbin/oracle`.

Limites

Ce modèle ne prend pas en charge les fonctionnalités et configurations suivantes :

- Définition du `ARCHIVE_LAG_TARGET` paramètre de base de données sur une valeur située en dehors de la plage de 60 à 7 200
- Désactivation du mode journal de l'instance de base de données () `NOARCHIVELOG`
- Désactiver l'`EBS-optimized`attribut de l' EC2 instance
- Modification des volumes Amazon Elastic Block Store (Amazon EBS) originaux attachés à l'instance EC2
- Ajouter de nouveaux volumes EBS ou modifier le type de volume de `gp2` `gp3`
- Support pour le fichier TNS
- Modification de l'`control_file`emplacement et du nom (cela doit être le cas `/rdsdbdata/db/VISCDB_A/controlfile/control-01.ctl`, où `VISCDB` est le nom du CDB)

Pour plus d'informations sur ces configurations et sur d'autres configurations non prises en charge, consultez la section Corriger les configurations non prises en charge dans la documentation Amazon RDS.

Versions du produit

Pour les versions de base de données Oracle et les classes d'instances prises en charge par Amazon RDS Custom, consultez Disponibilité et exigences relatives à Amazon RDS Custom pour Oracle.

Architecture

Le schéma d'architecture suivant représente un système Oracle E-Business Suite exécuté dans une seule zone de disponibilité sur AWS. Le niveau application est accessible via un Application

Load Balancer, l'application et les bases de données se trouvent dans des sous-réseaux privés, et le niveau Amazon RDS Custom et Amazon EC2 Database utilise un système de fichiers partagé Amazon EFS pour stocker et accéder aux fichiers de sauvegarde RMAN.

Outils

Services AWS

- Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents. Il automatise les tâches et les opérations d'administration des bases de données tout en vous permettant, en tant qu'administrateur de base de données, d'accéder à votre environnement de base de données et de votre système d'exploitation et de les personnaliser.
- Amazon Elastic File System (Amazon EFS) est un système de fichiers élastique simple, sans serveur, qui permet d'ajouter et de supprimer des fichiers sans qu'il soit nécessaire de les gérer ou de les approvisionner. Ce modèle utilise un système de fichiers partagé Amazon EFS pour stocker et accéder aux fichiers de sauvegarde RMAN.
- AWS Secrets Manager est un service géré par AWS qui vous permet de transférer, de gérer et de récupérer facilement des informations d'identification de base de données, des clés d'API et d'autres informations secrètes. Amazon RDS Custom stocke la paire de clés et les informations d'identification de l'utilisateur de la base de données dans Secrets Manager lors de la création de la base de données. Dans ce modèle, vous récupérez les mots de passe des utilisateurs de la base de données à partir de Secrets Manager pour créer les `ADMIN` utilisateurs `RDSADMIN` et pour modifier les mots de passe système et système.

Autres outils

- RMAN est un outil qui fournit un support de sauvegarde et de restauration pour les bases de données Oracle. Ce modèle utilise RMAN pour effectuer une sauvegarde à froid de la base de données Oracle source sur Amazon EC2 qui est restaurée sur Amazon RDS Custom.

Bonnes pratiques

- Utilisez des noms d'hôtes logiques. Cela réduit considérablement le nombre de scripts post-clonage que vous devez exécuter. Pour plus d'informations, consultez la note de support Oracle 2246690.1.
- Amazon RDS Custom utilise Oracle Automatic Memory Management (AMM) par défaut. Si vous souhaitez utiliser le noyau hugemem, vous pouvez configurer Amazon RDS Custom pour qu'il utilise plutôt la gestion automatique de la mémoire partagée (ASMM).
- Laissez le `memory_max_target` paramètre activé par défaut. Le framework utilise ce paramètre en arrière-plan pour créer des répliques de lecture.
- Activez la base de données Oracle Flashback. Cette fonctionnalité est utile dans les scénarios de test de basculement (et non de commutation) afin de rétablir le mode veille.
- Pour les paramètres d'initialisation de la base de données, personnalisez le PFILE standard fourni par l'instance de base de données personnalisée Amazon RDS pour Oracle E-Business Suite au lieu d'utiliser le SPFILE de la base de données source Oracle. Cela est dû au fait que les espaces blancs et les commentaires posent problème lors de la création de répliques de lecture dans Amazon RDS Custom. Pour plus d'informations sur les paramètres d'initialisation de la base de données, consultez la note de support Oracle 396009.1.

Dans la section Epics suivante, nous avons fourni des instructions distinctes pour Oracle 12.1.0.2 et 19c, où les détails diffèrent.

Épopées

Arrêtez l'application source

Tâche	Description	Compétences requises

Arrêtez l'application.	Pour arrêter l'application source, utilisez les commandes suivantes :
	`$ su - applmgr`
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adstpall.sh`
		DBA

Tâche	Description	Compétences requises
Créez le fichier .zip.	Créez le `appsutil.zip` fichier au niveau de l'applica tion source. Vous utilisere z ce fichier ultérieurement pour configurer le nœud de base de données personnalisé Amazon RDS. `$ perl $AD_TOP/bin/ admkappsutil.pl`	DBA
Copiez le fichier .zip dans Amazon EFS.	Copiez `appsutil.zip` depuis `$INST_TOP/admin/ out` votre volume Amazon EFS partagé (`/RMAN/app sutil`). Vous pouvez transférer le fichier manuellem ent à l'aide d'une copie sécurisée (SCP) ou d'un autre mécanisme de transfert.	DBA

Pré-clonez la base de données source

Tâche	Description	Compétences requises

Pré-clonez le niveau de base de données sur Amazon EC2.	Connectez-vous en tant qu'utilisateur Oracle et exécutez :
	`$ cd $ORACLE_HOME/appsu til/scripts/$CONTE XT_NAME`
	`$ perl adpreclone.pl dbTier`
		DBA

Tâche	Description	Compétences requises
	Vérifiez le fichier journal généré pour confirmer que l'opération s'est terminée correctement.	

Copiez le fichier appsutil.zip dans le système de fichiers Amazon EFS partagé.	Créez une sauvegarde tar et `$ORACLE_HOME/appsutil` copiez-la dans le système de fichiers Amazon EFS partagé (par exemple,`/RMAN/appsutil`) :
	`$ cd $ORACLE_HOME`
	`$ tar cvf sourceappsutil.tar appsutil`
	`$ cp sourceappsutil.tar /RMAN/appsutil`
		DBA

Effectuez une sauvegarde complète RMAN à froid de la base de données Amazon EC2 source

Tâche	Description	Compétences requises
Créez un script de sauvegarde.	Effectuez une sauvegarde complète RMAN de la base de données source sur le système de fichiers Amazon EFS partagé. Pour des raisons de simplicité, ce modèle effectue une sauvegarde RMAN à froid. Vous pouvez toutefois modifier ces étapes pour effectuer une sauvegarde RMAN à chaud	DBA

Tâche	Description	Compétences requises

	avec Oracle Data Guard afin de réduire les temps d'arrêt.
	
	1. Démarrez la base de EC2 données Amazon source en mode montage :
	
	`$ sqlplus / as sysdba`
	`$ SQL> shutdown immediate`
	`$ SQL> startup mount`
	
	2. Créez un script de sauvegarde RMAN (utilisez l'un des exemples suivants, selon votre version d'Oracle, ou exécutez l'un de vos scripts RMAN existants) pour sauvegarder la base de données sur le système de fichiers Amazon EFS que vous avez monté (`/RMAN`dans cet exemple).
	
	Pour Oracle 12.1.0.2 :
	
	`$ vi FullRMANColdBackup.sh`
	`#!/bin/bash`
	`. /home/oracle/.bash_profile`
	
	`export ORACLE_SID=VIS`
	`export ORACLE_HOME=/d01/oracle/VIS/12.1.0`
	`export DATE=$(date +%y-%m-%d_%H%M%S)`	

Tâche	Description	Compétences requises

	rman target / log=/RMAN /VISDB_${DATE}.log << EOF
	run
	{
	allocate channel ch1 device type disk format '/RMAN/visdb_full_bkp_%u';
	allocate channel ch2 device type disk format '/RMAN/visdb_full_bkp_%u';
	crosscheck backup;
	delete noprompt obsolete;
	BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG;
	backup archivelog all;
	release channel ch1;
	release channel ch2;
	}
	EOF
	
	Pour Oracle 19c :
	
	$ vi FullRMANColdBackup.sh
	#!/bin/bash
	. /home/oracle/.bash_profile
	
	export ORACLE_SID=VISCDB
	export ORACLE_HOME=/d01/oracle/VIS/19c
	export DATE=$(date +%y-%m-%d_%H%M%S)	

Tâche	Description	Compétences requises
	`rman target / log=/RMAN /VISDB_${DATE}.log << EOF run { allocate channel ch1 device type disk format '/RMAN/visdb_full_ bkp_%u'; allocate channel ch2 device type disk format '/RMAN/visdb_full_ bkp_%u'; crosscheck backup; delete noprompt obsolete; BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG; backup archivelog all; backup current controlfile format '/ RMAN/cntrl.bak'; release channel ch1; release channel ch2; } EOF`	
Exécutez le script de sauvegarde.	Modifiez les autorisations, connectez-vous en tant qu'utilisateur Oracle et exécutez le script : `$ chmod 755 FullRMANC oldBackup.sh $ ./FullRMANColdBack up.sh`	DBA

Tâche	Description	Compétences requises

Vérifiez les erreurs et notez le nom du fichier de sauvegarde.	Vérifiez la présence d'erreurs dans le fichier journal RMAN. Si tout semble correct, listez la sauvegarde du fichier de contrôle. Notez le nom du fichier de sortie.
	
	Pour Oracle 12.1.0.2 :
	
	`RMAN> connect target /`
	
	`RMAN> list backup of controlfile;`
	
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`------- ---- -- ---------- --------- -- ------------ ---------- DISK 00:00:04 23-APR-22`
	`9 Full 1.11M DISK 00:00:04 23-APR-22`
	`BP Key: 9 Status: AVAILABLE Compressed: YES Tag: TAG20220423T121011`
	`Piece Name: /RMAN/visdb_full_bkp_100rlsbt`
	`Control File Included: Ckp SCN: 122045953 96727 Ckp time: 23-APR-22`
	
	Vous utiliserez le fichier de sauvegarde `/RMAN/visdb_full_bkp_100rls`
		DBA

Tâche	Description	Compétences requises

	`bt` ultérieurement, lorsque vous restaurez la base de données sur Amazon RDS Custom.
	
	Pour Oracle 19c :
	
	`RMAN> connect target /`
	
	`RMAN> list backup of controlfile;`
	
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`------- ---- -- ---------- --------- ---------- ---------- ---

Configuration de la base de données personnalisée Amazon RDS cible

Tâche	Description	Compétences requises

Modifiez le fichier hosts et définissez le nom d'hôte.	**Note**
	Les commandes de cette section doivent être exécutées en tant qu'utilisateur root.
	
	1. Modifiez le `/etc/hosts` fichier sur l'instance de base de données personnalisée Amazon RDS. Pour ce faire, une méthode simple consiste à copier les entrées de la base de données et de l'hôte de l'application à partir du fichier source des hôtes EC2 de base de données Amazon.
	
	`<IP-address> OEBS-app01.localdomain OEBS-app01 OEBS-app01log.localdomain OEBS-app01log`
	`<IP-address> OEBS-db01.localdomain OEBS-db01 OEBS-db01log.localdomain OEBS-db01log`
	
	où se `<IP-address>` trouve l'adresse IP du nœud de base de données, que vous devez remplacer par l'adresse IP personnalisée Amazon RDS.
		DBA

Tâche	Description	Compétences requises

	Les noms d'hôtes logiques sont ajoutés à. `*log`
	
	2. Modifiez le nom d'hôte de la base de données en exécutant la `hostnamectl` commande suivante :
	
	`$ sudo hostnamectl set-hostname --static persistent-hostname`
	
	Par exemple :
	
	`$ sudo hostnamectl set-hostname --static OEBS-db01log`
	
	Pour plus d'informations, consultez l'article du centre de connaissances sur l'attribution de noms d'hôtes statiques.
	
	3. Redémarrez l'instance de base de données personnalisée Amazon RDS. Ne vous inquiétez pas de fermer la base de données, car vous la supprimerez ultérieurement.
	
	`$ reboot`
	
	4. Lorsque l'instance de base de données personnalisée Amazon RDS revient,	

Tâche	Description	Compétences requises

	connectez-vous et vérifiez que le nom d'hôte a changé :
	
	`$ hostname`
	`oebs-db01`	

Tâche	Description	Compétences requises

Installez le logiciel Oracle E-Business Suite.	Installez la suite Oracle E-Business recommandée sur le site RPMs d'origine d'Oracle sur l'instance de base de données personnalisée Amazon RDS. Pour plus de détails, consultez la note de support Oracle #1330701 .1. Voici une liste partielle. La liste des RPM change pour chaque version. Vérifiez donc que tous les fichiers requis RPMs sont installés.
	
	En tant qu'utilisateur root, exécutez :
	
	`$ sudo yum -y update`
	`$ sudo yum install -y elfutils-libelf-devel*`
	`$ sudo yum install -y libXp-1.0.2-2.1*.i686`
	`$ sudo yum install -y libXp-1.0.2-2.1*`
	`$ sudo yum install -y compat-libstdc++-*`
	
	Vérifiez que tous les correctifs requis sont installés avant de passer à l'étape suivante.
		DBA

Tâche	Description	Compétences requises

Installez le serveur VNC.	**Note**
	Vous pouvez omettre cette étape pour Oracle 19c car le CD Examples n'est plus nécessaire ; consultez la note de support Oracle 2782085.1.
	
	Pour Oracle 12.1.0.2 :
	
	Installez le serveur VNC et ses packages de bureau dépendants. Il s'agit d'une condition requise pour installer le CD d'exemples 12c à l'étape suivante.
	
	1. En tant qu'utilisateur root, exécutez :
	
	`$ sudo yum install -y tigervnc-server`
	`$ sudo yum install -y *kde*`
	`$ sudo yum install -y *xorg*`
	
	2. Démarrez le serveur VNC pour `rdsdb` l'utilisateur et définissez le mot de passe pour VNC :
	
	`$ su - rdsdb`
		DBA

Tâche	Description	Compétences requises

	``
	$ vncserver :1
	$ vncpassword
	``	

Tâche	Description	Compétences requises

Installez le CD 12c Examples.	**Note**
	Vous pouvez omettre cette étape pour Oracle 19c car le CD Examples n'est plus nécessaire ; consultez la note de support Oracle 2782085.1.
	
	Pour Oracle 12.1.0.2 :
	
	1. Téléchargez les fichiers d'installation depuis https://edelivery.oracle.com/. Pour Oracle E-Business Suite 12.2.11 — Oracle Database 12c version 1 (12.1.0.2), recherchez Examples for Linux x86-64 V100102-01.zip.
	
	2. Créez un répertoire pour stocker le CD Examples :
	
	`$ mkdir /RMAN/12c examples`
	
	3. Copiez le fichier .zip du CD Examples dans ce répertoire en utilisant le mécanisme de transfert de votre choix (par exemple, SCP) :
	
	`V100102-01.zip`
		DBA

Tâche	Description	Compétences requises

	4. Changez de propriétaire pour `rdsdb` :
	`$ chown -R rdsdb:rdsdb /RMAN/12cexamples`
	5. En tant qu'`rdsdb`utilisateur, décompressez le fichier :
	`$ unzip V10010201.zip`
	6. Connectez-vous depuis un client ayant accès au client VNC et à Amazon RDS Custom. Assurez-vous que la connectivité réseau et les ports de pare-feu nécessaires sont ouverts pour autoriser l'accès à VNC. Par exemple, un serveur VNC en cours d'exécution `display :1` aura besoin de l'ouverture du port 5901 sur le groupe de sécurité associé à l'hôte Amazon RDS Custom. EC2
	7. Accédez au répertoire dans lequel vous avez copié le CD Examples :
	`$ cd /RMAN/12cexamples/examples`
	8. Exécutez le programme d'installation. Assurez-vous	

Tâche	Description	Compétences requises

	de vérifier l'emplacement du `oraInst.loc` fichier.
	
	`./runInstaller -invPtrLoc /rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInst.loc`
	
	9. Utilisez les paramètres suivants lors de l'installation du CD Examples :
	
	`Skip Software Update Downloads`
	`Select Oracle Home 12.1.0.2 (Oracle Base = /rdsdbbin)`
	`(Software Location = /rdsdbbin/oracle/12.1.custom.r1.EE.1)`
	
	10. Le programme d'installation comprend cinq étapes accompagnées d'instructions. Suivez les étapes jusqu'à ce que l'installation soit terminée.	

Supprimez la base de données de départ et créez les répertoires pour stocker les fichiers de base de données

Tâche	Description	Compétences requises
Suspendez le mode d'automatisation.	Vous devez suspendre le mode d'automatisation sur votre instance de base de	DBA

Tâche	Description	Compétences requises
	données personnalisée Amazon RDS avant de passer aux étapes suivantes, afin de vous assurer que l'automat isation n'interfère pas avec l'activité RMAN. Interrompez l'automatisation à l'aide de la commande AWS Command Line Interface (AWS CLI) suivante. (Assurez-vous d'avoir d'abord configuré l'AWS CLI.) `aws rds modify-db-instance \ --db-instance-id entifier VIS \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Lorsque vous spécifiez la durée de la pause, assurez-vous de laisser suffisamment de temps pour la restaurat ion RMAN. Cela dépend de la taille de la base de données source. Modifiez donc la valeur 360 en conséquence.	

Tâche	Description	Compétences requises

Supprimez la base de données de départ.	Supprimez la base de données personnalisée Amazon RDS existante.
	
	En tant qu'utilisateur d'Oracle Home, exécutez les commandes suivantes. (L'utilisateur par défaut est `rdsdb`, sauf si vous l'avez personnalisé.)
	
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup nomount restrict;`
	`SQL> alter database mount;`
	`SQL> drop database;`
	`SQL> exit`
		DBA

Tâche	Description	Compétences requises

Créez des répertoires pour stocker les fichiers de base de données.	Pour Oracle 12.1.0.2 :
	
	Créez des répertoires pour la base de données, le fichier de contrôle, les fichiers de données et le journal en ligne. Utilisez le répertoire parent du `control_files` paramètre dans la commande précédent e (dans ce cas,`VIS_A`). Exécutez les commandes suivantes en tant qu'utilis ateur d'Oracle Home (par défaut,`rdsdb`).
	
	`$ mkdir -p /rdsdbdata/db/VIS_A/controlfile`
	`$ mkdir -p /rdsdbdata/db/VIS_A/datafile`
	`$ mkdir -p /rdsdbdata/db/VIS_A/onlinelog`
	
	Pour Oracle 19c :
	
	Créez des répertoires pour la base de données, le fichier de contrôle, les fichiers de données et le journal en ligne. Utilisez le répertoire parent du `control_files` paramètre dans la commande précédent e (dans ce cas,`VISCDB_A`). Exécutez les commandes suivantes en tant qu'utilis ateur d'Oracle Home (par défaut,`rdsdb`).
		DBA

Tâche	Description	Compétences requises

	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/controlfile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/datafile`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog`
	`$ mkdir -p /rdsdbdata/db/cdb/VISCDB_A/onlinelog/arch`
	`$ mkdir /rdsdbdata/db/pdb/VISCDB_A`	

Tâche	Description	Compétences requises
Créez et modifiez le fichier de paramètres pour Oracle E-Business Suite.	Au cours de cette étape, vous ne copierez pas le fichier de paramètres du serveur (SPFILE) depuis la base de données source. Vous utiliserez plutôt le fichier de paramètres standard (PFILE) créé avec l'instance de base de données personnalisée Amazon RDS et ajouterez les paramètres dont vous avez besoin pour Oracle E-Business Suite. Lorsque vous supprimez la base de données, Amazon RDS Automation crée une sauvegarde du `init.ora` fichier, qui est associée à la base de données personnalisée Amazon RDS. Ce fichier est appelé `oracle_pfile` et se trouve dans `/rdsdbdata/config` . Pour Oracle 12.1.0.2 : 1. Copiez `/rdsdbdata/config/oracle_pfile` dans `$ORACLE_HOME` . `$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVIS.ora` 2. Modifiez le `initVIS.ora` fichier sur l'instance de base	DBA

Tâche	Description	Compétences requises

	de données personnalisée Amazon RDS. Validez tous les paramètres de la source et ajoutez les paramètres nécessaires. Pour plus de détails, consultez la note de support Oracle 396009.1.
	
	⚠ Important
	Assurez-vous qu'il n'y a aucun commentaire dans les paramètres que vous ajoutez. Les commentaires peuvent entraîner des problèmes d'automatisation, tels que la création de répliques de lecture et l'émission de point-in-time récupérations ()PITRs.
	
	3. Ajoutez au `initVIS.ora` fichier des paramètres similaires aux suivants, en fonction de vos besoins :
	
	`*.workarea_size_policy='AUTO'`
	`*.plsql_code_type='INTERPRETED'`
	`*.cursor_sharing='EXACT'`	

Tâche	Description	Compétences requises
	*._b_tree_bitmap_plans=FALSE *.session_cached_cursors=500 *.optimizer_adaptive_features=false *.optimizer_secure_view_merging=false *.SQL92_SECURITY=TRUE *.temp_undo_enabled=true _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_characters = "." nls_comp = binary nls_sort = binary nls_date_format = DD-MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_elimination_cost_ratio =5 _like_with_bind_as_equality = TRUE _fast_full_scan_enabled = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view_merging = FALSE _optimizer_autostats_job = FALSE parallel_max_servers = 8 parallel_min_servers = 0	

Tâche	Description	Compétences requises
	parallel_degree_policy = MANUAL sec_case_sensitive_logon = FALSE compatible = 12.1.0 o7_dictionary_accessibility = FALSE utl_file_dir =/tmp 4. Modifier ce qui suit. Les valeurs dépendront de votre système source, alors révisez-les en fonction de votre configuration actuelle. *.open_cursors=500 *.undo_tablespace='APPS_UNDOTS1 5. Supprimez la référence SPFILE. *.spfile='/rdsdbbin/oracle/dbs/spfileVIS.ora' Remarques : • Ne modifiez pas les valeurs fournies par le fichier PFILE personnalisé Amazon RDS pour `control_files` et. `db_unique_name` Amazon RDS attend ces valeurs. Si vous vous en écartez, des problèmes se poseront si vous essayez	

Tâche	Description	Compétences requises

	de créer une réplique en lecture à l'avenir.
	• Amazon RDS Custom utilise la gestion automatique de la mémoire (AMM) par défaut. Si vous souhaitez utiliser hugemem, vous pouvez configurer Amazon RDS Custom pour utiliser la gestion automatique de la mémoire partagée (ASMM).
	• Laissez le `memory_max_target` paramètre activé par défaut. Le framework Amazon RDS l'utilise en arrière-plan pour créer des répliques de lecture.
	6. Vérifiez que le `initVIS.ora` fichier ne présente aucun problème en exécutant la `startup nomount` commande suivante :
	`SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVIS.ora;`
	`SQL> create spfile='/rdsdbdata/admin/VIS/pfile/spfileVIS.ora' from pfile;`
	`SQL> exit`	

Tâche	Description	Compétences requises

	7. Créez un lien symbolique pour SPFILE.
	`$ ln -s /rdsdbdata/admin/VIS/pfile/spfileVIS.ora $ORACLE_HOME/dbs/`
	Pour Oracle 19c :
	1. Copiez `/rdsdbdata/config/oracle_pfile` dans `$ORACLE_HOME` .
	`$ cp /rdsdbdata/config/oracle_pfile $ORACLE_HOME/dbs/initVISCDB.ora`
	2. Modifiez le `initVISCDB.ora` fichier sur l'instance de base de données personnalisée Amazon RDS. Validez tous les paramètres de la source et ajoutez les paramètres nécessaires. Pour plus de détails, consultez la note de support Oracle 396009.1.
	Important
	Assurez-vous qu'il n'y a aucun commentaire dans les paramètres que vous ajoutez. S'il	

Tâche	Description	Compétences requises

	y a des commentaires, ils peuvent entraîner des problèmes d'automatisation, tels que la création de répliques de lecture et l'émission de point-in-time récupérations ()PITRs.
	
	3. Ajoutez au `initVISCDB.ora` fichier des paramètres similaires aux suivants, en fonction de vos besoins.
	
	`*.instance_name=VISCDB`
	`*.sec_case_sensitive_logon= FALSE`
	`*.result_cache_max_size = 600M`
	`*.optimizer_adaptive_plans =TRUE`
	`*.optimizer_adaptive_statistics = FALSE`
	`*.pga_aggregate_limit = 0`
	`*.temp_undo_enabled = FALSE`
	`*._pdb_name_case_sensitive = TRUE`
	`*.event='10946 trace name context forever, level 8454144'`
	`*.workarea_size_policy='AUTO'`
	`*.plsql_code_type='INTERPRETED'`	

Tâche	Description	Compétences requises
	*.cursor_sharing=' EXACT' *._b_tree_bitmap_pla ns=FALSE *.session_cached_c ursors=500 *.optimizer_secu re_view_merging=false *.SQL92_SECURITY=TRUE _system_trig_enabled = TRUE nls_language = american nls_territory = america nls_numeric_charact ers = "." nls_comp = binary nls_sort = binary nls_date_format = DD- MON-RR nls_length_semantics = BYTE aq_tm_processes = 1 _sort_eliminatio n_cost_ratio =5 _like_with_bind _as_equality = TRUE _fast_full_scan_enable d = FALSE _b_tree_bitmap_plans = FALSE optimizer_secure_view _merging = FALSE _optimizer_autostats_ job = FALSE parallel_max_servers = 8 parallel_min_servers = 0 parallel_degree_policy = MANUAL	

Tâche	Description	Compétences requises

	4. Modifier ce qui suit. Les valeurs dépendent de votre système source, alors révisez-les en fonction de votre configuration actuelle.
	`*.open_cursors=500`
	`*.undo_tablespace='UNDOTBS1'`
	5. Supprimez la référence SPFILE :
	`*.spfile='/rdsdbbin/oracle/dbs/spfileVISCDB.ora'`
	Remarques :
	• Ne modifiez pas les valeurs fournies par le fichier PFILE personnalisé Amazon RDS pour `control_files` et. `db_unique_name` Amazon RDS attend ces valeurs. Si vous vous en écartez, des problèmes se poseront si vous essayez de créer une réplique en lecture à l'avenir.
	• Amazon RDS Custom utilise la gestion automatique de la mémoire (AMM) par défaut. Si vous souhaitez utiliser hugemem, vous pouvez configurer Amazon	

Tâche	Description	Compétences requises

	RDS Custom pour utiliser la gestion automatique de la mémoire partagée (ASMM).
	
	• Laissez le `memory_max_target` paramètre activé par défaut. Le framework Amazon RDS l'utilise en arrière-plan pour créer des répliques de lecture.
	
	6. Vérifiez que le `initVISCDB.ora` fichier ne présente aucun problème en exécutant la `startup nomount` commande suivante :
	
	`SQL> startup nomount pfile=/rdsdbbin/oracle/dbs/initVISCDB.ora;`
	`SQL> create spfile='/rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora' from pfile;`
	`SQL> exit`
	
	7. Créez un lien symbolique pour SPFILE.
	
	`$ ln -s /rdsdbdata/admin/VISCDB/pfile/spfileVISCDB.ora $ORACLE_HOME/dbs/`	

Tâche	Description	Compétences requises

Restaurez la base de données personnalisée Amazon RDS à partir de la sauvegarde.	Pour Oracle 12.1.0.2 :
	
	1. Restaurez le fichier de contrôle en utilisant le fichier de sauvegarde que vous avez précédemment capturé sur la source :
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFI`
	`LE FROM '/RMAN/vi`
	`sdb_full_bkp_100rl`
	`sbt';`
	
	`Starting restore at 10-`
	`APR-22`
	`using target database`
	` control file instead of`
	` recovery catalog`
	`allocated channel:`
	` ORA_DISK_1`
	`channel ORA_DISK_`
	`1: SID=201 device`
	` type=DISK`
	
	`channel ORA_DISK_1:`
	` restoring control file`
	`channel ORA_DISK_`
	`1: restore complete,`
	` elapsed time: 00:00:01`
	`output file name=/rds`
	`dbdata/db/VIS_A/co`
	`ntrolfile/control-`
	`01.ctl`
	`Finished restore at 10-`
	`APR-22`
		DBA

Tâche	Description	Compétences requises

	2. Cataloguez les pièces de sauvegarde afin de pouvoir émettre un RMAN `restore` :
	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	3. Créez un script pour restaurer la base de données :
	`$ vi restore.sh`
	`rman target / log=/home /rdsdb/rman.log << EOF`
	`run`
	`{`
	`set newname for database to '/rdsdbdata/db/VIS _A/datafile/%b';`
	`restore database;`
	`switch datafile all;`
	`switch tempfile all;`
	`}`
	`EOF`
	4. Restaurez la source dans la base de données personnalisée Amazon RDS cible. Vous devez modifier les autorisations du script pour autoriser son exécution, puis exécuter le `restore.sh` script pour restaurer la base de données.
	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`	

Tâche	Description	Compétences requises

	Pour Oracle 19c :
	
	1. Restaurez le fichier de contrôle en utilisant le fichier de sauvegarde que vous avez précédemment capturé sur la source :
	
	`RMAN> connect target /`
	`RMAN> RESTORE CONTROLFILE FROM '/RMAN/control.bak';`
	`Starting restore at 07-JUN-23`
	`using target database control file instead of recovery catalog`
	`allocated channel: ORA_DISK_1`
	`channel ORA_DISK_1: SID=201 device type=DISK`
	`channel ORA_DISK_1: restoring control file`
	`channel ORA_DISK_1: restore complete, elapsed time: 00:00:01`
	`output file name=/rdsdbdata/db/cdb/VISCDB_A/controlfile/control-01.ctl`
	`Finished restore at 07-JUN-23`
	
	2. Cataloguez les pièces de sauvegarde afin de pouvoir émettre un RMAN `restore` :	

Tâche	Description	Compétences requises

	`RMAN> alter database mount;`
	`RMAN> catalog start with '/RMAN/visdb';`
	
	Si vous rencontrez des problèmes avec la `start with` commande, vous pouvez ajouter les éléments de sauvegarde individue llement, par exemple :
	
	`RMAN> catalog backuppiece '/RMAN/visdb_full_bkp_1d1e507m';`
	
	puis répétez la commande pour chaque pièce de sauvegarde.
	
	3. Créez un script pour restaurer la base de données. Modifiez le nom de la base de données enfichable en fonction de vos besoins. Allouez des canaux parallèles en fonction du nombre de v CPUs disponibles pour accélérer le processus de restauration.
	
	`$ vi restore.sh`
	`rman target / log=/home/rdsdb/rmancdb.log <<`
	`EOF`
	`run {`	

Tâche	Description	Compétences requises
	`allocate channel c1 type disk; allocate channel c2 type disk; .... allocate channel c<N> type disk; set newname for database to '/rdsdbdata/db/cdb /VISCDB_A/datafile/ %b'; set newname for database root to '/rdsdbda ta/db/cdb/VISCDB_A/ datafile/%f_%b'; set newname for database "PDB$SEED" to '/rdsdbdata/db/cdb/ pdbseed/%f_%b'; set newname for pluggable database VIS to '/rdsdbdata/db/pdb /VISCDB_A/%f_%b'; restore database; switch datafile all; switch tempfile all; release channel c1; release channel c2; release channel c3; .... release channel c<N>; } EOF` 4. Restaurez la source dans la base de données personnalisée Amazon RDS cible. Vous devez modifier les autorisations du script pour autoriser son exécution, puis exécuter	

Tâche	Description	Compétences requises

	le `restore.sh` script pour restaurer la base de données.
	
	`$ chmod 755 restore.sh`
	`$ nohup ./restore.sh &`	

Tâche	Description	Compétences requises

Vérifiez les fichiers journaux pour détecter les problèmes.	Pour Oracle 12.1.0.2 :
	
	1. Vérifiez qu'il n'y a aucun problème en consultant le `rman.log` fichier :
	
	`$ cat /home/rdsdb/rman.log`
	
	2. Confirmez le chemin des fichiers journaux enregistrés dans le fichier de contrôle :
	
	`SQL> select member from v$logfile;`
	`MEMBER`
	`----------`
	`/d01/oracle/VIS/data/log1.dbf`
	`/d01/oracle/VIS/data/log2.dbf`
	`/d01/oracle/VIS/data/log3.dbf`
	
	3. Renommez les fichiers journaux pour qu'ils correspondent au chemin de fichier de la cible. Remplacez le chemin pour qu'il corresponde au résultat de l'étape précédente :
	
	`SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log1.`
		DBA

Tâche	Description	Compétences requises
	dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log1.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log2.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log2.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/oracle/VIS/data/log3.dbf' TO '/rdsdbdata/db/VIS_A/onlinelog/log3.dbf'; Pour Oracle 19c : 1. Vérifiez qu'il n'y a aucun problème en consultant le `rmancdb.log` fichier : `$ cat /home/rdsdb/rmancdb.log` 2. Confirmez le chemin des fichiers journaux enregistrés dans le fichier de contrôle : SQL> select member from v$logfile; MEMBER ---------- ---------- ---------- ---------- --------	

Tâche	Description	Compétences requises
	/d01/oracle/VIS/or adata/VISCDB/redo0 3.log /d01/oracle/VIS/orada ta/VISCDB/redo02.log /d01/oracle/VIS/ oradata/VISCDB/re do01.log 3. Renommez les fichiers journaux pour qu'ils correspon dent au chemin de fichier de la cible. Remplacez le chemin pour qu'il corresponde au résultat de l'étape précédente : SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo01.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log1.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo02.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log2.dbf'; SQL> ALTER DATABASE RENAME FILE '/d01/ora cle/VIS/oradata/VI SCDB/redo03.log' TO '/rdsdbdata/db/cdb/ VISCDB_A/onlinelog/ log3.dbf';	

Tâche	Description	Compétences requises

	4. Confirmez le chemin, l'état des fichiers journaux et le numéro de groupe enregistré dans le fichier de contrôle :
	
	`SQL> column REDOLOG_F ILE_NAME format a50 SQL> SELECT a.GROUP#, a.status, b.MEMBER AS REDOLOG_FILE_NAME, (a.BYTES/1024/1024) AS SIZE_MB FROM v$log a JOIN v$logfile b ON a.Group#=b.Group# ORDER BY a.GROUP#;`
	
	`GROUP# STATUS REDOLOG_F ILE_NAME SIZE_MB 1 CURRENT /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log1.dbf 512 2 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log2.dbf 512 3 INACTIVE /rdsdbdat a/db/cdb/VISCDB_A/ onlinelog/log3.dbf 512`	

Tâche	Description	Compétences requises
Vérifiez que vous pouvez ouvrir la base de données personnalisée Amazon RDS et créer des fichiers journaux OMF.	Amazon RDS Custom pour Oracle utilise Oracle Managed Files (OMF) pour simplifier les opérations. Vous pouvez convertir les répliques de lecture en instances autonomes, mais vous devez d'abord créer les fichiers journaux à l'aide d'OMF. Cela permet de garantir que le chemin correct est utilisé lors de la promotion de l'instanc e. Pour plus d'informations sur la manière de promouvoi r les répliques de lecture, consultez la documentation Amazon RDS. Le fait de ne pas utiliser les fichiers OMF peut entraîner des problèmes lorsque vous essayez de promouvoir des répliques de lecture. 1. Ouvrez la base de données avec `resetlogs` : `SQL> alter database open resetlogs;` **Note** Si vous recevez le message d'erreur ORA-00392 : le journal xx du thread 1 est	DBA

Tâche	Description	Compétences requises
	en cours d'effacement, opération non autorisée, suivez les étapes de la section Dépannage pour ORA-00392.	

	2. Vérifiez que la base de données est ouverte :
	`SQL> select open_mode from v$database;`
	`OPEN_MODE`
	`----------`
	`READ WRITE`	

	3. Créez les fichiers journaux OMF. Modifiez les numéros de groupe, le nombre de groupes et la taille en fonction de vos besoins en utilisant le résultat de la requête de fichier journal précédente. L'exemple suivant commence au groupe 4 et ajoute trois groupes pour des raisons de simplicité.
	`SQL> alter database add logfile group 4 size 512M;`
	`Database altered.`
	`SQL> alter database add logfile group 5 size 512M;`
	`Database altered.`	

Tâche	Description	Compétences requises

	`SQL> alter database add logfile group 6 size 512M;`
	`Database altered.`
	
	4. Supprimez les anciens fichiers non-OMF. Voici un exemple que vous pouvez personnaliser en fonction de vos besoins et du résultat de la requête des étapes précédentes :
	
	`SQL> alter database drop logfile group 1;`
	`System altered.`
	`SQL> alter database drop logfile group 2;`
	`System altered.`
	`SQL> alter database drop logfile group 3;`
	`System altered.`
	
	Note
	Si vous recevez un message d'erreur ORA-01624 lorsque vous tentez de supprimer les fichiers journaux, consultez la section Dépannage.
	
	5. Vérifiez que vous pouvez voir les fichiers OMF qui ont été créés. (Le chemin du	

Tâche	Description	Compétences requises

	répertoire varie pour Oracle 12.1.0.2 et 19c, mais le concept est le même.)
	
	`SQL> select member from v$logfile;`
	
	`MEMBER`
	`----------`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_4_ksrbslny_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_5_ksrchw0k_.log`
	`/rdsdbdata/db/cdb/VISCDB_A/onlinelog/o1_mf_6_ksrcnl9v_.log`
	
	6. Redémarrez la base de données et vérifiez que SPFILE est utilisé par l'instance :
	
	`SQL> shutdown immediate`
	`SQL> startup`
	`SQL> show parameter spfile`
	
	Pour Oracle 12.1.0.2, cette requête renvoie :
	
	`spfile /rdsdbbin/oracle/dbs/spfileVIS.ora`	

Tâche	Description	Compétences requises

	Pour Oracle 19c, la requête renvoie :
	
	`spfile /rdsdbbin /oracle/dbs/spfile VISCDB.ora`
	
	7. Pour Oracle 19c uniquement, vérifiez l'état de la base de données de conteneurs et ouvrez-la si nécessaire :
	
	`SQL> show pdbs CON_ID CON_NAME OPEN MODE RESTRICTED ---------- --------- ---------- --------- - 2 PDB$SEED READ ONLY NO 3 VIS MOUNTED NO`
	
	`SQL> alter session set container=VIS; Session altered.`
	
	`SQL> alter database open; Database altered.`
	
	`SQL> alter database save state; Database altered.`
	
	`SQL> show pdbs CON_ID CON_NAME OPEN MODE RESTRICTED`	

Tâche	Description	Compétences requises
	``` ---------- --------- ---------- ---------- ----- 3 VIS READ WRITE NO SQL> exit ```	
	8. Supprimez le `init.ora` fichier de`$ORACLE_HOME/dbs`, car vous n'utilisez pas le PFILE : ``` $ cd $ORACLE_HOME/dbs ```	

	Pour Oracle 12.1.0.2, utilisez la commande suivante :
	``
	$ pwd
	/rdsdbbin/oracle/dbs
	$ rm initVIS.ora
	``	

	Pour Oracle 19c, utilisez la commande :
	``
	$ pwd
	/rdsdbbin/oracle/dbs
	$ rm initVISCDB.ora
	``	

Récupérez les mots de passe depuis Secrets Manager, créez des utilisateurs et modifiez les mots de passe

Tâche	Description	Compétences requises
Récupérez les mots de passe depuis Secrets Manager.	Vous pouvez effectuer ces étapes dans la console ou à l'aide de l'AWS CLI. Les étapes suivantes fournissent des instructions pour la console. 1. Connectez-vous à AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/. 2. Dans le volet de navigation, choisissez Databases, puis sélectionnez la base de données Amazon RDS. 3. Choisissez Configuration, puis notez l'ID de ressource de l'instance (il sera au format :`db-WZ4WLCK6AOQ6TJGZKMGRCDCI3Y`). 4. Ouvrez la console AWS Secrets Manager à l'adresse https://console.aws.amazon.com/secretsmanager/. 5. Choisissez le secret qui porte le même nom	DBA

Tâche	Description	Compétences requises
	quedo-not-delete-custom-<resource_id> , où resource-id fait référence à l'ID de l'instance que vous avez noté à l'étape 3. 6. Choisissez Retrieve secret value (Récupérer la valeur d'un secret).	

Tâche	Description	Compétences requises
Créez l'utilisateur RDSADMIN.	`RDSADMIN`est un utilisateur de base de données de surveillance et d'orchestration dans l'instance de base de données personnalisée Amazon RDS. Étant donné que la base de données de départ a été supprimée et que la base de données cible a été restaurée à partir de la source à l'aide de RMAN, vous devez recréer cet utilisateur après l'opération de restauration pour vous assurer que la surveillance personnalisée d'Amazon RDS fonctionne comme prévu. Vous devez également créer un profil et un espace disque logique distincts pour l'`RDSADMIN`utilisateur. Les instructions diffèrent légèrement pour Oracle 12.1.0.2 et 19c. Pour Oracle 12.1.0.2 : 1. Entrez les commandes suivantes à l'invite SQL : `SQL> set echo on feedback on serverout on SQL> @?/rdbms/admin/utlpwdmg.sql`	DBA

Tâche	Description	Compétences requises
	SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_F UNCTION NULL; 2. Créez le profil RDSADMIN : SQL> create profile RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400	

Tâche	Description	Compétences requises

	`PASSWORD_GRACE_TIME 604800/86400;`
	
	3. Définissez les profils `SYSSYSTEM`, et `DBSNMP` utilisateur pour `RDSADMIN` :
	
	`SQL> set echo on feedback on serverout on`
	`SQL> alter user SYS profile RDSADMIN;`
	`SQL> alter user SYSTEM profile RDSADMIN;`
	`SQL> alter user DBSNMP profile RDSADMIN;`
	
	4. Créez le `RDSADMIN` tablespace :
	
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent managemen t local autoallocate default nocompress segment space managemen t auto;`
	
	5. Créez l'`RDSADMIN`utilisateur. Remplacez le `RDSADMIN` mot de passe par le mot de passe que vous avez obtenu précédemment auprès de Secrets Manager :	

Tâche	Description	Compétences requises

	`SQL> create user rdsadmin identified by xxxxxxxxxx`
	`Default tablespace rdsadmin`
	`Temporary tablespace temp`
	`profile rdsadmin ;`	

	6. Accordez des privilèges à `RDSADMIN` :
	`SQL> grant select on sys.v_$instance to rdsadmin;`
	`SQL> grant select on sys.v_$archived_log to rdsadmin;`
	`SQL> grant select on sys.v_$database to rdsadmin;`
	`SQL> grant select on sys.v_$database_incarnation to rdsadmin;`
	`SQL> grant select on dba_users to rdsadmin;`
	`SQL> grant alter system to rdsadmin;`
	`SQL> grant alter database to rdsadmin;`
	`SQL> grant connect to rdsadmin with admin option;`
	`SQL> grant resource to rdsadmin with admin option;`
	`SQL> alter user rdsadmin account unlock identified by xxxxxxxxxxx;`	

Tâche	Description	Compétences requises

	`SQL> @?/rdbms/admin/userlock.sql`
	`SQL> @?/rdbms/admin/utlrp.sql`
	
	Pour Oracle 19c :
	
	1. Entrez les commandes suivantes à l'invite SQL :
	
	`SQL> set echo on feedback on serverout on`
	`SQL> @?/rdbms/admin/utlpwdmg.sql`
	
	`SQL> alter profile default LIMIT FAILED_LOGIN_ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED PASSWORD_VERIFY_FUNCTION NULL;`
	
	2. Créez le profil`RDSADMIN`.
	
	Note
	`RDSADMIN`possède le préfixe `C##` in Oracle 19c. Cela est dû au fait que le paramètre de base de données `common_user_prefix` est défini sur`C##`.	

Tâche	Description	Compétences requises
	RDSADMINn'a aucun préfixe dans Oracle 12.1.0.2. SQL> create profile C##RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER_CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTEMPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400;	

Tâche	Description	Compétences requises

	3. Définissez les profils SYSSYSTEM, et DBSNMP utilisateur pour RDSADMIN :
	`SQL> alter user SYS profile C##RDSADMIN;`
	`SQL> alter user SYSTEM profile C##RDSADMIN;`
	`SQL> alter user DBSNMP profile C##RDSADMIN;`
	4. Créez le RDSADMIN tablespace :
	`SQL> create bigfile tablespace rdsadmin datafile size 7M autoextend on next 1m Logging online permanent blocksize 8192 extent management local autoallocate default nocompress segment space management auto;`
	5. Créez l'RDSADMINutilisateur. Remplacez le RDSADMIN mot de passe par le mot de passe que vous avez obtenu précédemment auprès de Secrets Manager.
	`SQL> create user C##rdsadmin identified by xxxxxxxxxx profile C##rdsadmin container=all;`	

Tâche	Description	Compétences requises

	6. Accordez des privilèges à `RDSADMIN` :
	
	`SQL> grant select on sys.v_$instance to c##rdsadmin;`
	`SQL> grant select on sys.v_$archived_log to c##rdsadmin;`
	`SQL> grant select on sys.v_$database to c##rdsadmin;`
	`SQL> grant select on sys.v_$database_incarnation to c##rdsadmin;`
	`SQL> grant select on dba_users to c##rdsadmin;`
	`SQL> grant alter system to C##rdsadmin;`
	`SQL> grant alter database to C##rdsadmin;`
	`SQL> grant connect to C##rdsadmin with admin option;`
	`SQL> grant resource to C##rdsadmin with admin option;`
	`SQL> alter user C##rdsadmin account unlock identified by xxxxxxxxxxx;`
	`SQL> @?/rdbms/admin/userlock.sql`
	`SQL> @?/rdbms/admin/utlrp.sql`	

Tâche	Description	Compétences requises

Créez l'utilisateur principal.	Étant donné que la base de données de départ a été supprimée et que la base de données cible a été restaurée à partir de la source à l'aide de RMAN, vous devez recréer l'utilisateur principal. Dans cet exemple, le nom d'utilisateur principal est`admin`.
	
	Pour Oracle 12.1.0.2 :
	
	`SQL> create user admin identified by <password>; SQL> grant dba to admin`
	
	Pour Oracle 19c :
	
	`SQL> alter session set container=VIS;`
	
	`Session altered.`
	
	`SQL> create user admin identified by <password>;`
	
	`User created.`
	
	`SQL> grant dba to admin;`
	
	`Grant succeeded.`
		DBA

Tâche	Description	Compétences requises

Modifiez les mots de passe des superutilisateurs.	1. Modifiez les mots de passe du système en utilisant le mot de passe que vous avez récupéré dans Secrets Manager.
	
	Pour Oracle 12.1.0.2 :
	
	`SQL> alter user sys identified by xxxxxxxxxxx; SQL> alter user system identified by xxxxxxxxxx;`
	
	Pour Oracle 19c :
	
	`SQL> alter user sys identified by xxxxxxxxxxx container =all; SQL> alter user system identified by xxxxxxxxxx container =all;`
	
	1. Changez les `EBS_SYSTEM` mots de passe.
	
	Pour Oracle 12.1.0.2 :
	
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	Pour Oracle 19c :
		DBA

Tâche	Description	Compétences requises

	Pour cette version, vous devez également vous connecter à la base de données du conteneur pour y mettre à jour le `EBS_SYSTEM` mot de passe.
	
	`SQL> alter session set container=vis;`
	`SQL> alter user ebs_system identified by xxxxxxxxxx;`
	
	`SQL> exit;`
	
	Si vous ne modifiez pas ces mots de passe, Amazon RDS Custom affiche le message d'erreur suivant : L'utilisateur de surveillance de la base de données ou les informations d'identification de l'utilisateur ont changé.	

Créez des répertoires pour Oracle E-Business Suite, installez ETCC et exécutez Autoconfig

Tâche	Description	Compétences requises
Créez les répertoires requis pour Oracle E-Business Suite.	1. Sur la base de données Oracle personnalisée Amazon RDS, exécutez le script suivant en tant qu'utilis ateur d'Oracle Home, pour créer le `9idata` répertoire dans`$ORACLE_HOME/nls/d`	

Tâche	Description	Compétences requises

	`ata/9idata` . Ce répertoire est obligatoire pour Oracle E-Business Suite.
	
	`perl $ORACLE_HOME/nls/data/old/cr9idata.pl`
	
	Ignorez le `ORA_NLS10` message, car vous allez créer l'environnement contextuel ultérieurement.
	
	2. Copiez le `appsutil.tar` fichier, que vous avez créé précédemment à partir du système de fichiers Amazon EFS partagé, et décompressez-le dans le répertoire d'accueil Oracle personnalisé d'Amazon RDS. Cela crée le `appsutil` répertoire dans le `$ORACLE_HOME` répertoire.
	
	`$ cd /RMAN/appsutil`
	`$ cp sourceappsutil.tar $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	`$ tar xvf sourceappsutil.tar appsutil`
	
	3. Copiez le `appsutil.zip` fichier que vous avez précédemment enregistré sur le système de fichiers partagé Amazon EFS. Il s'agit du	

Tâche	Description	Compétences requises

	fichier que vous avez créé au niveau de l'application.
	
	En tant qu'`rdsdb`utilisateur de l'instance de base de données personnalisée Amazon RDS :
	
	`$ cp /RMAN/appsutil/appsutil.zip $ORACLE_HOME`
	`$ cd $ORACLE_HOME`
	
	4. Décompressez le `appsutil.zip` fichier pour créer le `appsutil` répertoire et les sous-répertoires dans le répertoire de base d'Oracle :
	
	`$ unzip -o appsutil.zip`
	
	`-o`Cette option signifie que certains fichiers seront remplacés.	

Tâche	Description	Compétences requises

Configurez les fichiers tsanames.ora et sqlnet.ora.	Vous devez configurer le `tnsnames.ora` fichier afin de pouvoir vous connecter à la base de données avec l'outil Autoconfig. Dans l'exemple suivant, vous pouvez voir que le `tnsnames.ora` fichier est associé à des liens souples, mais qu'il est vide par défaut.
	`$ cd $ORACLE_HOME/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 373 Oct 31 2013 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Feb 9 17:17 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Feb 9 17:17 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	1. Créez l'`tnsnames.ora` entrée. En raison de la façon dont Amazon RDS automatise les fichiers, vous devez vous assurer que l'entrée ne contient
		DBA

Tâche	Description	Compétences requises

	pas d'espaces blancs, de commentaires ou de lignes supplémentaires. Sinon, vous risquez de rencontrer des problèmes lors de l'utilisation de certains outils APIs tels que create-db-instance-read-replica. Utilisez ce qui suit à titre d'exemple.
	
	2. Remplacez le port, l'hôte et le SID conformément à vos besoins :
	
	`$ vi tnsnames.ora`
	`VIS=(DESCRIPTION=`
	`(ADDRESS_LIST=(ADD`
	`RESS=(PROTOCOL=TCP`
	`)(PORT=1521)(HOST=`
	`xx.xx.xx.xx)))(CON`
	`NECT_DATA=(SID=VIS)`
	`(SERVER=DEDICATED)))`
	
	Note
	Il ne doit pas y avoir de lignes supplémentaires dans le fichier. Si vous ne supprimez pas les lignes, vous risquez de rencontrer des problèmes lors de la création d'une réplique en lecture à l'avenir. La création d'une	

Tâche	Description	Compétences requises

	réplique en lecture peut échouer avec le message d'erreur suivant : L'activité a généré une exception HostManagerExcepti on : Impossible d'appeler RestrictR eplication sur aucun hôte.
	
	3. Vérifiez que la base de données est accessible :
	
	`$ tnsping vis`
	`OK (0 msec)`
	
	4. Pour Oracle 19c uniquemen t, mettez à jour le `sqlnet.or a` fichier. Dans le cas contraire, l'erreur ORA-01017 s'affichera : nom d'utilisa teur/mot de passe non valide ; ouverture de session refusée lorsque vous essayez de vous connecter à la base de données. Modifiez `sqlnet.ora $ORACLE_H OME/network/admin` pour qu'il corresponde à ce qui suit :	

Tâche	Description	Compétences requises

	`NAMES.DIRECTORY_PATH=(TNSNAMES, ONAMES, HOSTNAME)`
	`SQLNET.EXPIRE_TIME= 10`
	`SQLNET.INBOUND_CONNECT_TIMEOUT =60`
	`SQLNET.ALLOWED_LOGON_VERSION_SERVER=10`
	`HTTPS_SSL_VERSION=undetermined`
	
	5. Testez la connectivité :
	
	`$ sqlplus apps/****@vis`	

Tâche	Description	Compétences requises

Configurez la base de données.	Maintenant que vous avez testé la connectivité à la base de données, vous pouvez configurer la base de données à l'aide de l'utilitaire appsutil pour créer un environnement contextuel.
	
	Pour Oracle 12.1.0.2 :
	
	1. Exécutez les commandes suivantes :
	
	`$ cd $ORACLE_HOME/appsutil/bin`
	`$ perl adbldxml.pl appsuser=apps`
	`Enter Hostname of Database server: oebs-db01`
	`Enter Port of Database server: 1521`
	`Enter SID of Database server: VIS`
	`Enter Database Service Name: VIS`
	`Enter the value for Display Variable: :1`
	`The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml`
	
	2. Créez `oraInst.loc` à partir de l'utilisateur root :
	
	`$ vi /etc/oraInst.loc`
		DBA

Tâche	Description	Compétences requises
	`inventory_loc=/rdsdbbin/oracle.12.1.custom.r1.EE.1/oraInventory inst_group=database`	

	3. Clonez le fichier de contexte pour définir le nom d'hôte logique à l'aide du fichier de contexte que vous avez créé à l'étape précédente. En tant qu'`rdsdb`utilisateur, exécutez :
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	où `oebs-db01log` fait référence au nom d'hôte logique. Par exemple :
	`$ perl adclonectx.pl \`
	`contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/VIS_oebs-db01.xml \`
	`template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp`
	`Target System Hostname (virtual or normal) [oebs-db01] : oebs-db01log`	

Tâche	Description	Compétences requises
	Target System Base Directory : /rdsdbbin/ oracle Target Instance is RAC (y/n) [n] : n Target System Database SID : VIS Oracle OS User [rdsdb] : Oracle OS Group [rdsdb] : database Role separation is supported y/n [n] ? : n Target System utl_file_ dir Directory List : / tmp Number of DATA_TOP's on the Target System [1] : Target System DATA_TOP Directory 1 [/rdsdbbi n/oracle/data] : / rdsdbdata/db/VIS_A/ datafile/ Target System RDBMS ORACLE_HOME Directory [/rdsdbbin/oracle/ 12.1.0] : /rdsdbbin/ oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as	

Tâche	Description	Compétences requises
	the source system (y/n) [y] ? : y The new database context file has been created : /rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml contextfile=/rdsdbbin/oracle.12.1.custom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml Pour Oracle 19c : 1. Exécutez les commandes suivantes : $ cd $ORACLE_HOME/appsutil/bin $ perl adbldxml.pl appsuser=apps Enter Hostname of Database server: oebs-db01 Enter Port of Database server: 1521 Enter SID of Database server: VIS Enter the database listener name:L_VISCDB_001 Enter the value for Display Variable: :1 The context file has been created at: /rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml	

Tâche	Description	Compétences requises

	2. Créez `oraInst.loc` à partir de l'utilisateur root :
	`$ vi /etc/oraInst.loc`
	`inventory_loc=/rdsdbbin/oracle/oraInventory`
	`inst_group=database`
	3. Clonez le fichier de contexte pour définir le nom d'hôte logique à l'aide du fichier de contexte que vous avez créé à l'étape précédente. En tant qu'`rdsdb`utilisateur, exécutez :
	`$ cd $ORACLE_HOME/appsutil/clone/bin`
	`$ perl adclonectx.pl \`
	`contextfile=[ORACLE_HOME]/appsutil/[current context file] \`
	`template=[ORACLE_HOME]/appsutil/template/adxdbctx.tmp`
	où `oebs-db01log` fait référence au nom d'hôte logique. Par exemple :
	`$ perl adclonectx.pl \`
	`contextfile=/rdsdbbin/oracle/appsutil/VIS_oebs-db01.xml \`
	`template=/rdsdbbin/oracle/appsutil/template/adxdbctx.tmp`	

Tâche	Description	Compétences requises
	Target System Hostname (virtual or normal) [oebs-db01] : oebs-db01log Target System Base Directory : /rdsdbbin/oracle Target Instance is RAC (y/n) [n] : n Target System CDB Name : VISCDB Target System PDB Name : VIS Oracle OS User [oracle] : rdsdb Oracle OS Group [dba] : database Role separation is supported y/n [n] ? : n Number of DATA_TOP's on the Target System [2] : Target System DATA_TOP Directory 1 [/d01/oracle/VISCDB] : /rdsdbdata/db/pdb/VISCDB_A Target System DATA_TOP Directory 2 [/d01/oracle/data] : /rdsdbdata/db/pdb/VISCDB_A/datafile Specify value for OSBACKUPDBA group [database] : Specify value for OSDGDBA group [database] : Specify value for OSKMDBA group [database] :	

Tâche	Description	Compétences requises
	Specify value for OSRACDBA group [database] : Target System RDBMS ORACLE_HOME Directory [/d01/oracle/19.0. 0] : /rdsdbbin/oracle Do you want to preserve the Display [:1] (y/n) : y Do you want the target system to have the same port values as the source system (y/n) [y] ? : y Validating if the source port numbers are available on the target system.. Complete port informati on available at / rdsdbbin/oracle/a ppsutil/clone/bin/ out/VIS_oebs-db01log/ portpool.lst New context path and file name [VIS_oebs -db01log.xml] : / rdsdbbin/oracle/a ppsutil/VIS_oebs-d b01log.xml Do you want to overwrite it (y/n) [n] ? : y Replacing /rdsdbbin /oracle/appsutil/V IS_oebs-db01log.xml file. The new database context file has been created : contextfile=/rdsdbbin/ oracle/appsutil/VIS_o ebs-db01log.xml	

Tâche	Description	Compétences requises
	`Check Clone Context logfile /rdsdbbin/oracle/appsutil/clone/bin/CloneContext_0609141428.log for details.`	

Tâche	Description	Compétences requises

Installez ETCC et lancez Autoconfig.	1. Installez le vérificateur de niveau de code technologique (ETCC) d'Oracle E-Business Suite.
	
	Téléchargez le correctif 17537119 depuis My Oracle Support et suivez les instructions indiquées dans. `README.txt` Vous allez créer un répertoire appelé `etcc` dans le `$ORACLE_HOME` répertoire, décompresser le correctif pour créer un script appelé`checkMTpatch.sh` , puis exécuter le script pour vérifier les versions du correctif.
	
	2. Exécutez l'utilitaire Autoconfig et transmettez le nouveau fichier de contexte de nom d'hôte logique.
	
	Pour Oracle 12.1.0.2 :
	
	`cd $ORACLE_HOME/appsutil/bin`
	`$ ./adconfig.sh contextfile=/rdsdbbin/oracle.12.1.customstom.r1.EE.1/appsutil/clone/bin/VIS_oebs-db01log.xml`
	
	Pour Oracle 19c :
		DBA

Tâche	Description	Compétences requises

	Autoconfig s'attend à ce que le nom de l'écouteur corresponde. `CDBNAME` Par conséquent, le fichier de configuration d'origine de l'écouteur sauvegardé sera utilisé `L_<CDBNAME>_001` temporairement.
	
	`$ lsnrctl stop L_VISCDB_001`
	`$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_orig`
	`$ vi /rdsdbdata/config/listener.ora`
	`:%s/L_VISCDB_001/VISCDB/g`
	`$ lsnrctl start VISCDB`
	`$ cd /rdsdbbin/oracle/appsutil`
	`$ . ./txkSetCfgCDB.env dboraclehome=/rdsdbbin/oracle.19.custom.r1.EE-CDB.1`
	
	`Oracle Home being passed: /rdsdbbin/oracle`
	
	`$ echo $ORACLE_HOME`
	`/rdsdbbin/oracle.19.custom.r1.EE-CDB.1`
	`$ export ORACLE_SID=VISCDB`
	`$ cd $ORACLE_HOME/appsutil/bin`	

Tâche	Description	Compétences requises

	`$ perl $ORACLE_HOME/appsutil/bin/txkPostPDBCreationTasks.pl -dboraclehome=$ORACLE_HOME -outdir=$ORACLE_HOME/appsutil/log -cdbsid=VISCDB -pdbsid=VIS -appsuser=apps -dbport=1521 -servicetype=onpremise`
	
	`Enter the APPS Password: <apps password>`
	
	`Enter the CDB SYSTEM Password:<password from secrets manager>`
	
	Note
	Si les répertoires de votre base de données ont changé, suivez les instructions de la note de support Oracle 2525754.1.	

Configuration des entrées TNS pour Amazon RDS Custom et Oracle E-Business Suite

Tâche	Description	Compétences requises
Configurez les entrées TNS pour Amazon RDS Custom et Oracle E-Business Suite.	Autoconfig génère les fichiers TNS dans les emplacements par défaut. Pour Oracle 12.1.0.2 (qui n'est pas un	DBA

Tâche	Description	Compétences requises
	CDB) et pour Oracle19c PDB, l'emplacement par défaut est. `$ORACLE_HOME/network/admin/$<CONTEXT_NAME>` Le CDB pour Oracle 19c utilise la valeur par défaut`$ORACLE_HOME/network/admin/` , telle que définie `$TNS_ADMIN` dans les fichiers d'environnement générés lorsque vous avez exécuté Autoconfig dans les étapes précédentes. Pour Oracle 12.1.0.2 et 19c CDB, vous ne les utiliserez pas car les `listener.ora` fichiers `tnsnames.ora` et générés par Autoconfig ne respectent pas les exigences d'Amazon RDS, telles que l'absence d'espaces blancs ou de commentaires. Vous utilisez plutôt les fichiers génériques fournis avec la base de données personnalisée Amazon RDS pour garantir la conformité avec les attentes du système et pour réduire la marge d'erreur. Par exemple, Amazon RDS Custom attend le format de dénomination suivant :	

Tâche	Description	Compétences requises

	`L_<INSTANCE_NAME>_001`
	
	Pour Oracle 12.1.0.2, ce serait :
	
	`L_VIS_001`
	
	Pour Oracle 19c, ce serait :
	
	`L_VISCDB_001`
	
	Voici un exemple du `listener.ora` fichier que vous allez utiliser. Cela a été généré lorsque vous avez créé la base de données personnalisée Amazon RDS. À ce stade, vous n'avez apporté aucune modification à ce fichier et vous le conserverez comme fichier par défaut.
	
	Pour Oracle 12.1.0.2 :
	
	`$ cd $ORACLE_HOME/network/admin`
	`$ cat listener.ora`
	`ADR_BASE_L_VIS_001=/rdsdbdata/log/`
	`SID_LIST_L_VIS_001=(SID_LIST =`
	`(SID_DESC = (SID_NAME = VIS)(GLOBAL_DBNAME = VIS) (ORACLE_HOME = /rdsdbbin/oracle)))`
	`L_VIS_001=(DESCRIPTION_LIST =`	

Tâche	Description	Compétences requises

	(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = 127.0.0.1)))) SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VIS_001=OFF
	
	Pour Oracle 19c : restaurez le `listener.ora` fichier d'origine avec le nom de l'écouteur. `L_<INSTANCE_NAME>_001`
	
	$ cd $ORACLE_HOME/network/admin
	
	$ cp -rp /rdsdbdata/config/listener.ora /rdsdbdata/config/listener.ora_autoconfig
	$ cp -rp /rdsdbdata/config/listener.ora_orig /rdsdbdata/config/listener.ora
	
	$ cat listener.ora
	SUBSCRIBE_FOR_NODE_DOWN_EVENT_L_VISCDB_001=OFF
	ADR_BASE_L_VISCDB_001=/rdsdbdata/log/
	USE_SID_AS_SERVICE_L_VISCDB_001=ON
	L_VISCDB_001=(DESCRIPTION_LIST = (DESCRIPT	

Tâche	Description	Compétences requises

	`ION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = xx.xx.xx.xx))) (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(PORT = 1521)(HOST = 127.0.0.1)))) SID_LIST_L_VISCDB_001= (SID_LIST = (SID_DESC = (SID_NAME = VISCDB)(GLOBAL_DBNAME = VISCDB) (ORACLE_HOME = /rdsdbbin/oracle)))`
	
	Démarrez l'écouteur `L_<INSTANCE_NAME>_001` pour les opérations Amazon RDS standard :
	
	`$ lsnrctl stop`
	`$ lsnrctl start L_VISCDB_001`
	
	Pour Oracle 12.1.0.2 :
	
	Modifiez le fichier d'environnement Oracle E-Business Suite pour modifier le `$TNS_ADMIN` chemin d'utilisation des fichiers TNS génériques Amazon RDS Custom. Le fichier d'environnement a été créé lorsque vous avez exécuté Autoconfig plus tôt. Modifiez la `TNS_ADMIN` variable en	

Tâche	Description	Compétences requises

	supprimant le `<CONTEXT_NAME>` suffixe.
	
	Note
	Vous devez modifier le fichier d'environnement uniquement dans Oracle 12.1.0.2, car le répertoire d'accueil par défaut pour 19c est `$ORACLE_HOME/network/admin` le même que celui par défaut pour Amazon RDS Custom.
	
	Par exemple, dans Oracle 12.1.0.2, modifiez le fichier :
	
	`$ vi $ORACLE_HOME/VIS_oebs-db01log.env`
	
	Changez le chemin à partir de :
	
	`TNS_ADMIN=”/rdsdbbin/oracle/network/admin/VIS_oebs-db01log”`
	`export TNS_ADMIN`
	
	par :	

Tâche	Description	Compétences requises

	`TNS_ADMIN=”/rdsdbbin/oracle/network/admin”`
	`export TNS_ADMIN`
	
	Note
	Chaque fois que vous exécutez Autoconfig, vous devez répéter cette étape pour vous assurer que les bons fichiers TNS sont utilisés. (12.1.0.2 uniquement).
	
	Pour Oracle 19c :
	
	1. Remplacez la valeur de la variable de contexte de niveau de base de données par `s_cdb_tnsadmin` au `<ORACLE_HOME>/network/admin` lieu de`<ORACLE_HOME>/network/admin/<CONTEXT_NAME>` .
	
	Note
	Ne mettez pas à jour la variable de `s_db_tnsadmin` contexte. Laissez-le tel quel`<ORACLE_H`	

Tâche	Description	Compétences requises

	OME>/network/admin/<CONTEXT_NAME> .
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ vi $CONTEXT_FILE`
	
	2. Enregistrez les modifications que vous avez apportées à la valeur des_cdb_tnsadmin .
	
	Les valeurs pour s_db_tnsadmin et s_cdb_tnsadmin doivent ressembler à ce qui suit, avec le nom PDB comme VIS et le nom logique du nœud de base de données commeoebs-db01log .
	
	`$ grep -i tns_admin $CONTEXT_FILE`
	`<TNS_ADMIN oa_var="s_db_tnsadmin">/rdsdbbin/oracle/network/admin/VIS_oebs-db01log</TNS_ADMIN>`
	`<CDB_TNS_ADMIN oa_var="s_cdb_tnsadmin">/rdsdbbin/oracle/network/admin</CDB_TNS_ADMIN>`	

Tâche	Description	Compétences requises

	3. Exécutez Autoconfig au niveau de la base de données :
	
	`$ . $ORACLE_HOME/VISCDB_oebs-db01log.env`
	`$ export ORACLE_PDB_SID=VIS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/appsutil/admin/adgrants.sql APPS`
	`$ sqlplus "/ as sysdba" @$ORACLE_HOME/rdbms/admin/utlrp.sql`
	
	`$ . $ORACLE_HOME/VIS_oebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`
	
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`
	`$ ./adautocfg.sh`	

Tâche	Description	Compétences requises

Définissez l'environnement pour l'utilisateur rdsdb.	Ignorez cette étape pour Oracle 19c.
	
	Pour Oracle 12.1.0.2 :
	
	Maintenant que vous avez terminé les entrées Autoconfig et TNS, vous devez charger le fichier d'environnement en le définissant dans le profil de l'`rdsdb`utilisateur.
	
	Mise `.bash_profile` à jour pour appeler le `.env` fichier de base de données Oracle E-Business Suite. Vous devez mettre à jour le profil pour vous assurer que l'environnement est chargé. Ce fichier d'environnement a été créé lorsque vous avez exécuté Autoconfig plus tôt.
	
	L'exemple de fichier d'environnement suivant est créé lorsque vous exécutez Autoconfig :
	
	`. /rdsdbbin/oracle/VIS_oebs-db01log.env`
	
	En tant qu'`rdsdb`utilisateur :
	
	`cd $HOME`
	`vi .bash_profile`
		DBA

Tâche	Description	Compétences requises

	`export LD_LIBRARY_PATH=${ORACLE_HOME}/lib:${ORACLE_HOME}/ctx/lib`
	`export SHLIB_PATH=${ORACLE_HOME}/lib`
	`export PATH=$PATH:${ORACLE_HOME}/bin`
	`alias sql='rlwrap -c sqlplus / as sysdba'`
	`. ${ORACLE_HOME}/VIS_oebs-db01log.env`
	
	Note
	Pour Oracle 19c, il n'est pas nécessaire de charger l'environnement CDB. `.bash_profile` Cela est dû au fait que le chemin par défaut `ORACLE_HOME` est défini sur le chemin par défaut`$ORACLE_HOME/network/admin`, qui est le répertoire d'accueil par défaut de l'utilisateur `rdsdb` (Oracle Home).	

Tâche	Description	Compétences requises
Configurez l'application et la base de données pour Amazon RDS Custom.	Effectuez les deux premières étapes pour Oracle 12.1.0.2 et 19c. Les étapes suivantes sont différentes pour chaque version. 1. Au niveau de l'application, modifiez `/etc/hosts` et remplacez l'adresse IP de la base de données par l'adresse IP personnalisée Amazon RDS : `xx.xx.xx.xx OEBS-db01 .localdomain OEBS-db01 OEBS-db01log.local domain OEBS-db01log` Comme vous utilisez des noms d'hôte logiques, vous pouvez remplacer le nœud de base de données de manière presque fluide. 2. Sur l'instance de base de données personnalisée Amazon RDS, ajoutez ou modifiez le groupe de sécurité attribué à l' EC2 instance source pour refléter l'instanc e de base de données personnalisée Amazon RDS, afin de garantir que l'applica tion peut accéder au nœud. Pour Oracle 12.1.0.2 :	DBA

Tâche	Description	Compétences requises

	3. Exécutez Autoconfig. En tant que propriétaire de l'application (par exemple,`applmgr`), exécutez :
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	4. Vérifiez les `fnd_nodes` entrées :
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`----------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	5. Confirmez que vous pouvez vous connecter et démarrer l'application :
	`$ ./adstrtal.sh`
	Pour Oracle 19c :
	1. Vérifiez si le PDB est ouvert et ouvrez-le si nécessaire :	

Tâche	Description	Compétences requises

	`SQL> show pdbs`
	
	`CON_ID CON_NAME OPEN MODE RESTRICTED`
	`---------- --------- ---------- ----------`
	`2 PDB$SEED READ ONLY NO`
	`3 VIS MOUNTED`
	
	`SQL> alter session set container=vis;`
	
	`SQL> alter database open;`
	
	`SQL> alter database save state;`
	
	2. Testez la connectivité en tant que `apps` :
	
	`SQL> sqlplus apps/**** @vis`
	
	3. Exécutez Autoconfig au niveau de la base de données :
	
	`$ . $ORACLE_HOME/VIS_ebs-db01log.env`
	`$ echo $ORACLE_SID`
	`VIS`
	
	`$ cd $ORACLE_HOME/appsutil/scripts/$CONTEXT_NAME`	

Tâche	Description	Compétences requises

	`$ ./adautocfg.sh`
	
	4. Exécutez Autoconfig au niveau de l'application en tant que propriétaire de l'application (par exemple,`applmgr`) :
	
	`$ cd $INST_TOP/admin/scripts`
	`$ ./adautocfg.sh`
	`AutoConfig completed successfully.`
	
	5. Vérifiez les `fnd_nodes` entrées :
	
	`SQL> select node_name from apps.fnd_nodes`
	`NODE_NAME`
	`----------`
	`AUTHENTICATION`
	`OEBS-APP01LOG`
	`OEBS-DB01LOG`
	
	6. Lancez l'application :
	
	`$ ./adstrtal.sh`	

Exécuter les étapes postérieures à la migration

Tâche	Description	Compétences requises

Reprenez l'automatisation pour confirmer qu'elle fonctionne.	Reprenez l'automatisation à l'aide de la commande AWS CLI suivante :
	`aws rds modify-db-instance \ --db-instance-identifier vis \ --automation-mode full \`
	La base de données est désormais gérée par Amazon RDS Custom. Par exemple, si l'écouteur ou la base de données tombe en panne, l'agent Amazon RDS Custom les redémarrera. Pour tester cela, exécutez des commandes telles que les suivantes.
	Exemple d'arrêt de l'écouteur :
	`-bash-4.2$ lsnrctl stop vis`
	Exemple d'arrêt de la base de données :
	`SQL> shutdown immediate ;`
		DBA

Tâche	Description	Compétences requises
Validez le schéma, les connexions et les tâches de maintenance.	Pour finaliser la migration , vous devez au minimum effectuer les tâches suivantes. • Exécutez `FS_CL0NE` pour synchroniser le système de fichiers de correctifs. • Collectez les statistiques du schéma. • Assurez-vous que les interfaces et systèmes externes peuvent se connecter à la nouvelle base de données personnal isée Amazon RDS. • Configurez vos sauvegard es et vos calendriers de maintenance. • Vérifiez qu'AD Online Patching (ADOP) fonctionn e comme prévu en émettant une coupure pour changer de système de fichiers.	DBA

Résolution des problèmes

Problème	Solution
Vous recevez un message d'erreur ORA-01624 lorsque vous essayez de supprimer les fichiers journaux.	Si le message d'erreur ORA-01624 s'affiche lorsque vous essayez de supprimer les fichiers journaux, procédez comme suit. Émettez la commande suivante et attendez que le statut des fichiers journaux que vous

Problème	Solution

	souhaitez supprimer soit atteintINACTIVE. Pour plus d'informations sur les codes d'état contenus dansV$log, consultez la documentation Oracle. Voici un exemple de commande et son résultat :
	
	`SQL> select group#, status from v$log;`
	
	`GROUP# STATUS`
	`---------- ----------------`
	`1 ACTIVE`
	`2 CURRENT`
	`3 UNUSED`
	`4 UNUSED`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`
	
	Dans cet exemple, le fichier journal 1 estACTIVE. Vous devez donc forcer un changement de fichier journal à trois reprises pour vous assurer que le premier nouveau fichier journal que vous avez ajouté précédemment a le statut suivant CURRENT :
	
	`SQL>  alter system switch logfile;`
	`System altered.`
	`SQL>  alter system switch logfile;`
	`System altered.`
	`SQL>  alter system switch logfile;`
	`System altered.`
	
	Attendez que tous les fichiers journaux que vous souhaitez supprimer le soientINACTIVE, comme dans l'exemple suivant, puis exécutez la DROP LOGFILE commande.

Problème	Solution

	`SQL> select group#, status from v$log;`
	`GROUP# STATUS`
	`---------- ----------`
	`1 INACTIVE`
	`2 INACTIVE`
	`3 INACTIVE`
	`4 CURRENT`
	`5 UNUSED`
	`6 UNUSED`
	`6 rows selected.`

Vous recevez un message d'erreur ORA-00392 lorsque vous ouvrez la base de données avec. `resetlogs`	Si vous recevez le message d'erreur ORA-00392 : le journal xx du thread 1 est en cours d'effacement, l'opération n'est pas autorisée, exécutez la commande suivante (`xx`remplacez-la par le numéro du fichier journal), puis réexécutez la commande open : `resetlogs`
	`SQL> alter database clear logfile group xx;`
	`SQL> alter database open resetlogs;`

Problème	Solution
Vous ne parvenez pas à vous connecter à l'application à l'aide de l'administrateur système ou de l'utilisateur de l'application.	Pour confirmer le problème, exécutez la requête SQL suivante : `SQL> select dbms_java.get_jdk_ version() from dual; select dbms_java.get_jdk_version() from dual ERROR at line 1: ORA-29548: Java system class reported: release of Java system classes in the database (19.0.0.0.220719 1.8) does not match that of the oracle executabl e (19.0.0.0.0 1.8)` Cause première : la base de données source a été appliquée avec plusieurs correctifs, mais Amazon RDS Custom `DB_HOME` est une nouvelle installation, ou le CEV n'a pas inclus tous les correctifs parce que vous n'avez pas utilisé les correctifs RSU nécessaires, tels que OJVM, lorsque vous avez créé le CEV. Pour valider cela, vérifiez si les détails du correctif source sont répertoriés sur `$ORACLE_H OME/sqlpath $ORACLE_HOME/.patc h_storage` , et`opatch – lsinventory` . Référence : datapatch -verbose échoue avec une erreur : « Patch xxxxxx : le répertoire de correctifs archivé est vide » (ID du document 2235541.1) Correctif : copiez les fichiers relatifs aux correctifs manquants de la source (`$ORACLE_H OME/sqlpatch/`) vers Amazon RDS Custom (`$ORACLE_HOME/sqlpatch/`), puis réexécutez. `./datapatch -verbose`

Problème	Solution

	Par exemple :
	`-bash-4.2$ cp -rp 18793246 20204035 20887355 22098146 22731026 $ORACLE_HOME/sqlpatch/`
	Vous pouvez également utiliser une solution en exécutant la commande suivante sur le CDB et le PDB :
	`@?/javavm/install/update_javavm_db.sql`
	Exécutez ensuite la commande suivante sur le PDB :
	`sql> alter session set container=vis; @?/javavm/install/update_javavm_db.sql`
	Maintenant, relancez le test :
	`SQL> select dbms_java.get_jdk_version() from dual;`

Ressources connexes

- Utilisation d'Amazon RDS Custom (documentation Amazon RDS)
- Amazon RDS Custom pour Oracle — Nouvelles fonctionnalités de contrôle dans l'environnement de base de données (blog d'actualités AWS)
- Intégrer Amazon RDS Custom pour Oracle à Amazon EFS (blog de base de données AWS)
- Migration d'Oracle E-Business Suite sur AWS (livre blanc AWS)
- Architecture de la suite Oracle E-Business sur AWS (livre blanc AWS)

- Configuration d'une architecture HA/DR pour Oracle E-Business Suite sur Amazon RDS Custom avec une base de données de secours active (AWS Prescriptive Guidance)

Informations supplémentaires

Opérations de maintenance

Appliquer de nouveaux correctifs à la page d'accueil de la base de données Oracle E-Business Suite

Le volume bin (`/rdsdbbin`) étant une out-of-place mise à niveau, son contenu est supprimé lors de la mise à niveau du CEV. Par conséquent, vous devez créer une copie du `appsutil` répertoire avant d'effectuer des mises à niveau à l'aide de CEV.

Sur l'instance Amazon RDS Custom source, avant de mettre à niveau le CEV, effectuez une sauvegarde de. `$ORACLE_HOME/appsutil`

> **Note**
>
> Cet exemple utilise un volume NFS. Toutefois, vous pouvez utiliser une copie sur Amazon Simple Storage Service (Amazon S3) à la place.

1. Créez un répertoire pour stocker appsutil sur l'instance Amazon RDS Custom source :

```
$ mkdir /RMAN/appsutil.preupgrade
```

2. Décompressez et copiez sur le volume Amazon EFS :

```
$ tar cvf /RMAN/appsutil.preupgrade appsutil
```

3. Vérifiez que le fichier tar existe :

```
$ bash-4.2$ ls -l /RMAN/appsutil.preupgrade
-rw-rw-r-- 1 rdsdb rdsdb 622981120 Feb  8 20:16 appsutil.tar
```

4. Effectuez une mise à niveau vers le dernier CEV (le CEV prérequis est déjà créé) en suivant les instructions de la section Mise à niveau d'une instance de base de données personnalisée RDS dans la documentation Amazon RDS).

Vous pouvez également appliquer un patch directement à l'aide d'OPATCH. Consultez la section Exigences et considérations relatives aux mises à niveau personnalisées RDS pour Oracle de la documentation Amazon RDS.

> **Note**
>
> L'adresse IP de la machine hôte ne change pas pendant le processus d'application des correctifs CEV. Ce processus effectue une out-of-place mise à niveau et, au démarrage, un nouveau volume bin est attaché à la même instance.

Migrer Oracle PeopleSoft vers Amazon RDS Custom

Créée par Gaurav Gupta (AWS)

Récapitulatif

Oracle PeopleSoft est une solution de planification des ressources d'entreprise (ERP) pour les processus à l'échelle de l'entreprise. PeopleSoft possède une architecture à trois niveaux : client, application et base de données. PeopleSoft peut être exécuté sur Amazon Relational Database Service (Amazon RDS). Désormais, vous pouvez également exécuter PeopleSoft Amazon RDS Custom, qui donne accès au système d'exploitation sous-jacent.

Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents. Lorsque vous migrez votre base de données Oracle vers Amazon RDS Custom, Amazon Web Services (AWS) peut gérer les tâches de sauvegarde et la haute disponibilité, tandis que vous pouvez vous concentrer sur la maintenance de votre PeopleSoft application et de ses fonctionnalités. Pour connaître les principaux facteurs à prendre en compte lors d'une migration, consultez les stratégies de migration des bases de données Oracle dans AWS Prescriptive Guidance.

Ce modèle se concentre sur les étapes de migration d'une PeopleSoft base de données sur Amazon Elastic Compute Cloud (Amazon EC2) vers Amazon RDS Custom à l'aide d'une sauvegarde Oracle Recovery Manager (RMAN). Il utilise un système de fichiers partagé Amazon Elastic File System (Amazon EFS) entre l' EC2 instance et Amazon RDS Custom, mais vous pouvez également utiliser Amazon FSx ou n'importe quel lecteur partagé. Le modèle utilise une sauvegarde complète RMAN (parfois appelée sauvegarde de niveau 0).

Conditions préalables et limitations

Prérequis

- Base de données source Oracle version 19C qui s'exécute sur Amazon EC2 avec Oracle Linux 7, Oracle Linux 8, Red Hat Enterprise Linux (RHEL) 7 ou RHEL 8. Dans les exemples de ce modèle, le nom de la base de données source est`FSDM092`, mais ce n'est pas obligatoire.

> **Note**
>
> Vous pouvez également utiliser ce modèle avec les bases de données source Oracle locales. Vous devez disposer de la connectivité réseau appropriée entre le réseau sur site et un cloud privé virtuel (VPC).

- Une instance de démonstration PeopleSoft 9.2.
- Un seul niveau PeopleSoft d'application. Toutefois, vous pouvez adapter ce modèle pour qu'il fonctionne avec plusieurs niveaux d'application.
- Amazon RDS Custom configuré avec au moins 8 Go d'espace de swap.

Limites

Ce modèle ne prend pas en charge les configurations suivantes :

- Définition du `ARCHIVE_LAG_TARGET` paramètre de base de données sur une valeur située en dehors de la plage de 60 à 7 200
- Désactivation du mode journal de l'instance de base de données () `NOARCHIVELOG`
- Désactivation de l'attribut optimisé pour Amazon Elastic Block Store (Amazon EBS) de l'instance EC2
- Modification des volumes EBS d'origine attachés à l'instance EC2
- Ajouter de nouveaux volumes EBS ou changer le type de volume de gp2 à gp3
- Modification du format d'extension du `LOG_ARCHIVE_FORMAT` paramètre (obligatoire`*.arc`)
- Multiplexage ou modification de l'emplacement et du nom du fichier de contrôle (cela doit être `/rdsdbdata/db/*DBNAME*/controlfile/control-01.ctl` le cas)

Pour plus d'informations sur ces configurations et sur d'autres configurations non prises en charge, consultez la documentation Amazon RDS.

Versions du produit

Pour les versions de base de données Oracle et les classes d'instances prises en charge par Amazon RDS Custom, consultez Exigences et limites relatives à Amazon RDS Custom pour Oracle.

Architecture

Pile technologique cible

- Application Load Balancer
- Amazon EFS
- Amazon RDS Custom for Oracle
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)

Architecture cible

Le schéma d'architecture suivant représente un PeopleSoft système exécuté dans une seule zone de disponibilité sur AWS. Le niveau application est accessible via un Application Load Balancer. L'application et les bases de données se trouvent dans des sous-réseaux privés, et l'instance de EC2 base de données Amazon RDS Custom et Amazon utilisent un système de fichiers partagé Amazon EFS pour stocker et accéder aux fichiers de sauvegarde RMAN. Amazon S3 est utilisé pour créer le moteur Oracle RDS personnalisé et pour stocker les métadonnées des journaux redo.

Outils

Outils

Services AWS

- Amazon RDS Custom for Oracle est un service de base de données géré pour les applications existantes, personnalisées et packagées qui nécessitent un accès au système d'exploitation et à l'environnement de base de données sous-jacents. Il automatise les tâches d'administration des bases de données, telles que les sauvegardes et la haute disponibilité.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS. Ce modèle utilise un système de fichiers partagé Amazon EFS pour stocker et accéder aux fichiers de sauvegarde RMAN.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Dans ce modèle, vous récupérez les mots de passe des utilisateurs de la base de données à partir de Secrets Manager pour créer les `ADMIN` utilisateurs `RDSADMIN` et pour modifier les `system` mots de passe `sys` et.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité. Ce modèle utilise un Application Load Balancer.

Autres outils

- Oracle Recovery Manager (RMAN) fournit un support de sauvegarde et de restauration pour les bases de données Oracle. Ce modèle utilise RMAN pour effectuer une sauvegarde à chaud de la base de données Oracle source sur Amazon EC2 qui est restaurée sur Amazon RDS Custom.

Bonnes pratiques

- Pour les paramètres d'initialisation de la base de données, personnalisez le fichier standard fourni par l'instance de base de données personnalisée Amazon RDS PeopleSoft au lieu d'utiliser le fichier spfile de la base de données source Oracle. Cela est dû au fait que les espaces blancs et les commentaires posent problème lors de la création de répliques de lecture dans Amazon RDS Custom. Pour plus d'informations sur les paramètres d'initialisation de la base de données, consultez la note de support Oracle 1100831.1 (nécessite un compte Oracle Support).
- Amazon RDS Custom utilise la gestion automatique de la mémoire par Oracle par défaut. Si vous souhaitez utiliser le noyau Hugemem, vous pouvez configurer Amazon RDS Custom pour qu'il utilise plutôt la gestion automatique de la mémoire partagée.
- Laissez le `memory_max_target` paramètre activé par défaut. Le framework l'utilise en arrière-plan pour créer des répliques de lecture.
- Activez la base de données Oracle Flashback. Cette fonctionnalité est utile lors du rétablissement du mode veille dans le cadre de scénarios de test de basculement (et non de basculement).

Épopées

Configuration de l'instance de base de données et du système de fichiers

Tâche	Description	Compétences requises
Créez l'instance de base de données.	Dans la console Amazon RDS, créez une instance de base de données Amazon RDS personnalisée pour Oracle avec un nom de base de données appelé FSDMO92 (ou le nom de votre base de données source). Pour obtenir des instructions, consultez Working with Amazon RDS Custom dans la documentation AWS et le billet de blog Amazon RDS Custom for Oracle — New Control Capabilities in Database Environment. Cela garantit que le nom de la base de données est le même que celui de la base de données source. (Si ce champ est laissé vide, le nom de l' EC2 instance et de la base de données sera défini sur`ORCL`.)	DBA

Effectuez une sauvegarde complète RMAN de la base de données Amazon EC2 source

Tâche	Description	Compétences requises
Créez un script de sauvegarde.	Créez un script de sauvegarde RMAN pour sauvegarder	DBA

Tâche	Description	Compétences requises
	la base de données sur le système de fichiers Amazon EFS que vous avez monté (`/efs`dans l'exemple suivant). Vous pouvez utiliser l'exemple de code ou exécuter l'un de vos scripts RMAN existants. `#!/bin/bash` `Dt=`date +'%Y%m%d-%H%M'` `BACKUP_LOG="rman-${ORACLE_SID}-$Dt"` `export TAGDATE=`date +%Y%m%d%H%M`;` `LOGPATH=/u01/scripts/logs` `rman target / >> $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF` `SQL "ALTER SYSTEM SWITCH LOGFILE";` `SQL "ALTER SESSION SET NLS_DATE_FORMAT="DD.MM.YYYY HH24:MI:SS"";` `RUN` `{` `ALLOCATE CHANNEL ch11 TYPE DISK MAXPIECESIZE 5G;` `ALLOCATE CHANNEL ch12 TYPE DISK MAXPIECESIZE 5G;` `BACKUP AS COMPRESSED BACKUPSET FULL DATABASE FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_FULL' ;`	

Tâche	Description	Compétences requises
	`  SQL "ALTER SYSTEM ARCHIVE LOG CURRENT";  BACKUP FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_ARCHIVE' ARCHIVELOG ALL DELETE ALL INPUT ;  BACKUP CURRENT CONTROLFILE FORMAT '/efs/rman_backup/FSCM/%d_%T_%s_%p_CONTROL';}EXIT;EOF`	

Exécutez le script de sauvegarde.	Pour exécuter le script de sauvegarde RMAN, connectez-vous en tant qu'utilisateur Oracle Home, puis exécutez le script.
	`$  chmod a+x rman_backup.sh`
	`$ ./rman_backup.sh &`
		DBA

Tâche	Description	Compétences requises

Vérifiez les erreurs et notez le nom du fichier de sauvegarde.	Vérifiez la présence d'erreurs dans le fichier journal RMAN. Si tout semble correct, listez la sauvegarde du fichier de contrôle en exécutant la commande suivante.
	`RMAN> list backup of controlfile;`
	`using target database control file instead of recovery catalog`
	Notez le nom du fichier de sortie.
	`List of Backup Sets`
	`==========`
	`BS Key Type LV Size Device Type Elapsed Time Completion Time`
	`12 Full 21.58M DISK 00:00:01 13-JUL-22`
	`BP Key: 12 Status: AVAILABLE Compressed: NO Tag: TAG20220713T150155`
	`Piece Name: /efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL`
		DBA

Tâche	Description	Compétences requises
	`Control File Included: Ckp SCN: 165591599 85898 Ckp time: 13-JUL-22` Vous utiliserez le fichier de contrôle de sauvegarde `/efs/rman_backup/FSCM/FSDM092_20220713_12_1_CONTROL` lorsque vous restaurez la base de données sur Amazon RDS Custom.	

Arrêtez le niveau de l'application source

Tâche	Description	Compétences requises
Arrêtez l'application.	Pour arrêter le niveau de l'application source, utilisez l'`psadmin`utilitaire ou l'utilitaire de ligne de `psadmin` commande. 1. Pour arrêter le serveur Web, exécutez la commande suivante. `psadmin -w shutdown -d "webserver domain name"` 2. Pour arrêter le serveur d'applications, exécutez la commande suivante.	DBA, administrateur PeopleSoft

Tâche	Description	Compétences requises

	`psadmin -c shutdown -d "application server domain name"`
	3. Pour arrêter le planificateur de processus, exécutez la commande suivante.
	`psadmin -p stop -d "process scheduler domain name"`	

Configuration de la base de données personnalisée Amazon RDS cible

Tâche	Description	Compétences requises
Installez le package rpm nfs-utils.	Pour installer le `nfs-utils rpm` package, exécutez la commande suivante. `$ yum install -y nfs-utils`	DBA
Montez le système de stockage EFS.	Obtenez la commande de montage Amazon EFS sur la page de la console Amazon EFS. Montez le système de fichiers EFS sur l'instance Amazon RDS à l'aide d'un client NFS (Network File System). `sudo mount -t nfs4 -o nfsvers=4.1,rsize=1048576,wsize=1048`	DBA

Tâche	Description	Compétences requises
	576,hard,timeo=600 ,retrans=2,noresvp ort fs-xxxxxxxxxx.efs. eu-west-1.amazonaw s.com:/ /efs sudo mount -t nfs4 -o nfsvers=4.1,rsize= 1048576,wsize=1048 576,hard,timeo=600 ,retrans=2,noresvp ort fs-xxxxxxxxxx.efs. eu-west-1.amazonaw s.com:/ /efs	

Supprimez la base de données de départ et créez les répertoires pour stocker les fichiers de base de données

Tâche	Description	Compétences requises
Suspendez le mode d'automatisation.	Vous devez suspendre le mode d'automatisation sur votre instance de base de données personnalisée Amazon RDS avant de passer aux étapes suivantes, afin de vous assurer que l'automatisation n'interfère pas avec l'activité de restauration RMAN. Vous pouvez suspendre l'automatisation à l'aide de la console AWS ou de la commande AWS Command Line Interface (AWS CLI) (assurez-vous d'avoir d'abord	DBA

Tâche	Description	Compétences requises
	configuré l'interface de ligne de commande AWS). `aws rds modify-db-instance \ --db-instance-id entifier peoplesoft-fscm-92 \ --automation-mode all-paused \ --resume-full-au tomation-mode-minute 360 \ --region eu-west-1` Lorsque vous spécifiez la durée de la pause, assurez-vous de laisser suffisamment de temps pour la restaurat ion RMAN. Cela dépend de la taille de la base de données source. Modifiez donc la valeur 360 en conséquence. Assurez-vous également que la durée totale de l'automat isation suspendue ne coïncide pas avec la fenêtre de sauvegarde ou de maintenan ce de la base de données.	

Tâche	Description	Compétences requises

Créez et modifiez le fichier de paramètres pour PeopleSoft	Pour créer et modifier le fichier pour PeopleSoft, utilisez le fichier standard créé avec l'instance de base de données personnalisée Amazon RDS. Ajoutez les paramètres dont vous avez besoin PeopleSoft.
	1. Passez à `rds user rdsdb` en exécutant la commande suivante.
	`$ sudo su - rdsdb`
	2. Connectez-vous à SQL*Plus sur la base de données de départ et créez le fichier pfile en exécutant la commande suivante.
	`SQL> create pfile from spfile;`
	Cela crée le fichier dans. `$ORACLE_HOME/dbs`
	3. Effectuez une sauvegarde de ce fichier.
	4. Modifiez le fichier pour ajouter ou mettre à jour des PeopleSoft paramètres.
	`*._gby_hash_aggregation_enabled=false`
	`*._unnest_subquery=false`
		DBA

Tâche	Description	Compétences requises
	``` *.nls_language=' AMERICAN' *.nls_length_sem antics='CHAR' *.nls_territ ory='AMERICA' *.open_cursors=1000 *.db_files=1200 *.undo_tablespace=' UNDOTBS1' ``` PeopleSoft les paramètres associés se trouvent dans la note de support Oracle 1100831.1. 5. Supprimez la référence spfile du fichier. ``` *.spfile='/rdsdbbi n/oracle/dbs/spfil eFSDMO92.ora' ```	

Tâche	Description	Compétences requises

Supprimez la base de données de départ.	Pour supprimer la base de données personnalisée Amazon RDS existante, utilisez le code suivant.
	`$ sqlplus / as sysdba`
	`SQL> shutdown immediate ;`
	`SQL> startup mount exclusive restrict;`
	`SQL> drop database;`
	`SQL> exit`	

Tâche	Description	Compétences requises

Restaurez la base de données personnalisée Amazon RDS à partir de la sauvegarde.	Restaurez la base de données à l'aide du script suivant. Le script restaurera d'abord le fichier de contrôle, puis l'intégralité de la base de données à partir des éléments de sauvegarde stockés sur le support EFS.
	
	`#!/bin/bash`
	`Dt=`date +'%Y%m%d-%H%M'``
	`BACKUP_LOG="rman-${ORACLE_SID}-$Dt"`
	`export TAGDATE=`date +%Y%m%d%H%M`;`
	`LOGPATH=/rdsdbdata/scripts/logs`
	`rman target / >> $LOGPATH/rman-${ORACLE_SID}-$Dt << EOF`
	`restore controlfile from "/efs/rman_backup/FSCM/FSDMO92_20220713_12_1_CONTROL";`
	`alter database mount;`
	`run`
	`{`
	`set newname for database to '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b';`
	`SET NEWNAME FOR TEMPFILE 1 TO '/rdsdbdata/db/FSDMO92_A/datafile/%f_%b';`
	`RESTORE DATABASE;`
	`SWITCH DATAFILE ALL;`
	`SWITCH TEMPFILE ALL;`
		DBA

Tâche	Description	Compétences requises
	RECOVER DATABASE; } EOF sqlplus / as sysdba >> $LOGPATH/rman-${OR ACLE_SID}-$Dt<<-EOF ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 1.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo01.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 2.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo02.log'; ALTER DATABASE RENAME FILE '/u01/psoft/db/ oradata/FSDMO92/redo0 3.log' TO '/rdsdbda ta/db/FSDMO92_A/on linelog/redo03.log'; alter database clear unarchived logfile group 1; alter database clear unarchived logfile group 2; alter database clear unarchived logfile group 3; alter database open resetlogs; EXIT EOF	

Récupérez les mots de passe depuis Secrets Manager, créez des utilisateurs et modifiez les mots de passe

Tâche	Description	Compétences requises
Récupérez le mot de passe dans Secrets Manager.	Vous pouvez effectuer cette étape à l'aide de la console AWS ou de l'interface de ligne de commande AWS. Les étapes suivantes indiquent les instructions relatives à la console. 1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon RDS. 2. Dans le volet de navigation, choisissez Databases, puis sélectionnez la base de données Amazon RDS. 3. Choisissez l'onglet Configuration et notez l'ID de ressource de l'instance. Il sera au format `db-<ID>` (par exemple,`db-73GJNHLGDNZNDOXNWXSECUW6LE`). 4. Ouvrez la console Secrets Manager. 5. Choisissez le secret qui porte le même nom que`do-not-delete-custom-<resource_id>` , où `resource-id` fait référence à l'ID de	DBA

Tâche	Description	Compétences requises
	ressource que vous avez noté à l'étape 3. 6. Choisissez Retrieve secret value (Récupérer la valeur d'un secret). Ce mot de passe sera le même pour les `admin` utilisateurs `sys` `systemrdsadmin`,, et.	

Tâche	Description	Compétences requises
Créez l'utilisateur RDSADMIN.	`RDSADMIN`est l'utilisateur de base de données chargé de surveiller et d'orchestrer l'instance de base de données personnalisée Amazon RDS. Étant donné que la base de données de départ a été supprimée et que la base de données cible a été restaurée à partir de la source à l'aide de RMAN, vous devez recréer cet utilisateur après l'opérati on de restauration pour vous assurer que la surveillance personnalisée Amazon RDS fonctionne comme prévu. Vous devez également créer un profil et un espace disque logique distincts pour l'`RDSADMIN`utilisateur. 1. Entrez les commandes suivantes à l'invite SQL. `SQL> set echo on feedback on serverout on SQL> @?/rdbms/admin/utlpwdmg.sql SQL> ALTER PROFILE DEFAULT LIMIT FAILED_LOGIN_ ATTEMPTS UNLIMITED PASSWORD_LIFE_TIME UNLIMITED`	DBA

Tâche	Description	Compétences requises
	PASSWORD_VERIFY_F UNCTION NULL; 2. Créez le profilRDSADMIN. SQL> set echo on feedback on serverout on SQL> alter session set "_oracle_script"=t rue; SQL> CREATE PROFILE RDSADMIN LIMIT COMPOSITE_LIMIT UNLIMITED SESSIONS_PER_USER UNLIMITED CPU_PER_SESSION UNLIMITED CPU_PER_CALL UNLIMITED LOGICAL_READS_PER _SESSION UNLIMITED LOGICAL_READS_PER _CALL UNLIMITED IDLE_TIME UNLIMITED CONNECT_TIME UNLIMITED PRIVATE_SGA UNLIMITED FAILED_LOGIN_ATTE MPTS 10 PASSWORD_LIFE_TIME UNLIMITED PASSWORD_REUSE_TIME UNLIMITED PASSWORD_REUSE_MAX UNLIMITED PASSWORD_VERIFY_F UNCTION NULL	

Tâche	Description	Compétences requises
	PASSWORD_LOCK_TIME 86400/86400 PASSWORD_GRACE_TIME 604800/86400; 3. Créez le RDSADMIN tablespace. SQL> CREATE BIGFILE TABLESPACE rdsadmin '/rdsdbdata/db/FSDMO92_A/datafile/rdsadmin.dbf' DATAFILE SIZE 7M AUTOEXTEND ON NEXT 1m LOGGING ONLINE PERMANENT BLOCKSIZE 8192 EXTENT MANAGEMENT LOCAL AUTOALLOCATE DEFAULT NOCOMPRESS SEGMENT SPACE MANAGEMENT AUTO; 4. Créez l'RDSADMINutilisateur. Remplacez le RDSADMIN mot de passe par le mot de passe que vous avez obtenu précédemment auprès de Secrets Manager. SQL> CREATE USER rdsadmin IDENTIFIED BY xxxxxxxxxx DEFAULT TABLESPACE rdsadmin TEMPORARY TABLESPACE TEMP profile rdsadmin ;	

Tâche	Description	Compétences requises

	5. Accordez des privilèges à RDSADMIN.
	
	`SQL> GRANT "CONNECT" TO RDSADMIN WITH ADMIN OPTION;`
	`SQL> GRANT "RESOURCE" TO RDSADMIN WITH ADMIN OPTION;`
	`SQL> GRANT "DBA" TO RDSADMIN;`
	`SQL> GRANT "SELECT_CATALOG_ROLE" TO RDSADMIN WITH ADMIN OPTION;`
	`SQL> GRANT ALTER SYSTEM TO RDSADMIN;`
	`SQL> GRANT UNLIMITED TABLESPACE TO RDSADMIN;`
	`SQL> GRANT SELECT ANY TABLE TO RDSADMIN;`
	`SQL> GRANT ALTER DATABASE TO RDSADMIN;`
	`SQL> GRANT ADMINISTER DATABASE TRIGGER TO RDSADMIN;`
	`SQL> GRANT ANY OBJECT PRIVILEGE TO RDSADMIN WITH ADMIN OPTION;`
	`SQL> GRANT INHERIT ANY PRIVILEGES TO RDSADMIN;`
	`SQL> ALTER USER RDSADMIN DEFAULT ROLE ALL;`
	
	6. Set the SYS, SYSTEM, and DBSNMP	

Tâche	Description	Compétences requises

	user profiles to RDSADMIN.
	
	`SQL> set echo on`
	`feedback on serverout`
	`on`
	`SQL> alter user SYS`
	`profile RDSADMIN;`
	`SQL> alter user SYSTEM`
	`profile RDSADMIN;`
	`SQL> alter user DBSNMP`
	`profile RDSADMIN;`	

Créez l'utilisateur principal.	Étant donné que la base de données de départ a été supprimée et que la base de données cible a été restaurée à partir de la source à l'aide de RMAN, vous devez recréer l'utilisateur principal. Dans cet exemple, le nom d'utilisateur principal est `admin`.
	
	`SQL> create user`
	`admin identified by`
	`<password>;`
	`SQL> grant dba to admin`
		DBA

Tâche	Description	Compétences requises

Modifiez les mots de passe du système.	Modifiez les mots de passe du système en utilisant le mot de passe que vous avez récupéré dans Secrets Manager.
	
	`SQL> alter user sys identified by xxxxxxxxxx;`
	`SQL> alter user system identified by xxxxxxxxxx;`
	
	Si vous ne modifiez pas ces mots de passe, Amazon RDS Custom affiche le message d'erreur suivant : « L'utilisateur de surveillance de la base de données ou les informations d'identification de l'utilisateur ont changé ».
		DBA

Configurez les entrées TNS pour Amazon RDS Custom et PeopleSoft

Tâche	Description	Compétences requises
Configurez le fichier tnsnames.	Pour vous connecter à la base de données depuis le niveau application, configure z le `tnsnames.ora` fichier de manière à pouvoir vous connecter à la base de données depuis le niveau application. Dans l'exemple suivant, vous pouvez voir qu'il existe un lien logiciel vers le	DBA

Tâche	Description	Compétences requises

	`tnsnames.ora` fichier, mais le fichier est vide par défaut.
	
	`$ cd /rdsdbbin/oracle/network/admin`
	`$ ls -ltr`
	`-rw-r--r-- 1 rdsdb database 1536 Feb 14 2018 shrept.lst`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 listener.ora -> /rdsdbdata/config/listener.ora`
	`lrwxrwxrwx 1 rdsdb database 28 Apr 5 13:19 sqlnet.ora -> /rdsdbdata/config/sqlnet.ora`
	`lrwxrwxrwx 1 rdsdb database 30 Apr 5 13:19 tnsnames.ora -> /rdsdbdata/config/tnsnames.ora`
	
	1. Créez l'`tsnames.ora` entrée. En raison de la façon dont Amazon RDS automatise les fichiers, vous devez vous assurer que l'entrée ne contient pas d'espaces blancs, de commentaires ou de lignes supplémentaires. Sinon, vous risquez de rencontrer des problèmes lors de l'utilisation de certains d'entre APIs eux, tels que	

Tâche	Description	Compétences requises

	create-db-instance-read - replica.
	2. Remplacez le port, l'hôte et le SID conformém ent aux exigences de votre PeopleSoft base de données. Utilisez le code suivant comme exemple.
	`$ vi tnsnames.ora`
	`FSDMO92=(DESCRIP TION = (ADDRESS_ LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_ DATA = (SERVER = DEDICATED) (SID = FSDMO92)))`
	3. Pour vérifier que la PeopleSoft base de données est accessible, exécutez la commande suivante.
	`$ tnsping FSDMO92`
	`TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on 14- JUL-2022 10:16:45`
	`Copyright (c) 1997, 2021, Oracle. All rights reserved.`	

Tâche	Description	Compétences requises
	Used parameter files: /rdsdbbin/oracle/network/admin/sqlnet.ora Used TNSNAMES adapter to resolve the alias Attempting to contact (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = x.x.x.x)(PORT = 1521))) (CONNECT_DATA = (SERVER = DEDICATED) (SID = FSDMO92))) OK (0 msec)	

Créez le lien souple spfile

Tâche	Description	Compétences requises
Créez le lien souple spfile.	1. Pour créer un fichier spfile à cet emplacement/ `rdsdbdata/admin/FSDMO92/pfile` , exécutez la commande suivante. `SQL> create spfile='/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' from pfile;` 2. Accédez au `$ORACLE_HOME/dbs` fichier spfile et	DBA

Tâche	Description	Compétences requises
	créez un lien souple pour celui-ci. `ln -s '/rdsdbdata/admin/FSDMO92/pfile/spfileFSDMO92.ora' spfileFSDMO92.ora` 3. Une fois ce fichier créé, vous pouvez arrêter et démarrer la base de données à l'aide du fichier spfile.	

Exécuter les étapes postérieures à la migration

Tâche	Description	Compétences requises
Validez le schéma, les connexions et les tâches de maintenance.	Pour finaliser la migration, effectuez les tâches suivantes. • Collectez les statistiques du schéma. • Assurez-vous que le niveau PeopleSoft application peut se connecter à la nouvelle base de données personnalisée Amazon RDS. • Configurez vos programmes de sauvegarde et de maintenance.	DBA

Ressources connexes

- Utilisation d'Amazon RDS Custom

- Amazon RDS Custom pour Oracle — Nouvelles fonctionnalités de contrôle dans l'environnement de base de données (article de blog)
- Intégrer Amazon RDS Custom pour Oracle à Amazon EFS (article de blog)
- Configuration d'Amazon RDS en tant que PeopleSoft base de données Oracle (livre blanc AWS)

Migrer la fonctionnalité Oracle ROWID vers PostgreSQL sur AWS

Créée par Rakesh Raghav (AWS) et Ramesh Pathuri (AWS)

Récapitulatif

Ce modèle décrit les options de migration de la fonctionnalité de `ROWID` pseudocolonne d'Oracle Database vers une base de données PostgreSQL dans Amazon Relational Database Service (Amazon RDS) pour PostgreSQL, Amazon Aurora PostgreSQL Compatible Edition ou Amazon Elastic Compute Cloud (Amazon). EC2

Dans une base de données Oracle, la `ROWID` pseudocolonne est l'adresse physique d'une ligne d'une table. Cette pseudocolonne est utilisée pour identifier une ligne de manière unique même si la clé primaire n'est pas présente sur une table. PostgreSQL possède une pseudocolonne similaire `ctid` appelée, mais elle ne peut pas être utilisée en tant que. `ROWID` Comme expliqué dans la documentation de PostgreSQL`ctid`, cela peut changer en cas de mise à jour ou après chaque processus. `VACUUM`

Vous pouvez créer la fonctionnalité de `ROWID` pseudocolonne de trois manières dans PostgreSQL :

- Utilisez une colonne de clé primaire plutôt `ROWID` que pour identifier une ligne dans un tableau.
- Utilisez une clé primaire/unique logique (qui peut être une clé composite) dans la table.
- Ajoutez une colonne avec des valeurs générées automatiquement et faites-en une clé primaire/unique à imiter. `ROWID`

Ce modèle vous guide à travers les trois implémentations et décrit les avantages et les inconvénients de chaque option.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Expertise en codage Language/PostgreSQL (PL/pgSQL (procédural)
- Base de données Oracle source
- Un cluster compatible avec Amazon RDS for PostgreSQL ou Aurora PostgreSQL, ou une instance pour héberger la base de données PostgreSQL EC2

Limites

- Ce modèle fournit des solutions de contournement pour cette fonctionnalité. `ROWID` PostgreSQL ne fournit pas d'équivalent `ROWID` à Oracle Database.

Versions du produit

- PostgreSQL 11.9 ou version ultérieure

Architecture

Pile technologique source

- Oracle Database

Pile technologique cible

- Compatible avec Aurora PostgreSQL, Amazon RDS for PostgreSQL ou instance avec une base de données PostgreSQL EC2

Options de mise en œuvre

Il existe trois options pour contourner le manque de `ROWID` support dans PostgreSQL, selon que votre table possède une clé primaire ou un index unique, une clé primaire logique ou un attribut d'identité. Votre choix dépend du calendrier de votre projet, de votre phase de migration en cours et des dépendances vis-à-vis du code de l'application et de la base de données.

Option	Description	Avantages	Inconvénients
Clé primaire ou index unique	Si votre table Oracle possède une clé primaire, vous pouvez utiliser les attributs de cette clé pour identifier une ligne de manière unique.	• Aucune dépendance à l'égard des fonctionnalités de base de données propriétaires. • Impact minimal sur les performances,	• Nécessite des modifications du code de l'application et de la base de données qui repose sur le passage `ROWID`

		car les champs de clé primaire sont indexés.	aux champs de clé primaire.
Clé principale/unique logique	Si votre table Oracle possède une clé primaire logique, vous pouvez utiliser les attributs de cette clé pour identifier une ligne de manière unique. Une clé primaire logique est constituée d'un attribut ou d'un ensemble d'attributs qui peuvent identifier une ligne de manière unique, mais qui n'est pas imposée à la base de données par le biais d'une contrainte.	• Aucune dépendance à l'égard des fonctionnalités de base de données propriétaires.	• Nécessite des modifications du code de l'application et de la base de données qui repose sur le passage `ROWID` aux champs de clé primaire. • Impact significatif sur les performances si les attributs de la clé primaire logique ne sont pas indexés. Toutefois, vous pouvez ajouter un index unique pour éviter les problèmes de performances.

Attribut d'identité	si votre table Oracle ne possède pas de clé primaire, vous pouvez créer un champ supplémentaire en tant que`GENERATED ALWAYS AS IDENTITY`. Cet attribut génère une valeur unique chaque fois que des données sont insérées dans la table. Il peut donc être utilisé pour identifier de manière unique une ligne pour les opérations DML (Data Manipulation Language).	• Aucune dépendance à l'égard des fonctionnalités de base de données propriétaires. • La base de données PostgreSQL renseigne l'attribut et conserve son caractère unique.	• Nécessite des modifications du code de l'application et de la base de données sur `ROWID` lequel repose le passage à l'attribut d'identité. • Impact significatif sur les performances si le champ supplémentaire n'est pas indexé. Vous pouvez toutefois ajouter un index pour éviter les problèmes de performances.

Outils

- Amazon Relational Database Service (Amazon RDS) pour PostgreSQL vous aide à configurer, exploiter et dimensionner une base de données relationnelle PostgreSQL dans le cloud AWS.
- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande. Dans ce modèle, vous pouvez utiliser l'interface de ligne de commande AWS pour exécuter des commandes SQL via pgAdmin.
- pgAdmin est un outil de gestion open source pour PostgreSQL. Il fournit une interface graphique qui vous permet de créer, de gérer et d'utiliser des objets de base de données.

- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Épopées

Identifier les tables sources

Tâche	Description	Compétences requises
Identifiez les tables Oracle qui utilisent `ROWID` cet attribut.	Utilisez l'outil AWS Schema Conversion Tool (AWS SCT) pour identifier les tables Oracle dotées de `ROWID` fonctionnalités. Pour plus d'informations, consultez la documentation AWS SCT. —ou— Dans Oracle, utilisez la `DBA_TAB_COLUMNS` vue pour identifier les tables dotées d'un `ROWID` attribut. Ces champs peuvent être utilisés pour stocker des caractères alphanumériques de 10 octets. Déterminez l'utilisation et convertissez-les en `VARCHAR` champ, le cas échéant.	DBA ou développeur
Identifiez le code qui fait référence à ces tables.	Utilisez AWS SCT pour générer un rapport d'évaluation de la migration afin d'identifier les procédures concernées par`ROWID`. Pour	DBA ou développeur

Tâche	Description	Compétences requises
	plus d'informations, consultez la documentation AWS SCT. —ou— Dans la base de données Oracle source, utilisez le champ de texte du `dba_source` tableau pour identifier les objets qui utilisent des `ROWID` fonctionnalités.	

Déterminer l'utilisation des clés primaires

Tâche	Description	Compétences requises
Identifiez les tables dépourvues de clés primaires.	Dans la base de données Oracle source, utilisez `DBA_CONSTRAINTS` pour identifier les tables dépourvues de clés primaires. Ces informations vous aideront à déterminer la stratégie pour chaque table. Par exemple : `select dt.* from dba_tables dt where not exists (select 1 from all_constraints ct where ct.owner = Dt.owner and ct.table_name = Dt.table_name`	DBA ou développeur

Tâche	Description	Compétences requises

	<pre>and
	ct.constraint_type =
	'P'
	)
	and dt.owner = '{schema}
	'</pre>	

Identifier et appliquer la solution

Tâche	Description	Compétences requises
Appliquez les modifications aux tables dotées d'une clé primaire définie ou logique.	Apportez les modifications au code de l'application et de la base de données indiquées dans la section Informations supplémentaires pour utiliser une clé primaire unique ou une clé primaire logique afin d'identifier une ligne de votre table.	DBA ou développeur
Ajoutez un champ supplémentaire aux tables qui ne possèdent pas de clé primaire définie ou logique.	Ajoutez un attribut de type`GENERATED ALWAYS AS IDENTITY`. Apportez les modifications au code de l'application et de la base de données indiquées dans la section Informations supplémentaires.	DBA ou développeur
Ajoutez un index si nécessaire.	Ajoutez un index au champ supplémentaire ou à la clé primaire logique pour améliorer les performances SQL.	DBA ou développeur

Ressources connexes

- CTID de PostgreSQL (documentation de PostgreSQL)
- Colonnes générées (documentation PostgreSQL)
- Pseudocolonne ROWID (documentation Oracle)

Informations supplémentaires

Les sections suivantes fournissent des exemples de code Oracle et PostgreSQL pour illustrer les trois approches.

Scénario 1 : utilisation d'une clé primaire unique

Dans les exemples suivants, vous créez la table `testrowid_s1` avec `emp_id` comme clé primaire.

Code Oracle :

```
create table testrowid_s1 (emp_id integer, name varchar2(10), CONSTRAINT testrowid_pk
 PRIMARY KEY (emp_id));
INSERT INTO testrowid_s1(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s1(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s1(emp_id,name) values (3,'empname3');
INSERT INTO testrowid_s1(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 empname2
AAAF3pAAAAAAAMOAAC          3 empname3
AAAF3pAAAAAAAMOAAD          4 empname4

UPDATE testrowid_s1 SET name = 'Ramesh' WHERE rowid = 'AAAF3pAAAAAAAMOAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s1;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3pAAAAAAAMOAAA          1 empname1
AAAF3pAAAAAAAMOAAB          2 Ramesh
AAAF3pAAAAAAAMOAAC          3 empname3
```

```
AAAF3pAAAAAAAM0AAD          4 empname4
```

Code PostgreSQL :

```
CREATE TABLE public.testrowid_s1
(
    emp_id integer,
    name character varying,
    primary key (emp_id)
);

insert into public.testrowid_s1 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s1 set name = 'Ramesh' where emp_id = 2 ;

select emp_id,name from testrowid_s1;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Scénario 2 : utilisation d'une clé primaire logique

Dans les exemples suivants, vous créez la table `testrowid_s2` avec `emp_id` comme clé primaire logique.

Code Oracle :

```
create table testrowid_s2 (emp_id integer, name varchar2(10) );
INSERT INTO testrowid_s2(emp_id,name) values (1,'empname1');
INSERT INTO testrowid_s2(emp_id,name) values (2,'empname2');
INSERT INTO testrowid_s2(emp_id,name) values (3,'empname3');
```

```
INSERT INTO testrowid_s2(emp_id,name) values (4,'empname4');
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 empname2
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4

UPDATE testrowid_s2 SET name = 'Ramesh' WHERE rowid = 'AAAF3rAAAAAAAMeAAB' ;
commit;

SELECT rowid,emp_id,name FROM testrowid_s2;
ROWID                  EMP_ID NAME
------------------ ---------- ----------
AAAF3rAAAAAAAMeAAA          1 empname1
AAAF3rAAAAAAAMeAAB          2 Ramesh
AAAF3rAAAAAAAMeAAC          3 empname3
AAAF3rAAAAAAAMeAAD          4 empname4
```

Code PostgreSQL :

```
CREATE TABLE public.testrowid_s2
(
    emp_id integer,
    name character varying
);

insert into public.testrowid_s2 (emp_id,name) values
(1,'empname1'),(2,'empname2'),(3,'empname3'),(4,'empname4');

select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      2 | empname2
      3 | empname3
      4 | empname4

update testrowid_s2 set name = 'Ramesh' where emp_id = 2 ;
```

```
select emp_id,name from testrowid_s2;
 emp_id |   name
--------+----------
      1 | empname1
      3 | empname3
      4 | empname4
      2 | Ramesh
```

Scénario 3 : utilisation d'un attribut d'identité

Dans les exemples suivants, vous créez la table `testrowid_s3` sans clé primaire et en utilisant un attribut d'identité.

Code Oracle :

```
create table testrowid_s3 (name varchar2(10));
INSERT INTO testrowid_s3(name) values ('empname1');
INSERT INTO testrowid_s3(name) values ('empname2');
INSERT INTO testrowid_s3(name) values ('empname3');
INSERT INTO testrowid_s3(name) values ('empname4');
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB empname2
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4

UPDATE testrowid_s3 SET name = 'Ramesh' WHERE rowid = 'AAAF3sAAAAAAAMmAAB' ;
commit;

SELECT rowid,name FROM testrowid_s3;
ROWID              NAME
------------------ ----------
AAAF3sAAAAAAAMmAAA empname1
AAAF3sAAAAAAAMmAAB Ramesh
AAAF3sAAAAAAAMmAAC empname3
AAAF3sAAAAAAAMmAAD empname4
```

Code PostgreSQL :

```
CREATE TABLE public.testrowid_s3
(
    rowid_seq bigint generated always as identity,
    name character varying
);

insert into public.testrowid_s3 (name) values
('empname1'),('empname2'),('empname3'),('empname4');

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         2 | empname2
         3 | empname3
         4 | empname4

update testrowid_s3 set name = 'Ramesh' where rowid_seq = 2 ;

select rowid_seq,name from testrowid_s3;
 rowid_seq |   name
-----------+----------
         1 | empname1
         3 | empname3
         4 | empname4
         2 | Ramesh
```

Migrer les codes d'erreur de la base de données Oracle vers une base de données compatible avec Amazon Aurora PostgreSQL

Créée par Sai Parthasaradhi (AWS) et Veeranjaneyulu Grandhi (AWS)

Récapitulatif

Ce modèle montre comment migrer les codes d'erreur de base de données Oracle vers une base de données Amazon Aurora PostgreSQL Edition compatible à l'aide d'une table de métadonnées prédéfinie.

Les codes d'erreur de base de données Oracle ne sont pas toujours associés à un code d'erreur PostgreSQL correspondant. Cette différence de codes d'erreur peut rendre difficile la configuration de la logique de traitement des procédures ou des fonctions dans l'architecture PostgreSQL cible.

Vous pouvez simplifier le processus en stockant les codes d'erreur de base de données source et cible pertinents pour votre programme PL/pgSQL dans une table de métadonnées. Configurez ensuite la table pour signaler les codes d'erreur valides de la base de données Oracle et les mapper à leurs équivalents PostgreSQL avant de poursuivre avec la logique de processus restante. Si le code d'erreur de la base de données Oracle ne figure pas dans la table de métadonnées, le processus se termine à une exception près. Vous pouvez ensuite examiner manuellement les détails de l'erreur et ajouter le nouveau code d'erreur au tableau si votre programme l'exige.

Grâce à cette configuration, votre base de données compatible avec Amazon Aurora PostgreSQL peut gérer les erreurs de la même manière que votre base de données Oracle source.

> **Note**
>
> La configuration d'une base de données PostgreSQL pour gérer correctement les codes d'erreur de base de données Oracle nécessite généralement de modifier le code de base de données et d'application.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle source avec des services d'instance et d'écoute opérationnels
- Un cluster compatible avec Amazon Aurora PostgreSQL qui est opérationnel

- Connaissance d'Oracle Database
- Connaissance des bases de données PostgreSQL

Architecture

Le schéma suivant montre un exemple de flux de travail de base de données compatible avec Amazon Aurora PostgreSQL pour la validation et le traitement des codes d'erreur relatifs aux données :

Le schéma suivant illustre le flux de travail suivant :

1. Une table contient les codes d'erreur et les classifications de la base de données Oracle ainsi que leurs codes d'erreur et classifications PostgreSQL équivalents. La table inclut une colonne valid_error qui classe si des codes d'erreur spécifiques prédéfinis sont valides ou non.
2. Lorsqu'une fonction PL/pgSQL (func_processdata) lance une exception, elle invoque une deuxième fonction PL/pgSQL (error_validation).
3. La fonction error_validation accepte le code d'erreur de la base de données Oracle comme argument d'entrée. Ensuite, la fonction compare le code d'erreur entrant au tableau pour voir si l'erreur est incluse dans le tableau.
4. Si le code d'erreur de la base de données Oracle est inclus dans la table, la fonction error_validation renvoie une valeur VRAIE et la logique du processus se poursuit. Si le code d'erreur n'est pas inclus dans le tableau, la fonction renvoie une valeur FALSE et la logique du processus s'arrête avec une exception.
5. Lorsque la fonction renvoie une valeur FAUSSE, les détails de l'erreur sont examinés manuellement par le responsable fonctionnel de l'application afin de déterminer sa validité.
6. Le nouveau code d'erreur est ensuite ajouté manuellement au tableau ou non. Si le code d'erreur est valide et ajouté à la table, la fonction error_validation renvoie une valeur TRUE la prochaine fois que l'exception se produira. Si le code d'erreur n'est pas valide et que le processus doit échouer lorsque l'exception se produit, le code d'erreur n'est pas ajouté au tableau.

Pile technologique

- Amazon Aurora PostgreSQL
- pgAdmin
- Oracle SQL Developer

Outils

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- pgAdmin est un outil d'administration et de développement open source pour PostgreSQL. Il fournit une interface graphique qui simplifie la création, la maintenance et l'utilisation des objets de base de données.
- Oracle SQL Developer est un environnement de développement intégré gratuit qui simplifie le développement et la gestion d'Oracle Database dans les déploiements traditionnels et dans le cloud.

Épopées

Migrez les codes d'erreur de la base de données Oracle vers votre base de données compatible avec Amazon Aurora PostgreSQL

Tâche	Description	Compétences requises

Créez une table dans la base de données compatible avec Amazon Aurora PostgreSQL.	Exécutez la commande PostgreSQL CREATE TABLE suivante :
	`(`
	`source_error_code numeric NOT NULL,`
	`target_error_code character varying NOT NULL,`
	`valid_error character varying(1) NOT NULL`
	`);`
		Développeur PostgreSQL, Oracle, RDS/Aurora pour PostgreSQL

Tâche	Description	Compétences requises

Ajoutez les codes d'erreur PostgreSQL et les codes d'erreur de base de données Oracle correspondants dans le tableau.	Exécutez la commande PostgreSQL INSERT pour ajouter les valeurs de code d'erreur requises à la table error_codes.
	
	Les codes d'erreur PostgreSQL doivent utiliser le type de données à caractère variable (valeur SQLSTATE). Les codes d'erreur Oracle doivent utiliser le type de données numérique (valeur SQLCODE).
	
	Exemple d'instructions Insérer :
	
	`insert into error_codes values (-1817,'22007','Y');`
	`insert into error_codes values (-1816,'22007','Y');`
	`insert into error_codes values (-3114,'08006','N');`
	
	Note
	Si vous détectez des exceptions de connectivité de base de données Java (JDBC) spécifiques à Oracle, vous devez les remplacer
		Développeur PostgreSQL, Oracle, RDS/Aurora pour PostgreSQL

Tâche	Description	Compétences requises
	par des exception s génériques entre bases de données ou passer à des exceptions spécifiques à PostgreSQL.	
Créez une fonction PL/pgSQL pour valider les codes d'erreur.	Créez une fonction PL/pgSQL en exécutant la commande PostgreSQL CREATE FUNCTION. Assurez-vous que la fonction effectue les opérations suivantes : • Accepte les codes d'erreur Oracle émis par un programme. • Vérifie si des codes d'erreur sont présents dans la table error_codes. • Renvoie une valeur TRUE ou FALSE, selon que le code d'erreur est présent ou non dans la table de métadonnées.	Développeur PostgreSQL, Oracle, RDS/Aurora pour PostgreSQL

Tâche	Description	Compétences requises
Vérifiez manuellement les nouveaux codes d'erreur tels qu'ils sont enregistrés par la fonction PL/pgSQL.	Vérifiez manuellement les nouveaux codes d'erreur. Si un nouveau code d'erreur est valide pour votre cas d'utilisation, ajoutez-le à la table error_codes en exécutant la commande PostgreSQL INSERT. -ou- Si un nouveau code d'erreur n'est pas valide pour votre cas d'utilisation, ne l'ajoutez pas au tableau. La logique du processus continuera à échouer et se terminera, sauf si l'erreur se produit.	Développeur PostgreSQL, Oracle, RDS/Aurora pour PostgreSQL

Ressources connexes

Annexe A. Codes d'erreur PostgreSQL (documentation PostgreSQL)

Messages d'erreur de base de données (documentation Oracle Database)

Migrer les charges de travail Redis vers Redis Enterprise Cloud sur AWS

Créée par Antony Prasad Thevaraj (AWS) et Srinivas Pendyala (Redis)

Récapitulatif

Ce modèle décrit le processus de haut niveau de migration des charges de travail Redis vers Redis Enterprise Cloud sur Amazon Web Services (AWS). Il décrit les étapes de migration, fournit des informations sur la sélection des outils disponibles et décrit les avantages, les inconvénients et les étapes d'utilisation de chaque outil. Si vous avez besoin d'une aide supplémentaire pour migrer des charges de travail depuis Redis, vous pouvez éventuellement faire appel aux services professionnels de Redis.

Si vous utilisez Redis OSS ou Redis Enterprise Software sur site, vous connaissez les coûts administratifs importants et la complexité opérationnelle liés à la maintenance de vos bases de données Redis dans votre centre de données. En migrant vos charges de travail vers le cloud, vous pouvez réduire considérablement cette charge opérationnelle et tirer parti de Redis Enterprise Cloud, une base de données en tant que service (DBaaS) entièrement hébergée proposée par Redis. Cette migration permet d'accroître l'agilité de votre entreprise, d'améliorer la fiabilité des applications et de réduire les coûts globaux tout en vous donnant accès aux dernières fonctionnalités de Redis Enterprise Cloud sur AWS, telles que la disponibilité de 99,999 %, la simplicité architecturale et l'évolutivité.

Il existe des applications potentielles pour Redis Enterprise Cloud dans les secteurs des services financiers, de la vente au détail, de la santé et des jeux, ainsi que dans les cas d'utilisation nécessitant des solutions pour la détection des fraudes, l'inventaire en temps réel, le traitement des réclamations et la gestion des sessions. Vous pouvez utiliser Redis Enterprise Cloud pour vous connecter à vos ressources AWS, par exemple à un serveur d'applications qui s'exécute sur des instances Amazon Elastic Compute Cloud (Amazon EC2) ou à un microservice déployé en tant que service AWS Lambda.

Conditions préalables et limitations

Hypothèses

- Vous utilisez actuellement un système de base de données sur site que vous souhaitez migrer vers le cloud.
- Vous avez identifié les exigences de migration pour vos charges de travail, notamment :
  - Exigences relatives à la cohérence des données

- Exigences relatives à l'infrastructure et à l'environnement du système
- Exigences en matière de mappage et de transformation des données
- Exigences relatives aux tests fonctionnels
- Exigences relatives aux essais de performance
- Exigences de validation
- Stratégie de transition définie

- Vous avez évalué les délais et les estimations de coûts nécessaires à la migration.
- Vos exigences tiennent compte de l'étendue du travail ainsi que des systèmes et bases de données que vous avez identifiés comme participant à la migration.
- Vous avez identifié les parties prenantes ainsi que leurs rôles et responsabilités dans une matrice responsable, responsable, consultée et informée (RACI).
- Vous avez reçu l'accord et les approbations nécessaires de la part de toutes les parties prenantes.

Coût

En fonction des spécifications techniques de votre base de données source existante (par exemple, le dimensionnement de la mémoire, le débit et la taille totale des données), un architecte de solutions Redis peut dimensionner le système cible sur Redis Enterprise Cloud. Pour obtenir des informations générales sur les prix, consultez la section Tarification Redis sur le site Web de Redis.

Personnel et compétences

Le processus de migration implique les rôles et responsabilités suivants.

Rôle	Description	Compétences requises
Architecte de solutions de migration	Un architecte technique spécialisé dans la définition, la planification et la mise en œuvre de stratégies de migration	Compréhension technique et applicative des systèmes source et cible ; expérience de la migration des charges de travail vers le cloud
Architecte de données	Architecte technique possédant une vaste expérience dans la définition, la mise en œuvre et la	Modélisation des données structurées et non structurées, compréhension approfondie et expérience de la mise en

	fourniture de solutions de données pour une grande variété de bases de données	œuvre de bases de données pour une entreprise
Architecte de solutions Redis	Un architecte technique qui peut vous aider à concevoir un cluster Redis de taille optimale pour le cas d'utilisation approprié	Expertise dans l'architecture et le déploiement de solutions Redis pour une grande variété de cas d'utilisation
Architecte de solutions cloud	Un architecte technique qui possède une connaissance approfondie des solutions cloud, en particulier sur AWS	Expertise en architecture de solutions pour le cloud ; expérience en matière de migration de charges de travail et de modernisation des applications
Architecte d'entreprise	Un architecte technique qui possède une compréhension complète du paysage technique de votre organisation, qui partage une vision commune de la future feuille de route, et qui met en pratique et établit les meilleures pratiques architecturales standardisées au sein de toutes les équipes de votre organisation	Certifications en architecture logicielle telles que TOGAF, compétences de base en génie logiciel et expertise en architecture de solutions et en architecture d'entreprise

DevOps Ingénieur informatique ou informatique	Ingénieur responsable de la création et de la maintenance de l'infrastructure, notamment de la surveillance de l'infrastructure pour détecter les problèmes, de l'exécution des tâches de maintenance et de la mise à jour selon les besoins.	Bonne connaissance de diverses technologies, notamment des systèmes d'exploitation, des réseaux et du cloud computing ; connaissance des langages de programmation tels que Python, Bash et Ruby, ainsi que d'outils tels que Docker, Kubernetes et Ansible

Architecture

Options de migration

Le schéma suivant montre les options de migration de vos sources de données sur site (basées sur Redis ou autres) vers AWS. Il présente plusieurs outils de migration parmi lesquels vous pouvez choisir, tels que l'exportation de fichiers Redis Database (RDB) vers Amazon Simple Storage Service (Amazon S3), à l'aide de la fonction de réplication Redis ou à l'aide d'AWS DMS.

1. Sources de données locales : bases de données qui ne sont pas basées sur Redis, telles que MySQL, PostgreSQL, Oracle, SQL Server ou MariaDB.
2. Sources de données sur site : bases de données basées sur le protocole Redis, telles que Redis OSS et Redis Enterprise Software.
3. Le moyen le plus simple de migrer des données à partir de bases de données basées sur Redis consiste à exporter des fichiers RDB et à les importer dans le Redis Enterprise Cloud sur AWS cible.
4. Vous pouvez également migrer les données de la source vers la cible à l'aide de la fonctionnalité de réplication (`ReplicaOf`) de Redis.
5. Si vos exigences en matière de migration de données incluent la transformation de données, vous pouvez utiliser les outils d'entrée/sortie Redis (RIOT) pour migrer les données.
6. Vous pouvez également utiliser AWS Data Migration Service (AWS DMS) pour migrer les données à partir de bases de données SQL.
7. Vous devez utiliser le peering du cloud privé virtuel (VPC) pour AWS DMS afin de réussir la migration des données vers le Redis Enterprise Cloud sur AWS cible.

Architecture cible

Le schéma suivant montre une architecture de déploiement typique pour Redis Enterprise Cloud sur AWS et illustre comment elle peut être utilisée avec les principaux services AWS.

1. Vous pouvez vous connecter aux applications professionnelles soutenues par Redis Enterprise Cloud sur AWS.
2. Vous pouvez exécuter des applications métier dans votre propre compte AWS, dans un VPC associé à ce compte.
3. Vous pouvez utiliser les points de terminaison de base de données Redis Enterprise Cloud pour vous connecter à vos applications. Les exemples incluent un serveur d'applications exécuté sur des EC2 instances, un microservice déployé en tant que service AWS Lambda, une application Amazon Elastic Container Service (Amazon ECS) ou une application Amazon Elastic Kubernetes Service (Amazon EKS).
4. Les applications professionnelles exécutées dans votre VPC nécessitent une connexion homologue VPC au VPC Redis Enterprise Cloud. Cela permet aux applications professionnelles de se connecter en toute sécurité via des points de terminaison privés.
5. Redis Enterprise Cloud on AWS est une plateforme de base de données NoSQL en mémoire déployée en tant que S DBaa sur AWS et entièrement gérée par Redis.
6. Redis Enterprise Cloud est déployé au sein d'un VPC dans un compte AWS standard créé par Redis.
7. Pour des raisons de sécurité, Redis Enterprise Cloud est déployé dans un sous-réseau privé accessible à la fois sur des points de terminaison privés et publics. Nous vous recommandons de connecter vos applications clientes à Redis sur des points de terminaison privés. Si vous prévoyez d'utiliser un point de terminaison public, nous vous recommandons vivement d'activer le protocole TLS pour chiffrer les données entre vos applications clientes et Redis Enterprise Cloud.

La méthodologie de migration Redis s'aligne sur la méthodologie de migration AWS, qui est illustrée dans Mobilize your organization to accelerate large-scale migrations sur le site Web AWS Prescriptive Guidance.

Automatisation et mise à l'échelle

Les tâches de configuration de l'environnement pour la migration peuvent être automatisées via AWS Landing Zone et des modèles d'infrastructure en tant que code (IaC) à des fins d'automatisation et de mise à l'échelle. Elles sont abordées dans la section Epics de ce modèle.

Outils

En fonction de vos besoins en matière de migration de données, vous pouvez choisir parmi une sélection d'options technologiques pour migrer vos données vers Redis Enterprise Cloud sur AWS. Le tableau suivant décrit et compare ces outils.

Outil	Description	Avantages	Inconvénients
Exportation et importation de RDB	Vous exportez les données de la base de données source (par exemple, Redis OSS ou Redis Enterprise Software) sous forme de fichiers RDB. Si votre base de données est fournie via un cluster Redis OSS, vous exportez chaque partition principale vers une RDB. Vous importez ensuite tous les fichiers RDB en une seule étape. Si votre base de données source est basée sur un cluster OSS mais que votre base de données cible n'utilise pas l'API OSS Cluster, vous devez modifier le code source de votre application pour utiliser une bibliothè	• C'est simple. • Fonctionne avec n'importe quelle solution basée sur Redis capable d'exporter des données au format RDB en tant que source (y compris Redis OSS et Redis Enterprise Software). • Assure la cohérence des données grâce à un processus simple.	• Ne répond pas aux exigences de transformation des données et ne prend pas en charge les fusions de bases de données logiques. • Cela prend du temps pour les ensembles de données plus volumineux. • Aucune prise en charge de la migration vers le delta ne peut prolonger les temps d'arrêt.

	que cliente Redis standard.
	Les exigences relatives à la transformation des données ou aux fusions de bases de données logiques nécessitent un processus plus complexe, qui est expliqué dans la section Fusion logique de bases de données plus loin dans ce tableau.

Fonction de réplication Redis (actif-passif)	Vous pouvez répliquer en continu les données d'une base de données Redis OSS, Enterprise Software ou Enterprise Cloud vers une base de données Redis Enterprise Cloud. Après la synchronisation initiale, la fonction de réplication Redis (`ReplicaOf `) effectue une migration delta, ce qui signifie qu'il n'y a pratiquement aucun temps d'arrêt de l'application observé. La fonctionnalité de réplication Redis est destinée à être utilisée de manière active-passive. La cible est supposée passive et est entièrement resynchronisée (vidée et synchronisée à partir de la base de données source). Il est donc un peu plus compliqué de passer de la source à la cible.	• Supporte la réplication continue (chargement initial des données suivi de deltas). • Pratiquement aucun temps d'arrêt (dépend du délai de réplication). • Assure la cohérence des données.	• Un seul site est censé être actif, il est donc plus compliqué de passer d'un site à l'autre. • Prend en charge un maximum de 32 partitions principales lorsque vous migrez depuis un cluster OSS.

	Il est possible de répliquer depuis un cluster Redis OSS vers une base de données Redis Enterprise Cloud en cluster standard en spécifiant toutes les partitions principal es du cluster OSS comme sources. Cependant, la fonctionnalité de réplication Redis autorise un maximum de 32 bases de données sources.		
AWS DMS	Vous pouvez utiliser AWS DMS pour migrer les données de n'importe quelle base de données source prise en charge vers un magasin de données Redis cible avec un temps d'arrêt minimal. Pour plus d'informations, consultez la section Utilisation de Redis comme cible pour AWS DMS dans la documentation AWS DMS.	• Prend en charge la migration des sources de données NoSQL et SQL. • Fonctionne bien avec les autres services AWS. • Prend en charge les cas d'utilisa tion de la migration en direct et de la capture des données modifiées (CDC).	• Les valeurs clés Redis ne peuvent pas contenir de caractères spéciaux tels que %. • Ne prend pas en charge la migration de données contenant des caractères spéciaux dans les lignes ou dans les noms de champs. • Ne prend pas en charge le mode LOB (Full Large Binary Object).

Fusion logique de bases de données	Les exigences particulières en matière de fusion de bases de données peuvent nécessite r une solution de migration de données personnalisée. Par exemple, vous pouvez avoir quatre bases de données logiques (`SELECT 0..3`) dans Redis OSS, mais vous souhaiterez peut-être utiliser un seul point de terminaison de base de données au lieu de déplacer les données vers plusieurs bases de données Redis Enterprise Cloud. Redis Enterprise ne prend pas en charge les bases de données logiques sélection nables. Vous devrez donc transformer le modèle de données physique de la base de données source. Par exemple, vous pouvez mapper chaque index de base de données à un préfixe (`01`to `usrcmp`,	• Contrôle granulaire de la mise en forme des données lors de la migration vers le système cible à l'aide de scripts personnalisés.	• Si vous décidez de ne pas terminer la migration, la restauration peut s'avérer très difficile , en particulier si les données les plus récentes doivent être restaurées vers les systèmes sources. • Le coût de création peut être élevé si l'objectif est de créer une solution unique pour une migration unique. • Les coûts de maintenance liés au code, à l'infrast ructure, au temps de développe ment et à d'autres domaines peuvent être élevés si les exigences de migration changent fréquemment.

	to, etc.), puis utiliser un script de migration ou un outil d'extract ion, de transformation et de chargement (ETL) pour générer un fichier RDB, que vous pouvez ensuite importer dans la base de données cible.

En outre, vous pouvez utiliser les outils et services suivants d'AWS.

Outils d'évaluation et de découverte :

- AWS Application Discovery Service
- Évaluateur de migration

Outils de migration d'applications et de serveurs :

- AWS Application Migration Service

Outils de migration de base de données :

- Outil de conversion de schéma AWS (AWS SCT)
- Service de migration de base de données AWS (AWS DMS)

Outils de migration de données :

- AWS Storage Gateway
- AWS DataSync
- AWS Direct Connect
- AWS Snowball
- Amazon Data Firehose

Gestion de la migration :

- AWS Migration Hub

Solutions pour les partenaires AWS :

- AWS Migration Competency Partners

Épopées

Terminez les tâches de découverte et d'évaluation

Tâche	Description	Compétences requises
Identifiez les charges de travail.	Identifiez les charges de travail des candidats appropriés que vous souhaitez migrer. Tenez compte des points suivants avant de choisir une charge de travail à migrer : • Quel est l'intérêt commercial de migrer ou de ne pas migrer cette charge de travail ? • Existe-t-il un plan d'urgence en cas d'échec de la migration de cette charge de travail vers le système cible ? Idéalement, choisissez une charge de travail qui a un impact commercial maximal avec un minimum de risques. Maintenez le processus global	Architecte de données, champions commerciaux, sponsors de projets de migration

Tâche	Description	Compétences requises
	itératif et migrez par petits incréments.	
Identifier les sources de données et les exigences ; concevoir un modèle de données.	Redis organise un atelier pour accélérer la découvert e et définir la planification de la migration pour le projet. Dans le cadre de cet atelier, les équipes Redis identifient les sources de données et les exigences du modèle de données source, et analysent comment celles-ci peuvent être remodelées dans Redis Enterprise Cloud. L'équipe de migration Redis (services professionnels) réalise un exercice détaillé de conception de modèle de données avec votre organisat ion. Dans le cadre de cet exercice, l'équipe Redis a : • Identifie les structures de données Redis cibles. • Définit la stratégie de mappage des données. • Documente l'approche et les recommandations en matière de migration. • Révise et finalise le modèle de données avec les parties prenantes.	Architecte de solutions Redis

Tâche	Description	Compétences requises
Identifiez les caractéristiques de la base de données source.	Identifiez le produit Redis utilisé dans les environnements source et cible. Par exemple : • La base de données source est-elle une base de données OSS Cluster, une base de données Redis autonome ou une base de données Redis Enterprise ? • La base de données cible sera-t-elle une base de données standard Redis Enterprise ou une base de données compatible avec OSS Cluster ? • Quelles sont les implications concernant le code source de l'application ?	Architecte de données
Rassemblez le SLA actuel du système et les autres indicateurs de dimensionnement.	Déterminez les accords de niveau de service actuels (SLAs) exprimés en termes de débit (opérations par seconde), de latence, de taille de mémoire globale par base de données et d'exigences de haute disponibilité (HA).	Architecte de données

Tâche	Description	Compétences requises
Identifiez les caractéristiques du système cible.	Déterminez les réponses à ces questions : • Quelle quantité de données doit être migrée ? • Combien de temps faut-il pour migrer la quantité de données donnée ? • Quels sont les temps d'arrêt requis pour la migration ? Est-il acceptable que votre service ou application ne soit pas disponible pendant une période donnée ? Dans l'affirmative, pendant combien de temps ? • Dans quelle mesure les données migrées doivent-elles être cohérentes ? La base de données cible peut-elle être légèrement incohérente (obsolète) ? • Les données doivent-elles être transformées avant d'être chargées dans la base de données cible ? (Par exemple, vous souhaiterez peut-être convertir les index de base de données sélectionnables en préfixes avant la migration.) • La base de données source est-elle accessibl	Architecte de données, architecte de solutions Redis (facultatif)

Tâche	Description	Compétences requises
	e depuis l'hôte de la base de données cible (par exemple, depuis un VPC homologue ou depuis un point de terminaison public utilisant le chiffrement) ? • Réalisez un exercice de dimensionnement des données et de dimension nement du cluster Redis avec un architecte technique Redis. • Identifiez les exigences en matière de réseau, d'infrast ructure, de versions logiciell es et de licences logiciell es, et procurez-vous tous les composants avant la migration. • Le transfert de ces données pose-t-il des problèmes de sécurité ?	

Tâche	Description	Compétences requises
Identifiez les dépendances.	Identifiez les dépendanc es en amont et en aval du système actuel à migrer. Assurez-vous que le travail de migration est aligné sur les autres migrations de systèmes dépendants. Par exemple, si vous envisagez de migrer d'autres applications métiers sur site vers le cloud AWS, identifiez ces applications et alignez-les en fonction des objectifs, des délais et des parties prenantes du projet.	Architecte de données, architecte d'entreprise

Tâche	Description	Compétences requises
Identifiez les outils de migration.	En fonction de vos besoins en matière de migration de données (tels que les exigences relatives aux données sources ou aux temps d'arrêt), vous pouvez utiliser l'un des outils décrits précédemment dans la section Outils. De plus, vous pouvez utiliser : • Réplication bidirectionnelle (active-active) à l'aide du déploiement CRDB. • Scripts d'exportation/importation personnalisés (par exemple, à l'aide de `DUMP/RESTORE` commandes). • Outils d'exportation/importation supplémentaires et outils d'assistance tels que RIOT ou les outils ECstats2ETL. • Des outils IaC tels que Terraform ou des modèles AWS CloudFormation .	Architecte de solutions de migration, architecte de solutions Redis
Créez un plan d'urgence.	Établissez un plan d'urgence pour revenir en arrière, au cas où vous rencontreriez des problèmes lors de la migration.	Gestion de projet, équipes techniques, y compris l'architecte

Mener à bien les tâches de sécurité et de conformité

Tâche	Description	Compétences requises
Sécurisez la console d'administration Redis.	Pour sécuriser la console d'administration, suivez les instructions de la documentation Redis.	Administrateur de l'infrastructure informatique
Sécurisez la base de données Redis.	Consultez les pages suivantes de la documentation Redis pour : • Définissez le contrôle d'accès basé sur les rôles. • Définissez la sécurité du réseau. • Activez le protocole TLS.	
Sécurisez Redis Cloud APIs.	Lorsque vous activez l'API, vous pouvez gérer les clés d'API pour tous les propriétaires de votre compte Redis Cloud. Pour un aperçu des fonctionnalités de sécurité de l'API, consultez la documentation d'authentification de l'API sur le site Web de Redis.	Administrateur de l'infrastructure informatique

Configuration du nouvel environnement

Tâche	Description	Compétences requises
Configurez un nouvel environnement sur AWS.	Cette tâche inclut : • Activités de configuration d'AWS Landing Zone. La	DevOps Ingénieur informatique ou informatique

Tâche	Description	Compétences requises
	zone d'atterrissage prend en charge : • Déploiements multicomptes • Base de sécurité minimale • Méthode automatisée de provisionnement de nouveaux comptes avec une base de sécurité et des prérequis ISV (mise en réseau, configuration de sécurité, etc.) • Notifications, journalisation centralisée et surveillance • Activités de configuration du logiciel ISV. Cela inclut les configurations qui doivent être incluses dans la migration, telles que les paramètres et les modifications du produit et de la charge de travail. • Activités IaC telles que la configuration ou la personnalisation de modèles AWS CloudFormation ou Terraform.	

Tâche	Description	Compétences requises
Déployez l'architecture de migration.	1. Configurez Redis Enterprise Cloud sur AWS. 2. Installez des outils de migration tels que RIOT ou AWS DMS. Consultez la section Outils pour obtenir la liste des outils disponibles. 3. Établissez la connectivité entre les couches d'application, de migration et de base de données. 4. Créez un exemple de charge de travail qui peut circuler à travers chaque couche et migrer un petit ensemble d'échantillons de données. Vous êtes maintenant prêt à exécuter les pipelines de migration de données réels et à les tester.	DevOps Ingénieur informatique ou informatique

Configuration de la mise en réseau

Tâche	Description	Compétences requises
Établissez la connectivité.	Établissez la connectivité entre l'infrastructure sur site et les ressources du cloud AWS. Utilisez des groupes de sécurité, AWS Direct Connect	DevOps Ingénieur informatique ou informatique

Tâche	Description	Compétences requises
	et d'autres ressources pour bénéficier de cette fonctionn alité. Pour plus d'informations, consultez Connect Your Data Center to AWS sur le site Web d'AWS.	
Configurez le peering VPC.	Établissez le peering VPC entre les applications métier VPCs qui exécutent (ou les EC2 instances qui exécutent les outils de migration ou le serveur de réplication AWS DMS) et le VPC qui exécute Redis Enterprise Cloud. Pour obtenir des instructi ons, consultez Get started with Amazon VPC dans la documentation Amazon VPC et Enable VPC peering dans la documentation Redis.	DevOps Ingénieur informati que ou informatique

Migrer les données

Tâche	Description	Compétences requises
Choisissez un outil de migration de données.	Consultez le tableau de la section Outils pour connaître les descriptions, les avantages et les inconvénients de ces outils : • Exportation et importation RDS	Architecte de solutions de migration

Tâche	Description	Compétences requises
	• Fonctionnalité de réplication Redis () `ReplicaOf` • AWS DMS • Fusion logique de bases de données Les lignes suivantes décrivent les tâches de migration de données associées à chaque outil.	

Tâche	Description	Compétences requises
Option 1 : utilisez l'exportation et l'importation RDB.	1. Déconnecter la source : arrêtez le trafic sur la base de données source (par exemple, en déconnectant les applications professionnelles). 2. Exporter : exportez les données de la base de données source sous forme de fichier RDB. 3. Étape : Chargez les données vers un emplacement accessible aux instances Redis Enterprise Cloud sur AWS (par exemple, vous pouvez les télécharger sur un compartiment S3 ou un serveur FTP). 4. Importer : importez les fichiers RDB (en les listant tous en une seule étape d'importation) dans votre base de données cible Redis Enterprise Cloud. 5. Trancher : passez à la base de données cible (par exemple, en connectant votre application, connectez-vous à celle-ci).	Architecte de solutions de migration, architecte de solutions Redis

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la documentation Redis.	

Tâche	Description	Compétences requises
Option 2 : utilisez la fonctionn alité de réplication Redis (actif-passif).	1. Connect database : établissez un `ReplicaOf` lien entre les bases de données source et cible. 2. Exécuter une synchroni sation initiale : attendez que la synchronisation initiale entre les bases de données source et cible soit terminée. 3. Déconnecter la source : arrêtez le trafic sur la base de données source (par exemple, en déconnectant l'application). 4. Exécuter la réplication delta : attendez que le delta soit répliqué sur la base de données cible. 5. Interrompre : passez à la base de données cible (par exemple, en y connectant votre application). 6. Supprimer : supprimez le `ReplicaOf` lien entre les bases de données source et cible. Pour plus d'informations, consultez la documentation Redis.	Architecte de solutions de migration, architecte de solutions Redis

Tâche	Description	Compétences requises
Option 3 : utilisez AWS DMS.	1. Configurer une instance de réplication AWS DMS : cette instance exécute tous les processus de migration. Pour obtenir des instructions : utilisation d'une instance de réplication AWS DMS dans la documentation AWS DMS. 2. Définissez la base de données source : définissez le point de terminaison source. Testez la connectivité entre le point de terminaison source et le serveur de réplication AWS DMS. Pour obtenir des instructions : création de points de terminaison source et cible dans la documentation AWS DMS. 3. Configuration de la base de données cible : configurez Redis Enterprise Cloud sur AWS et configurez la base de données vers laquelle effectuer la migration. 4. Définissez la base de données cible : définissez le point de terminaison cible. Assurez-vous que le peering VPC est établi entre le VPC sur lequel AWS DMS est exécuté et le VPC	Architecte de solutions de migration, architecte de solutions Redis

Tâche	Description	Compétences requises
	qui héberge Redis Enterprise Cloud sur AWS. Testez la connectivité entre le serveur de réplication AWS DMS et la base de données cible. 5. Création d'une tâche AWS DMS : créez une tâche ou un ensemble de tâches pour définir les tables et les processus de réplication que vous souhaitez utiliser pour migrer les données. Pour obtenir des instructions : utilisation des tâches AWS DMS dans la documentation AWS DMS. 6. Migrer : migrez les données en exécutant la tâche AWS DMS. 7. Interrompre : passez à la base de données cible (par exemple, en y connectant votre application).	
Option 4 : Utiliser la fusion logique des bases de données.	Cette option implique l'utilisation d'un script de migration ou d'un outil ETL capable de transformer le modèle de données physique de la base de données source et de générer un fichier RDB. Les services professionnels Redis peuvent vous aider à effectuer cette étape, si nécessaire.	Architecte de solutions de migration, architecte de solutions Redis

Migrez votre application

Tâche	Description	Compétences requises
Alignez les délais et les objectifs de gestion de projet.	Alignez les objectifs, les étapes et les délais du projet de migration de la couche applicative avec ceux du projet de migration de données Redis.	Gestion de projets
Alignez les activités de test.	Une fois la couche d'application migrée et modernisée dans le cloud AWS, pointez la couche d'application vers le Redis Enterprise Cloud sur AWS récemment migré à des fins de test.	Test

test

Tâche	Description	Compétences requises
Mettre en œuvre des plans de test.	Exécutez les routines de migration des données et les scripts développés pendant la phase de mise en œuvre dans un environnement de test, conformément aux exigences de test, sur votre site.	Test
Qualité des données de test.	Testez la qualité des données après leur migration.	Test
Fonctionnalité de test.	Testez les requêtes de données et la couche d'application pour vous assurer que	Test

Tâche	Description	Compétences requises
	l'application fonctionne au même niveau que dans le système source.	

Découper

Tâche	Description	Compétences requises
Prenez la décision de passer à un autre.	Une fois tous les tests au niveau de l'application et de la base de données terminés, l'équipe de direction et les parties prenantes prennent la décision finale concernant le passage au nouvel environnement sur AWS sur la base des résultats finaux confirmés par les équipes de test.	Gestion de projet, Champions du monde des affaires
Passez au cloud AWS.	Lorsque vous avez confirmé que tout est en place, pointez la couche d'application vers les données récemment migrées et dirigez les clients vers la nouvelle couche d'application qui s'exécute sur la base du nouveau système Redis Enterprise Cloud sur AWS.	Ingénieur informatique ou DevOps ingénieur, architecte de données, architecte de solutions de migration, architecte de solutions Redis

Ressources connexes

Ressources Redis

- Documentation Redis Enterprise Cloud

- Outil RIOT (GitHub référentiel)
- Terraform Provider (téléchargement)

Ressources AWS

- Migrations de démonstration
- Solutions pour les partenaires AWS
- Documentation
- Billets de blogs
- Livres blancs
- Tutoriels et vidéos
- Migration vers le cloud AWS
- Recommandations AWS

Informations supplémentaires

Pour connaître les exigences de sécurité standard relatives à la migration des charges de travail Redis vers le cloud AWS, consultez les meilleures pratiques en matière de sécurité, d'identité et de conformité sur le site Web d'AWS et le Redis Trust Center sur le site Web de Redis.

Migrez SAP ASE sur Amazon EC2 vers Amazon Aurora PostgreSQL compatible avec AWS SCT et AWS DMS

Créée par Amit Kumar (AWS) et Ankit Gupta (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données SAP Adaptive Server Enterprise (SAP ASE) hébergée sur une instance Amazon Elastic Compute Cloud (Amazon EC2) vers une édition compatible avec Amazon Aurora PostgreSQL à l'aide d'AWS Schema Conversion Tool (AWS SCT) et d'AWS Database Migration Service (AWS DMS). Le modèle se concentre à la fois sur les conversions en langage de définition des données (DDL) pour les objets stockés et sur la migration des données.

La compatibilité avec Aurora PostgreSQL prend en charge les charges de travail de traitement des transactions en ligne (OLTP). Ce service géré fournit des configurations qui s'adaptent automatiquement à la demande. Il peut automatiquement démarrer, arrêter, agrandir ou réduire votre base de données en fonction des besoins de votre application. Vous pouvez exécuter votre base de données dans le cloud sans gérer aucune instance de base de données. La compatibilité avec Aurora PostgreSQL constitue une option rentable pour les charges de travail peu fréquentes, intermittentes ou imprévisibles.

Le processus de migration comprend deux phases principales :

- Conversion du schéma de base de données à l'aide d'AWS SCT
- Migration des données à l'aide d'AWS DMS

Des instructions détaillées pour les deux phases sont fournies dans la section Epics. Pour plus d'informations sur la résolution des problèmes spécifiques à l'utilisation d'AWS DMS avec des bases de données SAP ASE, consultez la section Résolution des problèmes liés à SAP ASE dans la documentation AWS DMS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données SAP ASE source sur une EC2 instance avec des services de serveur, de base de données et d'écoute opérationnels

- Une base de données cible compatible avec Aurora PostgreSQL

Limites

- Le numéro de port pour les connexions doit être 5432.
- La fonctionnalité huge_pages est activée par défaut mais peut être modifiée.
- Point-in-time la granularité de récupération (PITR) est de 5 minutes.
- La réplication entre régions n'est actuellement pas disponible.
- La taille de stockage maximale d'une base de données Aurora est de 128 TiB.
- Vous pouvez créer jusqu'à 15 répliques de lecture.
- La limite de taille de table est limitée uniquement par la taille du volume du cluster Aurora, de sorte que la taille de table maximale pour un cluster de base de données compatible Aurora PostgreSQL est de 32 TiB. Nous vous recommandons de suivre les meilleures pratiques en matière de conception de tables, telles que le partitionnement de grandes tables.

Versions du produit

- Base de données source : AWS DMS prend actuellement en charge SAP ASE 15, 15.5, 15.7 et 16.x. Consultez le guide de l'utilisateur d'AWS DMS pour obtenir les dernières informations sur la prise en charge des versions de SAP ASE.
- Base de données cible : PostgreSQL 9.4 et versions ultérieures (pour les versions 9.x), 10.x, 11.x, 12.x, 13.x et 14.x. Consultez le guide de l'utilisateur d'AWS DMS pour connaître les dernières versions de PostgreSQL prises en charge.
- Amazon Aurora 1.x ou version ultérieure. Pour obtenir les informations les plus récentes, consultez les versions compatibles avec Aurora PostgreSQL et les versions du moteur dans la documentation Aurora.

Architecture

Pile technologique source

- Base de données SAP ASE exécutée sur Amazon EC2

Pile technologique cible

- Base de données compatible avec Aurora PostgreSQL

Architecture de migration

Outils

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- AWS Schema Conversion Tool (AWS SCT) prend en charge les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majeure partie du code personnalisé dans un format compatible avec la base de données cible.
- AWS DMS prend en charge plusieurs bases de données sources et cibles différentes. Pour plus d'informations, consultez les sections Sources pour la migration des données et cibles pour la migration des données dans la documentation AWS DMS. Pour bénéficier de la prise en charge la plus complète des versions et des fonctionnalités, nous vous recommandons d'utiliser la dernière version d'AWS DMS.

Épopées

Configuration de l'environnement

Tâche	Description	Compétences requises
Configurez l'accès réseau dans l' EC2 instance source.	Configurez des groupes de sécurité dans l' EC2 instance qui héberge votre base de données SAP ASE source. Pour obtenir des instructions, consultez les groupes EC2 de sécurité Amazon pour les instances Linux dans la EC2 documentation Amazon.	Administrateur de systèmes

Tâche	Description	Compétences requises
Créez votre cluster de base de données compatible Aurora PostgreSQL cible.	Installez, configurez et lancez un cluster compatible Aurora PostgreSQL pour votre base de données cible. Pour plus d'informations, consultez la section Création d'un cluster de base de données Amazon Aurora dans la documentation Aurora.	DBA
Configurez l'autorisation pour le cluster de base de données cible.	Configurez des groupes de sécurité et des pare-feux pour la base de données cible. Pour obtenir des instructi ons, consultez la section Création d'un cluster de base de données Amazon Aurora dans la documentation Aurora.	DBA, administrateur système

Convertissez le schéma de votre base de données avec AWS SCT

Tâche	Description	Compétences requises
Lancez AWS SCT.	Lancez AWS SCT en suivant les instructions de la documentation AWS SCT. AWS SCT fournit une interface utilisateur basée sur un projet pour convertir automatiq uement le schéma de base de données de votre base de données source SAP ASE	DBA

Tâche	Description	Compétences requises
	dans un format compatible avec votre instance de base de données cible compatible Aurora PostgreSQL.	
Créez des points de terminaison AWS SCT.	Créez des points de terminaison pour les bases de données SAP ASE source et les bases de données PostgreSQL cibles. Pour obtenir des instructions, consultez la documentation AWS SCT.	DBA
Créez un rapport d'évaluation.	Créez un rapport d'évaluation de la migration de base de données pour évaluer la migration et détecter tout objet ou fonction incompatible. Pour obtenir des instructions, consultez la documentation AWS SCT.	DBA
Convertissez le schéma.	Convertissez le schéma de base de données en suivant les instructions de la documentation AWS SCT.	DBA

Tâche	Description	Compétences requises
Validez les objets de base de données	Si AWS SCT ne parvient pas à convertir un objet de base de données, il identifiera son nom et d'autres informations. Vous devez convertir ces objets manuellement. Pour identifier ces incohéren ces, suivez les instructions du billet de blog AWS intitulé Validation des objets de base de données après la migration de SAP ASE vers Amazon RDS for PostgreSQL ou Amazon Aurora PostgreSQL.	DBA

Analyser la migration vers AWS DMS

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.	Vérifiez la compatibilité des versions de base de données SAP ASE avec AWS DMS. Pour plus d'informations, consultez les sections Sources pour AWS DMS et cibles pour AWS DMS dans la documenta tion AWS DMS.	DBA
Identifiez les exigences relatives au type et à la capacité de stockage.	Choisissez la capacité de stockage appropriée pour la base de données cible en fonction de la taille de votre base de données source.	DBA, administrateur système

Tâche	Description	Compétences requises
Choisissez le type d'instanc e, la capacité et les autres fonctionnalités de l'instance de réplication.	Choisissez le type d'instance, la capacité, les fonctionnalités de stockage et les fonctionn alités réseau qui répondent à vos besoins. Pour obtenir des conseils, consultez Choisir l'instanc e de réplication AWS DMS adaptée à votre migration dans la documentation AWS DMS.	DBA, administrateur système
Identifiez les exigences de sécurité d'accès au réseau.	Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible. Suivez les instructions de la section Configuration d'un réseau pour une instance de réplication dans la documenta tion AWS DMS.	DBA, administrateur système

Migrer les données

Tâche	Description	Compétences requises
Migrez les données en créant une tâche de migration dans AWS DMS.	Pour migrer des données, créez une tâche et suivez les instructions de la documenta tion AWS DMS. Nous vous recommandons d'utiliser la dernière version	DBA

Tâche	Description	Compétences requises
	d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.	
Validez les données.	Pour vérifier que vos données ont bien été migrées de la base de données source vers la base de données cible, suivez les directives de validation des données fournies dans la documentation AWS DMS.	DBA

Migrer l'application

Tâche	Description	Compétences requises
Identifiez la stratégie de migration des applications.	Choisissez l'une des sept stratégies (7R) de migration des applications vers le cloud.	DBA, propriétaire de l'application, administrateur système
Suivez la stratégie de migration des applications.	Effectuez les tâches de base de données identifiées par l'équipe chargée de l'application, notamment la mise à jour des détails de connexion DNS pour la base de données cible et la mise à jour des requêtes dynamiques.	DBA, propriétaire de l'application, administrateur système

Passez à la base de données cible

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.	Basculez la connexion entre la base de données source et la base de données cible. Pour plus d'informations, consultez la section Réduction de la stratégie de migration pour les bases de données relationnelles.	DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.	Mettez fin à toutes les tâches de migration, aux instances de réplication, aux points de terminaison et aux autres ressources AWS SCT et AWS DMS. Pour en savoir plus, consultez la documentation AWS DMS.	DBA, administrateur système
Passez en revue et validez les documents du projet.	Validez toutes les étapes de la documentation du projet pour vous assurer que toutes les tâches ont été effectuées avec succès.	DBA, propriétaire de l'application, administrateur système
Fermez le projet.	Clôturez le projet de migration et faites part de vos commentaires.	DBA, propriétaire de l'application, administrateur système

Ressources connexes

Références

- Activer les connexions chiffrées pour les instances de base de données PostgreSQL dans Amazon RDS (AWS Prescriptive Guidance)
- Transportez des bases de données PostgreSQL entre deux instances de base de données Amazon RDS à l'aide de pg_transport (AWS Prescriptive Guidance)
- Tarification d'Amazon Aurora
- Bonnes pratiques relatives à l'édition compatible avec Amazon Aurora PostgreSQL (documentation Amazon Aurora)
- Documentation AWS SCT
- Documentation AWS DMS
- Utilisation d'une base de données SAP ASE comme source pour AWS DMS

Tutoriels et vidéos

- Commencer à utiliser AWS Database Migration Service
- AWS Database Migration Service (vidéo)

Migrer les certificats SSL Windows vers un Application Load Balancer à l'aide d'ACM

Créée par Chandra Sekhar Yaratha (AWS) et Igor Kovalchuk (AWS)

Récapitulatif

Le modèle fournit des conseils sur l'utilisation d'AWS Certificate Manager (ACM) pour migrer des certificats SSL (Secure Sockets Layer) existants à partir de sites Web hébergés sur des serveurs sur site ou d'instances Amazon Elastic Compute Cloud (Amazon EC2) sur Microsoft Internet Information Services (IIS). Les certificats SSL peuvent ensuite être utilisés avec Elastic Load Balancing sur AWS.

Le protocole SSL protège vos données, affirme votre identité, améliore le classement dans les moteurs de recherche, aide à répondre aux exigences de la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) et améliore la confiance des clients. Les développeurs et les équipes informatiques qui gèrent ces charges de travail souhaitent que leurs applications Web et leur infrastructure, y compris le serveur IIS et Windows Server, restent conformes à leurs politiques de base.

Ce modèle couvre l'exportation manuelle des certificats SSL existants depuis Microsoft IIS, leur conversion du format Personal Information Exchange (PFX) au format Private Enhanced Mail (PEM) pris en charge par ACM, puis leur importation dans ACM sur votre compte AWS. Il décrit également comment créer un Application Load Balancer pour votre application et configurer l'Application Load Balancer pour utiliser vos certificats importés. Les connexions HTTPS sont ensuite interrompues sur l'Application Load Balancer, et vous n'avez pas besoin de surcharger davantage la configuration du serveur Web. Pour plus d'informations, consultez Créer un écouteur HTTPS pour votre Application Load Balancer.

Les serveurs Windows utilisent des fichiers .pfx ou .p12 pour contenir le fichier de clé publique (certificat SSL) et son fichier de clé privée unique. L'autorité de certification (CA) vous fournit votre fichier de clé publique. Vous utilisez votre serveur pour générer le fichier de clé privée associé dans lequel la demande de signature de certificat (CSR) a été créée.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cloud privé virtuel (VPC) sur AWS avec au moins un sous-réseau privé et un sous-réseau public dans chaque zone de disponibilité utilisée par vos cibles

- IIS version 8.0 ou ultérieure s'exécutant sur Windows Server 2012 ou version ultérieure
- Une application Web exécutée sur IIS
- Accès administrateur au serveur IIS

Architecture

Pile technologique source

- Implémentation du serveur Web IIS avec SSL pour garantir que les données sont transmises en toute sécurité dans le cadre d'une connexion cryptée (HTTPS)

Architecture source

Pile technologique cible

- Certificats ACM dans votre compte AWS
- Application Load Balancer configuré pour utiliser des certificats importés
- Instances Windows Server dans les sous-réseaux privés

Architecture cible

Outils

- AWS Certificate Manager (ACM) vous aide à créer, stocker et renouveler les certificats et clés SSL/TLS X.509 publics et privés qui protègent vos sites Web et applications AWS.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les EC2 instances, les conteneurs et les adresses IP dans une ou plusieurs zones de disponibilité.

Bonnes pratiques

- Appliquez les redirections de trafic de HTTP vers HTTPS.
- Configurez correctement les groupes de sécurité pour votre Application Load Balancer afin d'autoriser le trafic entrant uniquement vers des ports spécifiques.

- Lancez vos EC2 instances dans différentes zones de disponibilité pour garantir une haute disponibilité.
- Configurez le domaine de votre application pour qu'il pointe vers le nom DNS de l'équilibreur de charge d'application au lieu de son adresse IP.
- Assurez-vous que les contrôles de santé de la couche application sont configurés dans l'Application Load Balancer.
- Configurez le seuil pour les contrôles de santé.
- Utilisez Amazon CloudWatch pour surveiller l'Application Load Balancer.

Épopées

Exporter un fichier .pfx

Tâche	Description	Compétences requises
Exportez le fichier .pfx depuis Windows Server.	Pour exporter le certificat SSL sous forme de fichier .pfx depuis le gestionnaire IIS local de Windows Server : 1. Choisissez Démarrer, Administration, Internet Information Services (IIS) Manager. 2. Sélectionnez le nom du serveur, puis sous Sécurité, double-cliquez sur Certificats de serveur. 3. Choisissez le certificat que vous souhaitez exporter, puis sélectionnez Exporter. 4. Dans la zone Exporter le certificat, choisissez l'emplacement, le chemin et le nom de votre fichier .pfx.	Administrateur de systèmes

Tâche	Description	Compétences requises
	5. Spécifiez et confirmez un mot de passe pour votre fichier .pfx. **Note** Ce mot de passe est nécessaire pour installer le fichier .pfx. 6. Choisissez OK. Votre fichier .pfx doit maintenant être enregistré à l'emplacement et au chemin que vous avez spécifiés.	

Convertir le certificat codé au format PFX au format PEM

Tâche	Description	Compétences requises
Téléchargez et installez le kit d'outils OpenSSL.	1. Téléchargez et installez Win32/Win64 OpenSSL depuis le site Web de Shining Light Productions. 2. Ajoutez l'emplacement des fichiers binaires OpenSSL à votre variable `PATH` système, afin que les fichiers binaires soient disponibles pour une utilisation en ligne de commande.	Administrateur de systèmes

Tâche	Description	Compétences requises
Convertissez le certificat codé au format PFX au format PEM.	Les étapes suivantes convertissent le fichier de certificat signé codé au format PFX en trois fichiers au format PEM : • `cert-file.pem` contient le certificat SSL/TLS pour la ressource. • `privatekey.pem` contient la clé privée du certificat sans protection par mot de passe. • `ca-chain.pem` contient le certificat racine de l'autorité de certification. Pour convertir le certificat codé au format PFX : 1. Exécutez Windows PowerShell. 2. Utilisez la commande suivante pour extraire la clé privée du certificat du fichier PFX. Entrez le mot de passe du certificat lorsque vous y êtes invité. `openssl pkcs12 -in <filename>.pfx -nocerts -out withpw-privatekey.pem` La commande génère un fichier de clé privée codé	Administrateur de systèmes

Tâche	Description	Compétences requises

	au format PEM nommé. `privatekey.pem` Entrez une phrase secrète pour protéger le fichier de clé privée lorsque vous y êtes invité.
	3. Exécutez la commande suivante pour supprimer le mot de passe. Lorsque vous y êtes invité, saisissez le mot de passe que vous avez créé à l'étape 2.
	`openssl rsa -in withpw-privatekey.pem -out privatekey.pem`
	Si la commande aboutit, le message « écriture de la clé RSA » s'affiche.
	4. Utilisez la commande suivante pour transférer le certificat du fichier PFX vers un fichier PEM.
	`openssl pkcs12 -in <file_name>.pfx -clcerts -nokeys -out cert-file.pem`
	Cela crée un fichier de certificat codé au format PEM nommé. `cert-file.pem` Si la commande	

Tâche	Description	Compétences requises
	aboutit, le message « MAC vérifié OK » s'affiche. 5. Créez un fichier de chaîne CA à partir du fichier PFX. La commande suivante crée un fichier de chaîne CA nomméca-chain.pem . `openssl pkcs12 -in <file_name>.pfx -cacerts -nokeys -chain -out ca-chain.pem` Si la commande aboutit, le message « MAC vérifié OK » s'affiche.	

Importer un certificat dans ACM

Tâche	Description	Compétences requises
Préparez-vous à importer le certificat.	Sur la console ACM, choisissez Importer un certificat.	Administrateur du cloud
Indiquez le corps du certificat.	Pour Corps du certificat, collez le certificat codé PEM que vous souhaitez importer. Pour plus d'informations sur les commandes et les étapes décrites dans ce livre et sur les autres tâches décrites dans cette épopée, consultez la section Importation d'un	Administrateur du cloud

Tâche	Description	Compétences requises
	certificat dans la documentation d'ACM.	
Fournissez la clé privée du certificat.	Pour Certificate private key, collez la clé privée codée PEM, non chiffrée, correspondant à la clé publique du certificat.	Administrateur du cloud
Fournissez la chaîne de certificats.	Pour Chaîne de certificats, collez la chaîne de certificats codée PEM, qui est stockée dans le `CertificateChain.pem` fichier.	Administrateur du cloud
Importez le certificat.	Choisissez Review and import (Vérifier et importer). Vérifiez que les informations relatives à votre certificat sont correctes, puis choisissez Importer.	Administrateur du cloud

Création d'un Application Load Balancer

Tâche	Description	Compétences requises
Créez et configurez l'équilibreur de charge et les écouteurs.	Suivez les instructions de la documentation d'Elastic Load Balancing pour configurer un groupe cible, enregistrer des cibles et créer un Application Load Balancer et un écouteur. Ajoutez un deuxième écouteur (HTTPS) pour le port 443.	Administrateur du cloud

Résolution des problèmes

Problème	Solution
Windows PowerShell ne reconnaît pas la commande OpenSSL même après l'avoir ajoutée au chemin du système.	Vérifiez `$env:path` qu'il inclut l'emplacement des fichiers binaires OpenSSL. Si ce n'est pas le cas, exécutez la commande suivante dans PowerShell : `$env:path = $env:path + ";C:\OpenSSL-Win64\bin"`

Ressources connexes

Importer un certificat dans ACM

- Console ACM
- Format du certificat et de la clé pour l'importation
- Importer un certificat
- Guide de l'utilisateur d'AWS Certificate Manager

Création d'un Application Load Balancer

- Création d'un Application Load Balancer
- Guide de l'utilisateur de l'Application Load Balancer

Migrer une file d'attente de messagerie de Microsoft Azure Service Bus vers Amazon SQS

Créée par Nisha Gambhir (AWS)

Récapitulatif

Ce modèle décrit comment migrer une application Web ou console .NET Framework ou .NET Core depuis la plateforme de messagerie de file d'attente Microsoft Azure Service Bus vers Amazon Simple Queue Service Service Service Service Service Service (Amazon SQS).

Les applications utilisent les services de messagerie pour envoyer des données à d'autres applications et en recevoir. Ces services permettent de créer des microservices découplés et hautement évolutifs, des systèmes distribués et des applications sans serveur dans le cloud.

Les files d'attente Azure Service Bus font partie d'une infrastructure de messagerie Azure plus large qui prend en charge les mises en file d'attente et les messages de publication/d'abonnement.

Amazon SQS est un service de mise en file d'attente de messages entièrement géré qui vous permet de découpler et de dimensionner les microservices, les systèmes distribués et les applications sans serveur. Amazon SQS élimine la complexité et les frais associés à la gestion et à l'exploitation d'intergiciels orientés message, et permet aux développeurs de se concentrer sur la différenciation du travail. Amazon SQS vous permet d'envoyer, de stocker et de recevoir des messages entre des composants logiciels, quel que soit le volume, sans perdre de messages ni nécessiter la disponibilité d'autres services.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une application Web ou console .NET Framework ou .NET Core qui utilise les files d'attente Azure Service Bus (exemple de code joint)

Versions du produit

- .NET Framework 3.5 ou version ultérieure, ou .NET Core 1.0.1, 2.0.0 ou version ultérieure

Architecture

Pile technologique source

- Application Web ou console .NET (Core ou Framework) qui utilise une file d'attente Azure Service Bus pour envoyer des messages

Pile technologique cible

- Amazon SQS

Outils

Outils

- Microsoft Visual Studio

Code

Pour créer une politique de gestion des identités et des accès (IAM) AWS pour Amazon SQS :

1. Connectez-vous à AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

2. Dans le panneau de navigation à gauche, choisissez politiques, puis Créer une politique.

3. Choisissez l'onglet JSON et collez le code suivant :

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "sqs:DeleteMessage",
            "sqs:GetQueueUrl",
            "sqs:ChangeMessageVisibility",
            "sqs:SendMessageBatch",
            "sqs:ReceiveMessage",
            "sqs:SendMessage",
```

```
            "sqs:GetQueueAttributes",
            "sqs:ListQueueTags",
            "sqs:ListDeadLetterSourceQueues",
            "sqs:DeleteMessageBatch",
            "sqs:PurgeQueue",
            "sqs:DeleteQueue",
            "sqs:CreateQueue",
            "sqs:ChangeMessageVisibilityBatch",
            "sqs:SetQueueAttributes"
         ],
         "Resource": "arn:aws:sqs:*:<AccountId>:*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Allow",
         "Action": "sqs:ListQueues",
         "Resource": "*"
      }
   ]
}
```

4. Choisissez Réviser la politique, tapez un nom, puis choisissez Créer une politique.

5. Associez la nouvelle politique à votre rôle IAM existant ou créez-en un nouveau.

Épopées

Configuration d'Amazon SQS dans AWS

Tâche	Description	Compétences requises
Créez une politique IAM pour Amazon SQS.	Créez la politique IAM qui fournira l'accès à Amazon SQS. Consultez la section Code pour un exemple de politique.	Ingénieur système
Créez un profil AWS.	Créez un nouveau profil en exécutant les outils AWS pour la PowerShell commande Set-AWSCredential. Cette commande enregistre votre	Ingénieur système

Tâche	Description	Compétences requises
	clé d'accès et votre clé secrète dans votre fichier d'informations d'identification par défaut sous le nom de profil que vous spécifiez. Associez la politique Amazon SQS que vous avez créée précédemment à ce compte. Conservez l'ID de la clé d'accès AWS et la clé d'accès secrète. Ils seront nécessaires dans les prochaines étapes.	
Créez une file d'attente SQS.	Vous pouvez créer une file d'attente standard ou une file d'attente « premier entré, premier sorti » (FIFO). Pour obtenir des instructions, consultez le lien dans la section Références.	Ingénieur système

Révisez le code de votre application .NET

Tâche	Description	Compétences requises
Installez AWS Toolkit pour Visual Studio.	Ce kit d'outils est une extension pour Microsoft Visual Studio qui vous permet de créer et de déployer plus facilement des applications .NET dans AWS. Pour les instructions d'installation et d'utilisation, consultez le lien dans la section Références.	Développeur d'applications

Tâche	Description	Compétences requises
Installez le package AWSSDK .SQS. NuGet	Vous pouvez installer le AWSSDK fichier .SQS en choisissant « Gérer le NuGet package » dans Visual Studio ou en exécutant la commande « AWSSDK Install-P ackage .SQS ».	Développeur d'applications
Créez un AWSCredentials objet dans votre applicati on .NET.	L'exemple d'application en pièce jointe montre comment créer un AWSCredentials objet Basic, qui hérite de AWSCredentials. Vous pouvez utiliser l'ID de clé d'accès et la clé d'accès secrète antérieurs, ou laisser l'objet les sélection ner dans le dossier .aws dans le cadre du profil utilisateur lors de l'exécution.	Développeur d'applications
Créez un objet client SQS.	Créez un objet client SQS (AmazonSQSClient) pour .NET Framework. Cela fait partie de l'espace de noms Amazon.sqs. Cet objet est requis à la place du IQueue client, qui fait partie de Microsoft.Azure. ServiceBus espace de noms.	Développeur d'applications

Tâche	Description	Compétences requises
Appelez la SendMessageAsync méthode pour envoyer des messages à la file d'attente SQS.	Modifiez le code qui envoie le message à la file d'attente pour utiliser le amazonSqsClient. SendMessageAsync méthode. Pour plus de détails, consultez l'exemple de code ci-joint.	Développeur d'applications
Appelez la ReceiveMessageAsync méthode pour recevoir des messages de la file d'attente SQS.	Modifiez le code qui reçoit le message pour utiliser le amazonSqsClient. ReceiveMessageAsync méthode. Pour plus de détails, consultez l'exemple de code ci-joint.	Développeur d'applications
Appelez la DeleteMessageAsync méthode pour supprimer des messages de la file d'attente SQS.	Pour supprimer des messages, modifiez le code depuis le QueueClient. CompleteAsync méthode pour le amazonSqsClient. DeleteMessageAsync méthode. Pour plus de détails, consultez l'exemple de code ci-joint.	Développeur d'applications

Ressources connexes

- Manuel du développeur du kit SDK AWS pour .NET
- Messagerie à l'aide d'Amazon SQS
- Création et utilisation d'une file d'attente Amazon SQS avec le kit SDK AWS pour .NET
- Envoyer un message Amazon SQS
- Recevoir un message depuis une file d'attente Amazon SQS
- Supprimer un message d'une file d'attente Amazon SQS

- AWS Toolkit for Visual Studio

Informations supplémentaires

Ce modèle inclut deux exemples d'applications (voir la section des pièces jointes) :

- AzureSbTestAppinclut du code qui utilise la file d'attente Azure Service Bus.
- AmazonSqsTestApputilise Amazon SQS. Il s'agit d'une application console qui utilise .NET Core 2.2 et inclut des exemples d'envoi et de réception de messages.

Remarques :

- QueueClient est un objet de IQueue Client, qui fait partie de Microsoft.Azure. ServiceBus espace de noms (inclus dans le fichier Microsoft.Azure. ServiceBus NuGet paquet).
- amazonSqsClient est un objet d'AmazonSQSClient, qui fait partie de l'espace de noms Amazon.SQS (inclus dans le AWSSDK package .SQS). NuGet
- Selon l'endroit où le code est exécuté, disons s'il est exécuté EC2, le rôle doit être autorisé à écrire dans la file d'attente SQS.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer une base de données relationnelle vers MongoDB Atlas sur AWS

Créée par Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) et Igor Alekseev (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'une base de données relationnelle telle que SQL Server, MySQL ou PostgreSQL vers MongoDB Atlas dans le. AWS Cloud Il utilise MongoDB Relational Migrator pour accélérer la migration des données des bases de données relationnelles vers MongoDB Atlas.

Le modèle accompagne le guide Migrating to MongoDB Atlas AWS sur le site Web de Prescriptive AWS Guidance. Il fournit les étapes de mise en œuvre de l'un des scénarios de migration décrits dans ce guide. Pour d'autres scénarios de migration, consultez les modèles suivants sur le site Web des directives AWS prescriptives :

- Migrer un environnement MongoDB auto-hébergé vers MongoDB Atlas sur AWS
- Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS

Le modèle est destiné aux partenaires et aux AWS utilisateurs d'AWS System Integrator (SI).

Conditions préalables et limitations

Prérequis

- Une base de données relationnelle source (base de données Oracle, SQL Server, PostgreSQL, MySQL, SAP/Sybase ASE, etc.) à migrer vers MongoDB Atlas.
- Familiarité avec les bases de données relationnelles, MongoDB Atlas et. Services AWS Ce schéma explique certaines des étapes de migration à un niveau élevé. Des informations supplémentaires seront ajoutées dans les futures versions.

Versions du produit

- MongoDB version 5.0 ou ultérieure

Architecture

Le schéma suivant montre la migration d'une base de données du système de gestion de base de données relationnelle (RDBMS) vers MongoDB Atlas on. AWS

Pour les architectures de référence MongoDB Atlas qui prennent en charge différents scénarios d'utilisation, consultez la section Migration vers MongoDB Atlas AWS sur le site Web des directives prescriptives. AWS

Outils

- MongoDB Atlas est une base de données en tant que service (DBaaS) entièrement gérée pour le déploiement et la gestion des bases de données MongoDB dans le cloud.
- MongoDB Relational Migrator assure une transition fluide des données des bases de données relationnelles traditionnelles vers MongoDB. Il permet d'automatiser le processus de conversion et de transformer le modèle de données structuré des bases de données relationnelles dans le format de document flexible fourni par MongoDB. Le Relational Migrator préserve l'intégrité des données et les relations afin de simplifier la migration. Organisations peuvent tirer parti des avantages d'évolutivité, de performance et de polyvalence fournis par MongoDB tout en préservant la familiarité de leurs données existantes.

Bonnes pratiques

Pour connaître les meilleures pratiques relatives à l'utilisation de MongoDB sur AWS, consultez les articles publiés sur le blog du AWS Partner Network.

Épopées

Découverte et évaluation

Tâche	Description	Compétences requises
Déterminez les paramètres et la taille de la base de données relationnelle.	Estimez la taille de l'ensemble de travail en utilisant les recommandations du Relational Migrator et les informations provenant de l'`db.stats()` espace	Propriétaire de l'application, DBA

Tâche	Description	Compétences requises
	d'index total. Supposons qu'un pourcentage de votre espace de données soit fréquemment consulté. Cette tâche devrait prendre environ une semaine. Pour plus d'informations et des exemples concernant cette histoire et les autres de cette épopée, consultez la section Ressources connexes.	

Tâche	Description	Compétences requises
Estimez les besoins en bande passante du réseau.	Pour estimer les besoins en bande passante de votre réseau, multipliez la taille moyenne des documents par le nombre de documents servis par seconde. Tenez compte du trafic maximal que chaque nœud de votre cluster pourra supporter comme base. Pour calculer les taux de transfert de données en aval de votre cluster vers les applications clientes, utilisez la somme du total des documents renvoyés sur une période donnée. Si vos applications lisent à partir de nœuds secondair es, divisez le nombre total de documents par le nombre de nœuds pouvant effectuer des opérations de lecture. Pour connaître la taille moyenne des documents d'une base de données, utilisez la `db.stats().avgObjS ize` commande. Cette tâche prend généralement une journée.	DBA
Sélectionnez le niveau Atlas.	Suivez les instructions de la documentation MongoDB pour sélectionner le niveau de cluster Atlas approprié.	DBA

Tâche	Description	Compétences requises
Planifiez le transfert.	Planifiez le transfert des applications.	DBA, propriétaire de l'application

Configurer un nouvel environnement MongoDB Atlas sur AWS

Tâche	Description	Compétences requises
Créez un nouveau cluster MongoDB Atlas sur. AWS	Dans MongoDB Atlas, choisissez Build a Cluster. Dans la boîte de dialogue Créer un nouveau cluster, sélectionnez AWS comme fournisseur de cloud.	DBA
Sélectionnez Régions AWS une configuration globale du cluster.	Sélectionnez dans la liste des options disponibles Régions AWS pour votre cluster Atlas. Configurez des clusters globaux si nécessaire.	DBA
Sélectionnez le niveau du cluster.	Sélectionnez le niveau de cluster de votre choix. Le choix du niveau détermine des facteurs tels que la mémoire, le stockage et les spécifications IOPS.	DBA
Configurez des paramètres de cluster supplémentaires.	Configurez des paramètres de cluster supplémentaires tels que la version de MongoDB, les options de sauvegarde et de chiffrement. Pour plus d'informations sur ces	DBA

Tâche	Description	Compétences requises
	options, consultez la section Ressources connexes.	

Configuration de la sécurité et de la conformité

Tâche	Description	Compétences requises
Configurez la liste d'accès.	Pour vous connecter au cluster Atlas, vous devez ajouter une entrée à la liste d'accès du projet. Atlas utilise le protocole TLS/SSL pour chiffrer les connexions au cloud privé virtuel (VPC) de votre base de données. Pour configurer la liste d'accès au projet et pour plus d'informations sur les histoires de cette épopée, consultez la section Ressources connexes.	DBA
Authentifiez et autorisez les utilisateurs.	Vous devez créer et authentifier les utilisateurs de base de données qui accèderont aux clusters MongoDB Atlas. Pour accéder aux clusters d'un projet, les utilisateurs doivent appartenir à ce projet, et ils peuvent appartenir à plusieurs projets.	DBA
Créez des rôles personnalisés.	(Facultatif) Atlas prend en charge la création de rôles personnalisés dans les cas où les autorisations utilisateur	DBA

Tâche	Description	Compétences requises
	de la base de données Atlas intégrées ne couvrent pas l'ensemble des autorisations que vous souhaitez.	
Configurez le peering VPC.	(Facultatif) Atlas prend en charge le peering VPC avec d'autres options. VPCs AWS	Administrateur AWS
Configurez un AWS PrivateLink point de terminaison.	(Facultatif) Vous pouvez configurer des points de terminaison privés AWS en utilisant AWS PrivateLink. Pour plus d'informations, consultez la documentation Amazon VPC.	Administrateur AWS
Activez l'authentification à deux facteurs.	(Facultatif) Atlas prend en charge l'authentification à deux facteurs (2FA) pour aider les utilisateurs à contrôler l'accès à leurs comptes Atlas.	Administrateur AWS
Configurez l'authentification et l'autorisation des utilisateurs avec LDAP.	(Facultatif) Atlas prend en charge l'authentification et l'autorisation des utilisateurs avec le protocole LDAP (Lightweight Directory Access Protocol).	DBA

Tâche	Description	Compétences requises
Configurez un AWS accès unifié.	(Facultatif) Certaines fonctionn alités d'Atlas, notamment Atlas Data Lake et le chiffrement au repos à l'aide de la gestion des clés client, utilisent des rôles AWS Identity and Access Management (IAM) pour l'authentification.	Administrateur AWS
Configurez le chiffrement au repos à l'aide de AWS KMS.	(Facultatif) Atlas prend en charge l'utilisation de AWS Key Management Service (AWS KMS) pour chiffrer les moteurs de stockage et les sauvegardes des fournisseurs de cloud.	Administrateur AWS
Configurez le chiffrement au niveau des champs côté client.	(Facultatif) Atlas prend en charge le chiffrement au niveau des champs côté client, y compris le chiffrement automatique des champs.	Administrateur AWS

Migrer les données

Tâche	Description	Compétences requises
Ajoutez MongoDB Relational Migrator à la liste d'accès.	Ajoutez le Relational Migrator à la liste d'accès de votre base de données source. Cela permet de préparer l'environ nement source à se connecter au cluster Atlas cible.	DBA

Tâche	Description	Compétences requises
Évaluez les objets de base de données relationnelle.	Lancez MongoDB Relational Migrator et connectez-vous à votre base de données relationnelle. Lancez l'évaluation.	DBA
Acceptez les modèles de migration ou choisissez de les modifier en fonction des besoins de votre entreprise.	Acceptez les modèles de base de données recommandés par le Relational Migrator en fonction de l'évaluation initiale et des paramètres de performance, ou choisissez de les modifier en fonction des besoins de votre entreprise.	DBA
Lancez votre ensemble de répliques cible dans MongoDB Atlas.	Lancez votre ensemble de répliques cible dans MongoDB Atlas. Dans Relational Migrator, choisissez Je suis prêt à migrer.	DBA

Configuration de l'intégration opérationnelle

Tâche	Description	Compétences requises
Connectez-vous au cluster MongoDB Atlas.	Assurez-vous que la connectivité au cluster MongoDB Atlas fonctionne comme prévu.	Propriétaire de l'application
Interagissez avec les données du cluster.	Vérifiez les données du cluster.	DBA
Surveillez vos clusters.	Vérifiez que vos clusters sont correctement configurés.	DBA

Tâche	Description	Compétences requises
Sauvegardez et restaurez les données du cluster.	Planifiez les sauvegardes à une cadence régulière pour les données du cluster.	DBA

Ressources connexes

Tous les liens suivants, sauf indication contraire, renvoient à des pages Web de la documentation de MongoDB.

Guide de migration

- Migration vers MongoDB Atlas AWS sur AWS (conseils prescriptifs)

Découverte et évaluation

- Mémoire
- Exemple de dimensionnement avec des exemples de jeux de données Atlas
- Exemple de dimensionnement pour applications mobiles
- Trafic réseau
- Mise à l'échelle automatique du cluster
- Modèle de dimensionnement Atlas

Configuration de la sécurité et de la conformité

- Configuration des entrées de liste d'accès IP
- Configuration des utilisateurs de base de données
- Configurer l'accès à l'interface utilisateur d'Atlas
- Configuration de rôles de base de données personnalisés
- Configuration des utilisateurs de base de données
- Configuration d'une connexion d'appairage réseau
- En savoir plus sur les points de terminaison privés dans Atlas
- Gérez vos options d'authentification multifactorielle

- Configurer l'authentification et l'autorisation des utilisateurs avec LDAP
- Lac de données Atlas
- Chiffrement au repos à l'aide de la gestion des clés client
- Méthodes pour assumer un rôle (documentation IAM)
- Chiffrement au niveau des champs côté client
- Chiffrement automatique
- Contrôles de sécurité MongoDB Atlas
- Centre de gestion de la confidentialité MongoDB
- Configuration des fonctionnalités de sécurité pour les clusters

Configuration d'un nouvel environnement MongoDB Atlas sur AWS

- Fournisseurs de cloud et régions
- Gérer les clusters mondiaux
- Sélectionnez le niveau du cluster
- Configurer des paramètres supplémentaires
- Commencez avec Atlas
- Configurer l'accès à l'interface utilisateur d'Atlas
- Gérer les clusters

Migration des données

- Migrer ou importer des données

Clusters de surveillance

- Surveillez vos clusters

Intégration des opérations

- Se connecter à un cluster
- Interagissez avec vos données
- Surveillez vos clusters

- Sauvegarder, restaurer et archiver les données

Billets de blogs

- Modernisation des schémas RDBMS avec un modèle de document MongoDB

Migrer un environnement MongoDB auto-hébergé vers MongoDB Atlas sur AWS

Créée par Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) et Igor Alekseev (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'un environnement MongoDB autogéré (y compris MongoDB Community Server, Enterprise Server, Enterprise Advanced, mLab ou tout cluster MongoDB géré) vers MongoDB Atlas dans le. AWS Cloud Il utilise le service de migration Atlas Live pour accélérer la migration des données de MongoDB vers MongoDB Atlas.

Le modèle accompagne le guide Migrating to MongoDB Atlas AWS sur le site Web de Prescriptive AWS Guidance. Il fournit les étapes de mise en œuvre de l'un des scénarios de migration décrits dans ce guide. Pour d'autres scénarios de migration, consultez les modèles suivants sur le site Web des directives AWS prescriptives :

- Migrer une base de données relationnelle vers MongoDB Atlas sur AWS
- Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS

Le modèle est destiné aux partenaires et aux AWS utilisateurs de AWS Systems Integrator (SI).

Conditions préalables et limitations

Prérequis

- Un environnement MongoDB Enterprise Advanced, Community Server ou autre environnement MongoDB autogéré à migrer vers MongoDB Atlas.
- Connaissance de MongoDB, MongoDB Atlas et. Services AWS Ce schéma explique certaines des étapes de migration à un niveau élevé. Des informations supplémentaires seront ajoutées dans les futures versions.

Versions du produit

- MongoDB version 6.0.13 ou ultérieure

Architecture

Le schéma suivant montre le service de migration Atlas Live qui est utilisé pour migrer les données d'une base de données MongoDB Enterprise Advanced et d'une base de données communautaire MongoDB vers MongoDB Atlas on. AWS Utilisez ce service lorsque vous devez migrer des bases de données complexes et volumineuses vers MongoDB Atlas avec un temps d'arrêt minimal et une synchronisation continue des données. Ce modèle utilise le service de migration Atlas Live.

Le schéma suivant montre le service miroir MongoDB (`mongomirror`) que vous pouvez également utiliser pour migrer des données d'une base de données MongoDB Enterprise Advanced et d'une base de données MongoDB Community vers MongoDB Atlas via une connexion sécurisée. AWS AWS PrivateLink `mongomirror`À utiliser pour la réplication continue des données entre MongoDB sur site et MongoDB Atlas. Cet outil est idéal pour la reprise après sinistre ou les migrations par étapes, mais il n'entre pas dans le cadre de ce modèle.

Pour plus d'architectures de référence MongoDB Atlas prenant en charge différents scénarios d'utilisation, consultez la section Migration vers MongoDB Atlas AWS sur le site Web des directives prescriptives. AWS

Outils

- MongoDB Atlas est une base de données en tant que service (DBaaS) entièrement gérée pour le déploiement et la gestion des bases de données MongoDB dans le cloud.
- Atlas Live Migration Service est un utilitaire gratuit MongoDB qui permet de migrer des bases de données vers Atlas. Ce service assure la synchronisation de la base de données source avec la base de données de destination jusqu'au transfert. Lorsque vous êtes prêt à effectuer la transition, vous arrêtez vos instances d'application, vous les pointez vers le cluster Atlas de destination et vous les redémarrez. Pour accéder à ce service, choisissez les options de base de données dans votre cluster MongoDB Atlas.
- mongomirror est un outil permettant de migrer manuellement les données d'un jeu de répliques MongoDB existant vers un jeu de répliques MongoDB Atlas. `mongomirror`ne vous oblige pas à arrêter votre jeu de répliques ou vos applications existants, n'importe pas de données d'utilisateur ou de rôle, ni ne copie la base de données de configuration. Vous pouvez le télécharger `mongomirror` depuis la documentation de MongoDB.

Bonnes pratiques

Pour connaître les meilleures pratiques relatives à l'utilisation de MongoDB sur AWS, consultez les articles publiés sur le blog du AWS Partner Network.

Épopées

Découverte et évaluation

Tâche	Description	Compétences requises
Déterminez la taille du cluster.	Estimez la taille de l'ensemble de travail en utilisant les informations provenant de `db.stats()` pour l'espace d'index total. Supposons qu'un pourcentage de votre espace de données soit fréquemment consulté. Vous pouvez également estimer vos besoins en mémoire en vous basant sur vos propres hypothèses. Cette tâche devrait prendre environ une semaine. Pour plus d'informations et des exemples sur cette histoire et sur les autres histoires de cette épopée, consultez la section Ressources connexes.	DBA, propriétaire de l'application
Estimez les besoins en bande passante du réseau.	Pour estimer les besoins en bande passante de votre réseau, multipliez la taille moyenne des documents par le nombre de documents servis par seconde. Tenez compte du trafic maximal que	DBA

Tâche	Description	Compétences requises
	chaque nœud de votre cluster pourra supporter comme base. Pour calculer les taux de transfert de données en aval de votre cluster vers les applications clientes, utilisez la somme du total des documents renvoyés sur une période donnée. Si vos applications lisent à partir de nœuds secondaires, divisez le nombre total de documents par le nombre de nœuds pouvant effectuer des opérations de lecture. Pour connaître la taille moyenne des documents d'une base de données, utilisez la `db.stats().avgObjSize` commande. Cette tâche prend généralement une journée.	
Sélectionnez le niveau Atlas.	Suivez les instructions de la documentation MongoDB pour sélectionner le niveau de cluster Atlas approprié.	DBA
Planifiez le transfert.	Planifiez le transfert des applications.	DBA, propriétaire de l'application

Configuration d'un nouvel environnement MongoDB Atlas sur AWS

Tâche	Description	Compétences requises
Créez un nouveau cluster MongoDB Atlas sur. AWS	Connectez-vous à Atlas et ouvrez la page d'aperçu de votre projet. Cliquez sur le bouton Créer pour créer un cluster. Pour obtenir plus d'informations, consultez la documentation MongoDB.	DBA
Sélectionnez Régions AWS une configuration globale du cluster.	Sélectionnez dans la liste des options disponibles Régions AWS pour votre cluster Atlas. Configurez des clusters globaux si nécessaire. Pour obtenir plus d'informations, consultez la documentation MongoDB.	DBA
Sélectionnez le niveau du cluster.	Sélectionnez le niveau de cluster de votre choix. Le choix du niveau détermine des facteurs tels que la mémoire, le stockage et les spécifications d'IOPS.	DBA
Configurez des paramètres de cluster supplémentaires.	Configurez des paramètres de cluster supplémentaires tels que la version de MongoDB, les options de sauvegarde et de chiffrement. Pour plus d'informations sur ces options, consultez la section Ressources connexes.	DBA

Configuration de la sécurité et de la conformité

Tâche	Description	Compétences requises
Authentifiez et autorisez les utilisateurs.	Vous devez créer et authentifier les utilisateurs de base de données qui accèderont aux clusters MongoDB Atlas. Pour accéder aux clusters d'un projet, les utilisateurs doivent appartenir à ce projet, et ils peuvent appartenir à plusieurs projets. Atlas prend également en charge l'authentification basée sur AWS Identity and Access Management (IAM). Pour obtenir plus d'informations, consultez la documentation MongoDB.	DBA
Créez des rôles personnalisés.	(Facultatif) Atlas prend en charge la création de rôles personnalisés dans les cas où les autorisations utilisateur de la base de données Atlas intégrées ne couvrent pas l'ensemble des autorisations que vous souhaitez.	DBA
Configurez le peering VPC.	(Facultatif) Atlas prend en charge le couplage entre un cloud privé virtuel (VPC) et un autre cloud. VPCs AWS	Administrateur AWS
Configurez un AWS PrivateLink point de terminaison.	(Facultatif) Vous pouvez configurer des points de terminaison privés AWS en utilisant AWS PrivateLink.	Administrateur AWS

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la documentation Amazon VPC.	
Activez l'authentification à deux facteurs.	(Facultatif) Atlas prend en charge l'authentification à deux facteurs (2FA) pour aider les utilisateurs à contrôler l'accès à leurs comptes Atlas.	Administrateur AWS
Configurez l'authentification et l'autorisation des utilisateurs avec LDAP.	(Facultatif) Atlas prend en charge l'authentification et l'autorisation des utilisate urs avec le protocole LDAP (Lightweight Directory Access Protocol).	Administrateur AWS
Configurez un AWS accès unifié.	(Facultatif) Certaines fonctionn alités d'Atlas, notamment Atlas Data Lake et le chiffrement au repos à l'aide de la gestion des clés client, utilisent les rôles IAM pour l'authent ification.	Administrateur AWS
Configurez le chiffrement au repos à l'aide de AWS KMS.	(Facultatif) Atlas prend en charge l'utilisation de AWS Key Management Service (AWS KMS) pour chiffrer les moteurs de stockage et les sauvegardes des fournisseurs de cloud.	Administrateur AWS

Tâche	Description	Compétences requises
Configurez le chiffrement au niveau des champs côté client.	(Facultatif) Atlas prend en charge le chiffrement au niveau des champs côté client, y compris le chiffrement automatique des champs.	Administrateur AWS

Migrer les données

Tâche	Description	Compétences requises
Sélectionnez votre ensemble de répliques cible dans MongoDB Atlas.	Accédez au cluster Atlas de destination et cliquez sur le bouton représentant des points de suspension (...). Dans la liste des clusters, ce bouton apparaît sous le nom du cluster. Dans les détails du cluster, le bouton apparaît sur la droite, à côté des boutons Connect et Configuration. Pour obtenir plus d'informations, consultez la documentation MongoDB.	DBA
Ajoutez le service de migration Atlas Live à la liste d'accès.	Ajoutez le service de migration Atlas Live à la liste d'accès de votre cluster AWS source. Cela permet de préparer l'environnement source à se connecter au cluster Atlas cible.	DBA
Effectuez la migration avec Atlas Live Migration Service.	Choisissez Démarrer la migration. Lorsque le bouton Prepare to Cutover devient	DBA

Tâche	Description	Compétences requises
	vert, effectuez le découpage. Passez en revue les indicateurs de performance du cluster Atlas. Envisagez de mettre à jour la connexion à la base de données dans toutes les couches de l'application pour qu'elle pointe vers la nouvelle base de données.	

Configuration de l'intégration opérationnelle

Tâche	Description	Compétences requises
Connectez-vous au cluster MongoDB Atlas.	Assurez-vous que la connectivité au cluster MongoDB Atlas fonctionne comme prévu.	Propriétaire de l'application
Interagissez avec les données du cluster.	Testez les données du cluster.	DBA
Surveillez vos clusters.	Vérifiez que vos clusters sont correctement configurés.	DBA
Sauvegardez et restaurez les données du cluster.	Planifiez les sauvegardes à une cadence régulière pour les données du cluster.	DBA

Résolution des problèmes

Problème	Solution
Erreur : Impossible d'atteindre la source spécifiée	• Assurez-vous d'avoir ajouté les plages de sous-réseaux appropriées à la liste d'accès IP du cluster source. Vous pouvez trouver

Problème	Solution

	les quatre plages de sous-réseaux requises dans la fenêtre modale Live Migration.
	• Vérifiez que le nom d'hôte que vous avez spécifié correspond à une adresse IP publique. À l'invite de commandes, utilisez l'une des commandes suivantes :
	`nslookup <hostname>`
	`ping <hostname>`
	• Assurez-vous que vous n'utilisez pas de connexion d'appairage VPC, qui n'est pas compatible avec la migration en direct par pull. Si une connexion d'appairage VPC est votre seule option, utilisez-la à la place. `mongomirror`

Erreur : Impossible de résoudre le nom d'hôte	Aucune adresse IP n'a été trouvée pour le nom d'hôte indiqué. Vérifiez que le nom d'hôte indiqué est correct et accessible au public.
Toute autre erreur	Si vous rencontrez d'autres erreurs, consultez la section Troubleshoot Live Migration (Pull) dans la documentation de MongoDB.

Ressources connexes

Tous les liens suivants, sauf indication contraire, renvoient à des pages Web de la documentation de MongoDB.

Guide de migration

- Migration vers MongoDB Atlas AWS sur AWS (conseils prescriptifs)

Migration d'anciennes versions

- Migration des anciennes versions de MongoDB

Découverte et évaluation

- Mémoire
- Exemple de dimensionnement avec des exemples de jeux de données Atlas
- Exemple de dimensionnement pour applications mobiles
- Trafic réseau
- Mise à l'échelle automatique du cluster
- Modèle de dimensionnement Atlas

Configuration de la sécurité et de la conformité

- Configuration des entrées de liste d'accès IP
- Configuration des utilisateurs de base de données
- Configuration de l'accès à l'interface utilisateur d'Atlas
- Configuration de rôles de base de données personnalisés
- Configuration des utilisateurs de base de données
- Configuration d'une connexion d'appairage réseau
- En savoir plus sur les points de terminaison privés dans Atlas
- Gérez vos options d'authentification multifactorielle
- Configuration de l'authentification et de l'autorisation des utilisateurs avec LDAP
- Lac de données Atlas
- Chiffrement au repos à l'aide de la gestion des clés client
- Méthodes pour assumer un rôle (documentation IAM)
- Chiffrement au niveau des champs côté client
- Chiffrement automatique
- Contrôles de sécurité MongoDB Atlas
- Centre de gestion de la confidentialité MongoDB
- Configuration des fonctionnalités de sécurité pour les clusters

Configuration d'un nouvel environnement MongoDB Atlas sur AWS

- Fournisseurs de cloud et régions
- Gérer les clusters mondiaux
- Sélectionnez le niveau du cluster
- Configurer des paramètres supplémentaires
- Commencez avec Atlas
- Configuration de l'accès à l'interface utilisateur d'Atlas
- Gérer les clusters

Migration des données

- Migrer ou importer des données

Clusters de surveillance

- Surveillez vos clusters

Intégration des opérations

- Se connecter à un cluster
- Interagissez avec vos données
- Surveillez vos clusters
- Sauvegarder, restaurer et archiver les données

Entrainement

- Migration en direct avec MongoDB Atlas

Informations supplémentaires

Pour plus d'informations, consultez les rubriques suivantes dans la documentation de MongoDB :

- Pour déplacer des données vers une instance sans serveur, utilisez Compass pour exporter et importer des données, ou migrez des données à l'aide d'outils autogérés. Pour en savoir plus, consultez la section Limitations relatives aux instances sans serveur.

- Pour charger des données dans un nouveau cluster dans Atlas, voir Charger des données dans Atlas.
- Pour créer une copie de votre cluster à des fins de test, consultez la section Méthodes de sauvegarde pour un déploiement autogéré.
- Si l'application que vous souhaitez migrer nécessite une disponibilité quasi continue, contactez le support MongoDB et faites-lui part de vos besoins en termes de disponibilité et de configuration du cluster.
- Pour plus d'informations, consultez la section Migrer ou importer des données.

Migrer une EnterpriseOne base de données Oracle JD Edwards vers AWS à l'aide d'Oracle Data Pump et d'AWS DMS

Créée par Thanigaivel Thirumalai (AWS)

Récapitulatif

Vous pouvez migrer et exécuter votre EnterpriseOne base de données JD Edwards sur Amazon Relational Database Service (Amazon RDS). Lorsque vous migrez votre base de données vers Amazon RDS, AWS peut prendre en charge les tâches de sauvegarde et la configuration de la haute disponibilité, afin que vous puissiez vous concentrer sur la maintenance de votre EnterpriseOne application et de ses fonctionnalités. Pour une liste complète des facteurs clés à prendre en compte lors du processus de migration, consultez les stratégies de migration des bases de données Oracle dans AWS Prescriptive Guidance.

Il existe plusieurs méthodes pour migrer une EnterpriseOne base de données, notamment :

- Utilisation d'Oracle Universal Batch Engine (UBE) R98403 pour la création de schémas et de tables, et utilisation d'AWS Database Migration Service (AWS DMS) pour la migration
- Utilisation des outils natifs de base de données pour la création de schémas et de tables et utilisation d'AWS DMS pour la migration
- Utilisation des outils natifs de base de données pour la migration des données existantes (chargement complet) et utilisation d'AWS DMS pour les tâches de capture des données modifiées (CDC)

Ce modèle couvre la troisième option. Il explique comment migrer vos EnterpriseOne bases de données sur site vers Amazon RDS for Oracle en utilisant Oracle Data Pump avec AWS DMS et sa fonctionnalité CDC.

Oracle JD Edwards EnterpriseOne est une solution de planification des ressources d'entreprise (ERP) destinée aux entreprises qui fabriquent, construisent, distribuent, entretiennent ou gèrent des produits ou des actifs physiques. JD Edwards EnterpriseOne prend en charge divers matériels, systèmes d'exploitation et plateformes de base de données.

Lorsque vous migrez des applications ERP critiques telles que JD Edwards EnterpriseOne, il est essentiel de minimiser les temps d'arrêt. AWS DMS minimise les temps d'arrêt en prenant en charge à la fois le chargement complet et la réplication continue de la base de données source vers la base de données cible. AWS DMS fournit également une surveillance et une journalisation en temps réel

pour la migration, ce qui peut vous aider à identifier et à résoudre les problèmes susceptibles de provoquer des interruptions de service.

Lorsque vous répliquez des modifications avec AWS DMS, vous devez spécifier une heure ou un numéro de modification du système (SCN) comme point de départ pour lire les modifications dans les journaux de base de données. Il est essentiel de garder ces journaux accessibles sur le serveur pendant un certain temps (nous recommandons 15 jours) afin de garantir qu'AWS DMS a accès à ces modifications.

Conditions préalables et limitations

Prérequis

- Une base de données Amazon RDS for Oracle mise en service dans votre environnement cloud AWS en tant que base de données cible. Pour obtenir des instructions, consultez la documentation Amazon RDS.
- EnterpriseOne Base de données exécutée sur site ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2) sur AWS.

> **Note**
>
> Ce modèle est conçu pour effectuer une migration sur site vers AWS, mais il a été testé en utilisant une EnterpriseOne base de données sur une EC2 instance. Si vous envisagez de migrer depuis votre environnement sur site, vous devez configurer la connectivité réseau appropriée.

- Détails du schéma Identifiez le schéma de base de données Oracle (par exemple, DV92 0) pour lequel vous prévoyez de migrer EnterpriseOne. Avant de commencer le processus de migration, collectez les informations suivantes sur le schéma :
  - Taille du schéma
  - Le nombre d'objets par type d'objet
  - Le nombre d'objets non valides

Limites

- Vous devez créer les schémas de votre choix sur la base de données Amazon RDS for Oracle cible. AWS DMS ne les crée pas pour vous. (La section Epics décrit comment utiliser Data Pump pour exporter et importer des schémas.) Le nom du schéma doit déjà exister pour la base de

données Oracle cible. Les tables du schéma source sont importées vers l'utilisateur ou le schéma, et AWS DMS utilise le compte administrateur ou système pour se connecter à l'instance cible. Vous pouvez créer plusieurs tâches de réplication si vous avez plusieurs schémas à migrer. Vous pouvez également migrer des données vers différents schémas sur une instance cible. Pour ce faire, utilisez des règles de transformation de schéma sur les mappages de tables AWS DMS.

- Ce modèle a été testé avec un jeu de données de démonstration. Nous vous recommandons de valider la compatibilité de votre ensemble de données et sa personnalisation.
- Ce modèle utilise une EnterpriseOne base de données exécutée sous Microsoft Windows. Toutefois, vous pouvez utiliser le même processus avec d'autres systèmes d'exploitation pris en charge par AWS DMS.

Architecture

Le schéma suivant montre un système qui s'exécute EnterpriseOne sur une base de données Oracle en tant que base de données source, et une base de données Amazon RDS for Oracle en tant que base de données cible. Les données sont exportées depuis la base de données Oracle source et importées dans la base de données Amazon RDS for Oracle cible à l'aide d'Oracle Data Pump, puis répliquées pour les mises à jour du CDC à l'aide d'AWS DMS.

1. Oracle Data Pump extrait les données de la base de données source et les données sont envoyées à la base de données cible Amazon RDS for Oracle.
2. Les données CDC sont envoyées depuis la base de données source vers un point de terminaison source dans AWS DMS.
3. À partir du point de terminaison source, les données sont envoyées à l'instance de réplication AWS DMS, où la tâche de réplication est exécutée.
4. Une fois la tâche de réplication terminée, les données sont envoyées au point de terminaison cible dans AWS DMS.
5. À partir du point de terminaison cible, les données sont envoyées à l'instance de base de données Amazon RDS for Oracle.

Outils

Services AWS

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.

Autres services

- Oracle Data Pump vous aide à déplacer rapidement des données et des métadonnées d'une base de données à une autre.

Bonnes pratiques

Migrating LOBs

Si votre base de données source contient de gros objets binaires (LOBs) qui doivent être migrés vers la base de données cible, AWS DMS propose les options suivantes :

- Mode LOB complet : AWS DMS migre tous les éléments de la base de données source LOBs vers la base de données cible, quelle que soit leur taille. Bien que la migration soit plus lente que les autres modes, l'avantage est que les données ne sont pas tronquées. Pour de meilleures performances, vous pouvez créer une tâche distincte sur la nouvelle instance de réplication afin de migrer les tables LOBs dont la taille est supérieure à quelques mégaoctets.
- Mode LOB limité : vous spécifiez la taille maximale des données des colonnes LOB, ce qui permet à AWS DMS de préallouer des ressources et de les appliquer en bloc. LOBs Si la taille des colonnes LOB dépasse la taille spécifiée dans la tâche, AWS DMS tronque les données et envoie des avertissements au fichier journal AWS DMS. Vous pouvez améliorer les performances en utilisant le mode LOB limité si la taille de vos données LOB se situe dans les limites de la taille LOB limitée.
- Mode LOB en ligne : vous pouvez migrer LOBs sans tronquer les données ni ralentir les performances de votre tâche en répliquant à la fois les petites et les grandes tâches. LOBs Spécifiez d'abord une valeur pour le `InlineLobMaxSize` paramètre, qui n'est disponible que lorsque le mode LOB complet est défini sur. `true` La tâche AWS DMS transfère le petit LOBs en ligne, ce qui est plus efficace. AWS DMS migre ensuite le fichier volumineux LOBs en effectuant une recherche dans la table source. Cependant, le mode LOB en ligne ne fonctionne que pendant la phase de chargement complet.

Génération de valeurs de séquence

Au cours du processus CDC d'AWS DMS, les numéros de séquence incrémentiels ne sont pas répliqués à partir de la base de données source. Pour éviter les différences dans les valeurs de séquence, vous devez générer la valeur de séquence la plus récente à partir de la source pour toutes les séquences, et l'appliquer à la base de données Amazon RDS for Oracle cible.

AWS Secrets Manager

Pour vous aider à gérer vos informations d'identification, nous vous recommandons de suivre les instructions du billet de blog Gérer les informations d'identification de votre point de terminaison AWS DMS avec AWS Secrets Manager.

Performances

- Instances de réplication – Pour obtenir des conseils sur le choix de la meilleure taille d'instance, consultez la section Sélection de la meilleure taille pour une instance de réplication dans la documentation AWS DMS.
- Options de connectivité – Pour éviter les problèmes de latence, nous vous recommandons de choisir la bonne option de connectivité. AWS Direct Connect fournit le chemin le plus court vers les ressources AWS, car il s'agit d'une connexion dédiée entre les centres de données de votre entreprise et AWS. Pendant le transit, le trafic de votre réseau reste sur le réseau mondial AWS et ne passe jamais par Internet. Cela réduit le risque de rencontrer des goulots d'étranglement ou des augmentations inattendues de la latence par rapport à l'utilisation d'un VPN ou de l'Internet public.
- Bande passante réseau – Pour optimiser les performances, vérifiez que le débit de votre réseau est rapide. Si vous utilisez un tunnel VPN entre votre base de données source sur site et AWS DMS, assurez-vous que la bande passante est suffisante pour votre charge de travail.
- Parallélisme des tâches – Vous pouvez accélérer la réplication des données en chargeant plusieurs tables en parallèle pendant le chargement complet. Ce modèle utilise des points de terminaison RDBMS, de sorte que cette option ne s'applique qu'au processus de chargement complet. Le parallélisme des tâches est contrôlé par le `MaxFullLoadSubTasks` paramètre, qui détermine le nombre de sous-tâches à chargement complet exécutées en parallèle. Par défaut, ce paramètre est défini sur 8, ce qui signifie que huit tables (si elles sont sélectionnées dans le mappage des tables) sont chargées ensemble en mode complet. Vous pouvez ajuster ce paramètre dans la section des paramètres de chargement complet des tâches du script JSON correspondant à la tâche.
- Parallélisme de tables – AWS DMS vous permet également de charger une seule grande table à l'aide de plusieurs threads parallèles. Cela est particulièrement utile pour les tables source

Oracle contenant des milliards d'enregistrements ainsi que plusieurs partitions et sous-partitions. Si la table source n'est pas partitionnée, vous pouvez utiliser des limites de colonnes pour les chargements parallèles.

- Charges fractionnées – Lorsque vous répartissez les charges entre plusieurs tâches ou instances AWS DMS, n'oubliez pas les limites des transactions lorsque vous capturez les modifications.

Épopées

Utiliser Oracle Data Pump pour exporter le EnterpriseOne schéma

Tâche	Description	Compétences requises

Générez le SCN.	Lorsque la base de données source est active et utilisée par l' EnterpriseOne applicati on, lancez l'exportation des données avec Oracle Data Pump. Vous devez d'abord générer un numéro de modification du système (SCN) à partir de la base de données source pour garantir la cohérence des données lors de l'exportation avec Oracle Data Pump et comme point de départ pour le CDC dans AWS DMS.
	
	Pour générer le SCN actuel à partir de votre base de données source, utilisez l'instruction SQL suivante :
	
	`SQL> select current_scn`
	`from v$database;`
	
	`CURRENT_SCN`
	`----------`
		DBA

Tâche	Description	Compétences requises
	`30009727` Enregistrez le SCN généré. Vous utiliserez le SCN lorsque vous exporterez les données et pour créer la tâche de réplication AWS DMS.	

Tâche	Description	Compétences requises

Créez le fichier de paramètres.	Pour créer un fichier de paramètres pour exporter le schéma, vous pouvez utiliser le code suivant.
	
	`directory=DMS_DATA_PUMP_DIR logfile=export_dms.log dumpfile=export_dms_data.dmp schemas=<schema name> flashback_scn=<SCN from previous command>`
	
	Note
	Vous pouvez également définir le vôtre `DATA_PUMP_DIR` en utilisant les commandes suivantes, en fonction de vos besoins.
	
	`SQL> CREATE OR REPLACE DIRECTORY DMS_DATA_PUMP_DIR AS '<Directory for dump>'; Directory created.`
	
	`SQL> GRANT READ, WRITE ON DIRECTORY DMS_DATA_PUMP_DIR TO SYSTEM; Grant succeeded.`
		DBA

Tâche	Description	Compétences requises

Exportez le schéma.	Pour effectuer l'exportation, utilisez l'`expdp`utilitaire comme suit :
	
	`C:\Users\Administrator>expdp system/********@<DB Name> PARFILE='<Path to PAR file create above>'`
	
	`Export: Release 19.0.0.0.0 - Production on *** *** ** **:**:** ****`
	`Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production`
	`Starting "SYSTEM"."SYS_EXPORT_SCHEMA_02":  system/**********@<DB Name>PARFILE='E:\exp_dms_datapump.par'`
	`Processing object type SCHEMA_EXPORT/TABLE/TABLE_DATA`
	`Processing object type SCHEMA_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS`
	`Processing object type SCHEMA_EXPORT/TABL`
		DBA

Tâche	Description	Compétences requises
	E/STATISTICS/TABLE _STATISTICS Processing object type SCHEMA_EXPORT/STAT ISTICS/MARKER Processing object type SCHEMA_EXPORT/USER Processing object type SCHEMA_EXPORT/ROLE _GRANT Processing object type SCHEMA_EXPORT/DEFA ULT_ROLE Processing object type SCHEMA_EXPORT/TABL ESPACE_QUOTA Processing object type SCHEMA_EXPORT/PRE_ SCHEMA/PROCACT_SCHEMA Processing object type SCHEMA_EXPORT/TABLE/ TABLE Processing object type SCHEMA_EXPORT/TABL E/GRANT/OWNER_GRANT/ OBJECT_GRANT Processing object type SCHEMA_EXPORT/TABLE/ INDEX/INDEX Processing object type SCHEMA_EXPORT/TABLE/ CONSTRAINT/CONSTRAINT . . exported "<Schema Name>"."<Table Name>" 228.9 MB 496397 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _02" successfully loaded/unloaded	

Tâche	Description	Compétences requises
	``` ********** ********** ********** ********** **** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_02 is: E:\DMSDUMP\EXPORT_ DMS_DATA.DMP Job "SYSTEM"."SYS_EXPO RT_SCHEMA_02" successfully completed at *** *** ** **:**:** **** elapsed 0 00:01:57 ```	

Utiliser Oracle Data Pump pour importer le EnterpriseOne schéma

Tâche	Description	Compétences requises
Transférez le fichier de vidage vers l'instance cible.	Pour transférer vos fichiers à l'aide de cet `DBMS_FILE_TRANSFER` utilitaire, vous devez créer un lien de base de données entre la base de données source et l'instance Amazon RDS for Oracle. Une fois le lien établi, vous pouvez utiliser l'utilitaire pour transférer les fichiers Data Pump directement vers l'instance Amazon RDS. Vous pouvez également transférer les fichiers Data Pump vers Amazon Simple Storage Service (Amazon S3),	DBA

Tâche	Description	Compétences requises

	puis les importer dans l'instance Amazon RDS for Oracle. Pour plus d'informations sur cette option, consultez la section Informations supplémentaires.
	
	Pour créer un lien de base de données ORARDSDB qui se connecte à l'utilisateur principal Amazon RDS sur l'instance de base de données cible, exécutez les commandes suivantes sur la base de données source :
	
	`sqlplus / as sysdba`
	
	`SQL*Plus: Release 19.0.0.0.0 on *** *** ** **:**:** **** Version 19.3.0.0.0`
	
	`Copyright (c) 1982, 2019, Oracle. All rights reserved.`
	
	`Connected to: Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 Version 19.3.0.0.0`
	
	`SQL> create database link orardsdb connect to admin identified by "******" using '(DESCRIPTION = (ADDRESS = (PROTOCOL =`	

Tâche	Description	Compétences requises
	TCP)(HOST = orcl.**** **.us-east-1.rds.a mazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))'; Database link created. SQL>	
Testez le lien de base de données.	Testez le lien de base de données pour vous assurer que vous pouvez vous connecter à la base de données cible Amazon RDS for Oracle en `sqlplus` utilisant. SQL> select name from v $database@orardsdb; NAME --------- ORCL	DBA

Tâche	Description	Compétences requises

Transférez le fichier de vidage vers la base de données cible.	Pour copier le fichier dump dans la base de données Amazon RDS for Oracle, vous pouvez soit utiliser le répertoire `DATA_PUMP_DIR` par défaut, soit créer votre propre répertoire en utilisant le code suivant, qui doit être exécuté sur l'instance Amazon RDS cible :
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'DMS_TARGET_PUMP_DIR');`
	`PL/SQL procedure successfully completed.`
	Le script suivant copie un fichier de vidage nommé `EXPORT_DMS_DATA.DMP` depuis l'instance source vers une base de données Amazon RDS for Oracle cible en utilisant le lien `orardsdb` de base de données nommé. Vous devez exécuter le script sur l'instance de base de données source.
	`BEGIN DBMS_FILE_TRANSFER.PUT_FILE(`
		DBA

Tâche	Description	Compétences requises

	`source_directory_object => 'DMS_DATA_PUMP_DIR', source_file_name => 'EXPORT_DMS_DATA.DMP', destination_directory_object => 'DMS_TARGET_PUMP_DIR', destination_file_name => 'EXPORT_DMS_DATA.DMP', destination_database => 'orardsdb'); END;`
	
	`PL/SQL procedure successfully completed.`	

Répertoriez le fichier de vidage dans la base de données cible.	Une fois la procédure PL/SQL terminée, vous pouvez répertorier le fichier de vidage de données dans la base de données Amazon RDS for Oracle en utilisant le code suivant : `select * from table (rdsadmin.rds_file_util.listdir(p_directory => 'DMS_TARGET_PUMP_DIR'));`	DBA

Tâche	Description	Compétences requises

Créez des utilisateurs spécifiques à JDE dans l'instance cible.	Créez un profil et un rôle JD Edwards à l'aide des commandes suivantes dans l'instance cible :
	`SQL> CREATE PROFILE "JDEPROFILE" LIMIT IDLE_TIME 15;`
	`Profile created.`
	
	`SQL> CREATE ROLE "JDE_ROLE";`
	`Role created.`
	
	`SQL> CREATE ROLE "JDEADMIN";`
	`CREATE ROLE "JDEUSER";`
	`Role created.`
	`Role created.`
	
	Accordez les autorisations requises au rôle :
	`SQL> GRANT CREATE ANY SEQUENCE TO JDE_ROLE;`
	`GRANT DROP ANY SEQUENCE TO JDE_ROLE;`
	`GRANT CREATE ANY TRIGGER TO JDE_ROLE;`
	`GRANT DROP ANY TRIGGER TO JDE_ROLE;`
		DBA, JDE CNC

Tâche	Description	Compétences requises

Créez des tablespaces dans l'instance cible.	Créez les tablespaces requis dans l'instance cible à l'aide des commandes suivantes pour les schémas concernés par cette migration :
	`SQL> CREATE TABLESPACE <Tablespace Name for Tables>;`
	`Tablespace created.`
	
	`SQL> CREATE TABLESPACE <Tablespace Name for Indexes>;`
	`Tablespace created.`
		DBA, JDE CNC

Tâche	Description	Compétences requises
Lancez l'importation sur la base de données cible.	Avant de commencer le processus d'importation, configurez les rôles, les schémas et les tablespac es sur la base de données Amazon RDS for Oracle cible à l'aide du fichier de vidage de données. Pour effectuer l'importa tion, accédez à la base de données cible avec le compte utilisateur principal Amazon RDS et utilisez le nom de la chaîne de connexion dans le `tnsnames.ora` fichier, qui inclut la base de données Amazon RDS for Oracle. `tns-entry` Si nécessaire, vous pouvez inclure une option de remappage pour importer le fichier de vidage de données dans un autre tablespace ou sous un autre nom de schéma. Pour démarrer l'importation, utilisez le code suivant : `impdp admin@orardsdb directory=DMS_TARG ET_PUMP_DIR logfile=i mport.log dumpfile= EXPORT_DMS_DATA.DMP`	DBA

Tâche	Description	Compétences requises
	Pour garantir le succès de l'importation, vérifiez que le fichier journal d'importation ne contient aucune erreur et vérifiez les détails tels que le nombre d'objets, le nombre de lignes et les objets non valides. Si des objets ne sont pas valides, recompilez-les. Comparez également les objets de base de données source et cible pour vérifier qu'ils correspondent.	

Fournir une instance de réplication AWS DMS avec les points de terminaison source et cible

Tâche	Description	Compétences requises
Téléchargez le modèle .	Téléchargez le modèle AWS CloudFormation DMS_Instance.yaml pour provisionner l'instance de réplication AWS DMS ainsi que ses points de terminaison source et cible.	Administrateur cloud, DBA
Commencez la création de la pile.	1. Connectez-vous à la console de gestion AWS et ouvrez la CloudFormation console AWS à l'adresse https://console.aws.amazon.com/cloudformation. 2. Sélectionnez Créer la pile.	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	3. Dans Spécifier le modèle, sélectionnez Charger un modèle de fichier. 4. Choisissez Choisir un fichier. 5. Choisissez le `DMS_instance.yaml` fichier. 6. Choisissez Suivant.	

Tâche	Description	Compétences requises
Spécifiez les paramètres.	1. Dans Nom de la pile, entrez le nom de la pile. 2. Pour les paramètres d'instance AWS DMS, entrez les paramètres suivants : • DMSInstanceType : choisissez l'instance requise pour l'instance de réplication AWS DMS, en fonction des besoins de votre entreprise. • DMSStorageTaille — Entrez la taille de stockage de l'instance AWS DMS, en fonction de la taille de votre migration. 3. Pour la configuration de la base de données Oracle source, entrez les paramètres suivants : • SourceOracleEndpoi ntID : nom du serveur de base de données Oracle source • SourceOracleDataba seName— Le nom du service de base de données source ou l'ID de session (SID), le cas échéant	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	• SourceOracleUserName— Le nom d'utilisateur de la base de données source (par défaut est`system`) • SourceOracleDBPassword— Le mot de passe du nom d'utilisateur de la base de données source • SourceOracleDBPort— Le port de la base de données source 4. Pour la configuration de la base de données Target RDS pour Oracle, entrez les paramètres suivants : • Target RDSOracle EndpointID : point de terminaison de la base de données RDS cible • Cible RDSOracle DatabaseName : nom de la base de données RDS cible • Target RSOracle UserName — Le nom d'utilisateur RDS cible • Target RDSOracle DBPassword — Le mot de passe RDS cible • TargetOracleDBPort— Le port de base de données RDS cible	

Tâche	Description	Compétences requises
	5. Pour la configuration du VPC, du sous-réseau et du groupe de sécurité, entrez les paramètres suivants : • VPCID — Le VPC pour l'instance de réplication • VPCSecurityGroupId— Le groupe de sécurité VPC pour l'instance de réplication • DMSSubnet1— Le sous-réseau de la zone de disponibilité 1 • DMSSubnet2— Le sous-réseau de la zone de disponibilité 2 6. Choisissez Suivant.	
Créez la pile.	1. Sur la page Configurer les options de pile, pour les balises, entrez des valeurs facultatives. 2. Choisissez Suivant. 3. Sur la page Révision, vérifiez les informations, puis choisissez Soumettre. Le provisionnement devrait être terminé en 5 à 10 minutes environ. Il est terminé lorsque la page AWS CloudFormation Stacks affiche CREATE_COMPLETE.	Administrateur cloud, DBA

Tâche	Description	Compétences requises
Configurez les points de terminaison.	1. Ouvrez la console AWS DMS à l'adresse https://console.aws.amazon.com/dms/v2/. 2. Pour la gestion des ressources, choisissez Instances de réplication, puis passez en revue les instances de réplication. 3. Pour la gestion des ressources, choisissez Endpoints, puis passez en revue les endpoints.	Administrateur cloud, DBA
Testez la connectivité.	Une fois que les points de terminaison source et cible ont indiqué le statut Actif, testez la connectivité. Choisissez Exécuter le test pour chaque point de terminaison (source et cible) pour vous assurer que l'état indique que l'état est réussi.	Administrateur cloud, DBA

Création d'une tâche de réplication AWS DMS pour une réplication en direct

Tâche	Description	Compétences requises
Créez la tâche de réplication.	Créez la tâche de réplication AWS DMS en procédant comme suit : 1. Ouvrez la console AWS DMS à l'adresse https://	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	console.aws.amazon.com/dms/v2/. 2. Dans le volet de navigation, sous Migrer les données, sélectionnez Tâche de migration de base de données. 3. Dans le champ Configuration des tâches, pour Identifiant de tâche, entrez votre identifiant de tâche. 4. Pour instance de réplication, choisissez l'instance de réplication DMS que vous avez créée. 5. Pour Point de terminaison de base de données source, choisissez votre point de terminaison source. 6. Pour le point de terminaison de base de données cible, choisissez votre base de données Amazon RDS for Oracle cible. 7. Pour le type de migration, sélectionnez Répliquer uniquement les modifications de données. Si vous recevez un message indiquant que la journalisation supplémentaire doit être activée, suivez les	

Tâche	Description	Compétences requises
	instructions de la section Dépannage. 8. Dans la zone Paramètres des tâches, choisissez Spécifier le numéro de séquence du journal. 9. Pour le numéro de modification du système, entrez le SCN de base de données Oracle que vous avez généré à partir de la base de données Oracle source. 10. Choisissez Activer la validation. 11. Choisissez Activer CloudWatch les journaux. En activant cette fonctionnalité, vous pouvez valider les données et les CloudWatch journaux Amazon pour consulter les journaux des instances de réplication AWS DMS. 12. Sous Règles de sélection, complétez les informations suivantes : • Pour Schéma, choisissez Enter a schema. • Pour le nom du schéma, entrez le nom du schéma JDE (par exemple : DV920).	

Tâche	Description	Compétences requises
	• Dans Nom de la table, entrez %. • Pour Action, choisissez Inclure. 13. Choisissez Créer tâche. Après avoir créé la tâche, AWS DMS migre les modifications continues apportées à l'instance de base de données Amazon RDS for Oracle à partir du SCN que vous avez fourni en mode de démarrage CDC. Vous pouvez également vérifier la migration en consultant les CloudWatch journaux.	
Répétez la tâche de réplication.	Répétez les étapes précédentes pour créer des tâches de réplication pour les autres schémas JD Edwards inclus dans la migration.	Administrateur cloud, DBA, administrateur JDE CNC

Validez le schéma de base de données sur la base de données Amazon RDS for Oracle cible

Tâche	Description	Compétences requises
Validez le transfert de données.	Une fois la tâche AWS DMS lancée, vous pouvez consulter l'onglet Tableau des statistiques de la page Tâches pour voir les modifications apportées aux données.	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	Vous pouvez surveiller l'état de la réplication en cours dans la console sur la page des tâches de migration de base de données. Pour plus d'informations, consultez la section Validation des données AWS DMS.	

Découper

Tâche	Description	Compétences requises
Arrêtez la réplication.	Interrompez la procédure de réplication et arrêtez les services de l'application source.	Administrateur cloud, DBA
Lancez l'application JD Edwards.	Lancez l'application cible de présentation et de niveau logique de JD Edwards sur AWS, et dirigez-la vers la base de données Amazon RDS for Oracle. Lorsque vous accédez à l'application, vous devez remarquer que toutes les connexions sont désormais établies avec la base de données Amazon RDS for Oracle.	Administrateur DBA, JDE CNC
Éteignez la base de données source.	Après avoir confirmé qu'il n'y a plus de connexions, vous	DBA

Tâche	Description	Compétences requises
	pouvez désactiver la base de données source.	

Résolution des problèmes

Problème	Solution

Vous recevez un message d'avertissement vous demandant d'activer la journalisation supplémentaire dans la base de données source pour une réplication continue	Entrez les commandes suivantes pour activer la journalisation supplémentaire :
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;`
	`SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;`

La journalisation supplémentaire d'AWS DMS est désactivée.	La journalisation supplémentaire est désactivée par défaut dans AWS DMS. Pour l'activer pour un point de terminaison Oracle source : 1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS DMS à l'adresse https://console.aws.amazon.com/dms/v2/. 2. Choisissez Endpoints (Points de terminaison). 3. Choisissez le point de terminaison source Oracle auquel vous souhaitez ajouter la journalisation supplémentaire.

Problème	Solution
	4. Sélectionnez Modifier. 5. Choisissez Avancé, puis ajoutez le code suivant dans la zone de texte Attributs de connexion supplémentaires : `addSupplementalLogging=Y` 6. Sélectionnez Modifier.

La journalisation supplémentaire n'est pas activée au niveau de la CDB.	1. Entrez cette commande :
	`SQL> alter session set container = CDB$ROOT;`
	`Session altered.`
	2. Répétez les étapes pour activer la journalisation supplémentaire.

Vous recevez le message d'erreur suivant : « Échec du point de terminaison du test : état de l'application : 1020912, message de l'application : non pris en charge dans l'environnement Oracle PDB. L' LogMiner initialisation du point de terminaison a échoué ».	Si ce message d'erreur s'affiche, vous pouvez utiliser Binary Reader au lieu de LogMiner. Sous Paramètres du point de terminaison, ajoutez cette ligne aux attributs de connexion supplémentaires pour votre base de données source : `useLogMinerReader=N;useBfile=Y;`

Ressources connexes

- Commencer à utiliser AWS Database Migration Service
- Bonnes pratiques pour AWS Database Migration Service
- Migration des bases de données Oracle vers le cloud AWS
- Référence du type de ressource AWS Database Migration Service pour AWS CloudFormation

- Gérez les informations d'identification de votre point de terminaison AWS DMS avec AWS Secrets Manager
- Résolution des problèmes de migration dans AWS Database Migration Service
- Bonnes pratiques pour AWS Database Migration Service

Informations supplémentaires

Transférer des fichiers à l'aide d'Amazon S3

Pour transférer les fichiers vers Amazon S3, vous pouvez utiliser l'AWS CLI ou la console Amazon S3. Après avoir transféré les fichiers vers Amazon S3, vous pouvez utiliser l'instance Amazon RDS for Oracle pour importer les fichiers Data Pump depuis Amazon S3.

Si vous choisissez de transférer le fichier de vidage en utilisant l'intégration Amazon S3 comme méthode alternative, effectuez les étapes suivantes :

1. Créez un compartiment S3.
2. Exportez les données de la base de données source à l'aide d'Oracle Data Pump.
3. Téléchargez les fichiers Data Pump dans le compartiment S3.
4. Téléchargez les fichiers Data Pump depuis le compartiment S3 vers la base de données Amazon RDS for Oracle cible.
5. Effectuez l'importation à l'aide des fichiers Data Pump.

> **Note**
>
> Pour transférer des fichiers de données volumineux entre des instances S3 et RDS, nous vous recommandons d'utiliser la fonctionnalité Amazon S3 Transfer Acceleration.

Migrer une PeopleSoft base de données Oracle vers AWS à l'aide d'AWS DMS

Créée par sampath kathirvel (AWS)

Récapitulatif

Oracle PeopleSoft est une solution de planification des ressources d'entreprise (ERP) pour les processus à l'échelle de l'entreprise. PeopleSoft possède une architecture à trois niveaux : client, application et base de données. PeopleSoft peut être exécuté sur Amazon Relational Database Service (Amazon RDS).

Si vous migrez votre base de données Oracle vers Amazon RDS, Amazon Web Services (AWS) peut prendre en charge les tâches de sauvegarde et la haute disponibilité, vous laissant ainsi libre de vous concentrer sur la maintenance de votre PeopleSoft application et de ses fonctionnalités. Pour une liste complète des facteurs clés à prendre en compte lors du processus de migration, consultez les stratégies de migration des bases de données Oracle dans AWS Prescriptive Guidance.

Ce modèle fournit une solution pour migrer vos bases de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'Oracle Data Pump avec AWS Database Migration Service (AWS DMS) et de sa fonctionnalité de capture des données de modification (CDC).

Lors de la migration d'applications ERP critiques telles qu'Oracle PeopleSoft, il est essentiel de minimiser les temps d'arrêt. AWS DMS minimise les temps d'arrêt en prenant en charge à la fois le chargement complet et la réplication continue, de la base de données source vers la base de données cible. AWS DMS fournit également une surveillance et une journalisation en temps réel de la migration, ce qui peut vous aider à identifier et à résoudre les problèmes susceptibles de provoquer des interruptions de service.

Lorsque vous répliquez des modifications avec AWS DMS, vous devez spécifier une heure ou un numéro de modification du système (SCN) comme point de départ pour qu'AWS DMS puisse lire les modifications dans les journaux de base de données. Il est essentiel de garder ces journaux accessibles sur le serveur pendant un certain temps afin de garantir qu'AWS DMS ait accès à ces modifications.

Conditions préalables et limitations

Prérequis

- Vous avez provisionné la base de données Amazon RDS for Oracle dans votre environnement cloud AWS en tant que base de données cible.

- Une PeopleSoft base de données Oracle exécutée sur site ou sur Amazon Elastic Compute Cloud (Amazon EC2) dans le cloud AWS.

> **Note**
>
> Ce modèle est conçu pour effectuer une migration sur site vers AWS, mais il a été testé à l'aide d'Oracle Database sur une EC2 instance Amazon. Pour effectuer une migration depuis un environnement local, vous devez configurer la connectivité réseau appropriée.

- Détails du schéma Lors de la migration d'une PeopleSoft application Oracle vers Amazon RDS for Oracle, il est nécessaire d'identifier le schéma de base de données Oracle (par exemple`SYSADM`) à migrer. Avant de démarrer le processus de migration, collectez les informations suivantes sur le schéma :
  - Size
  - Le nombre d'objets par type d'objet
  - Le nombre d'objets non valides.

  Ces informations faciliteront le processus de migration.

Limites

- Ce scénario a été testé uniquement avec la base de données PeopleSoft DEMO. Il n'a pas été testé avec un grand ensemble de données.

Architecture

Le schéma suivant montre une instance exécutant une base de données Oracle en tant que base de données source et une base de données Amazon RDS for Oracle en tant que base de données cible. Les données sont exportées et importées de la base de données Oracle source vers la base de données Amazon RDS for Oracle cible à l'aide d'Oracle Data Pump et répliquées pour les modifications du CDC à l'aide d'AWS DMS.

1. La première étape consiste à extraire les données de la base de données source à l'aide d'Oracle Data Pump, puis à les envoyer à la base de données cible Amazon RDS for Oracle.
2. Les données sont envoyées depuis la base de données source vers un point de terminaison source dans AWS DMS.

3. À partir du point de terminaison source, les données sont envoyées à l'instance de réplication AWS DMS, où la tâche de réplication est exécutée.
4. Une fois la tâche de réplication terminée, les données sont envoyées au point de terminaison cible dans AWS DMS.
5. À partir du point de terminaison cible, les données sont envoyées à l'instance de base de données Amazon RDS for Oracle.

Outils

Services AWS

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.

Autres services

- Oracle Data Pump vous aide à déplacer des données et des métadonnées d'une base de données à une autre à grande vitesse.

Bonnes pratiques

Migrating LOBs

Si votre base de données source contient de gros objets binaires (LOBs) qui doivent être migrés vers la base de données cible, AWS DMS propose les options suivantes :

- Mode LOB complet : AWS DMS migre tous les éléments de la base de données source LOBs vers la base de données cible, quelle que soit leur taille. Bien que la migration soit plus lente, l'avantage est que les données ne sont pas tronquées. Pour de meilleures performances, vous pouvez créer une tâche distincte sur la nouvelle instance de réplication afin de migrer les tables dont la taille est LOBs supérieure à quelques mégaoctets.
- Mode LOB limité : vous spécifiez la taille maximale des données des colonnes LOB, ce qui permet à AWS DMS de préallouer des ressources et de les appliquer en bloc. LOBs Si la taille des colonnes LOB dépasse la taille spécifiée dans la tâche, AWS DMS tronque les données et envoie des avertissements au fichier journal AWS DMS. Vous pouvez améliorer les performances en

utilisant le mode LOB limité si la taille de vos données LOB se situe dans les limites de la taille LOB limitée.

- Mode LOB en ligne : vous pouvez migrer LOBs sans tronquer les données ni ralentir les performances de votre tâche en répliquant à la fois les petites et les grandes tâches. LOBs Spécifiez d'abord une valeur pour le InlineLobMaxSize paramètre, qui n'est disponible que lorsque le mode LOB complet est défini sur true. La tâche AWS DMS transfère le petit LOBs en ligne, ce qui est plus efficace. AWS DMS migre ensuite le fichier volumineux LOBs en effectuant une recherche dans la table source. Cependant, le mode LOB intégré ne fonctionne que pendant la phase de chargement complet.

Génération de valeurs de séquence

N'oubliez pas que pendant le processus de capture des données de modification avec AWS DMS, les numéros de séquence incrémentiels ne sont pas répliqués depuis la base de données source. Pour éviter les différences dans les valeurs de séquence, vous devez générer la valeur de séquence la plus récente à partir de la source pour toutes les séquences, et l'appliquer à la base de données Amazon RDS for Oracle cible.

Gestion des accréditations

Pour sécuriser vos ressources AWS, nous vous recommandons de suivre les meilleures pratiques relatives à AWS Identity and Access Management (IAM).

Épopées

Fournir une instance de réplication AWS DMS avec les points de terminaison source et cible

Tâche	Description	Compétences requises
Téléchargez le modèle .	Téléchargez le CloudFormation modèle AWS DMS_Instance.yaml pour provisionner l'instance de réplication AWS DMS ainsi que ses points de terminaison source et cible.	Administrateur cloud, DBA
Commencez la création de la pile.	1. Sur la console de gestion AWS, choisissez CloudFormation.	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	2. Sélectionnez Créer la pile. 3. Dans Spécifier le modèle, sélectionnez Charger un modèle de fichier. 4. Choisissez Choisir un fichier. 5. Choisissez le `DMS_instance.yaml` fichier. 6. Choisissez Suivant.	

Tâche	Description	Compétences requises
Spécifiez les paramètres.	1. Dans le champ Nom de la pile, entrez le nom de la pile. 2. Sous Paramètres d'instance AWS DMS, entrez les paramètres suivants : • DMSInstanceType : choisissez l'instance requise pour l'instance de réplication AWS DMS, en fonction des besoins de votre entreprise. • DMSStorageTaille — Entrez la taille de stockage de l'instance AWS DMS, en fonction de la taille de votre migration. 3. Dans Configuration de la base de données Oracle source, entrez les paramètres suivants : • SourceOracleEndpointID : nom du serveur de base de données Oracle source • SourceOracleDatabaseName— Le nom du service de base de données source ou l'ID de session (SID), le cas échéant	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	• SourceOracleUserName— Le nom d'utilisateur de la base de données source (le nom par défaut est system) • SourceOracleDBPassword— Le mot de passe du nom d'utilisateur de la base de données source • SourceOracleDBPort— Le port de la base de données source 4. Sous Configuration de la base de données Target RDS pour Oracle, entrez les paramètres suivants : • Target RDSOracle EndpointID : point de terminaison de la base de données RDS cible • Cible RDSOracle DatabaseName : nom de la base de données RDS cible • Target RSOracle UserName — Le nom d'utilisateur RDS cible • Target RDSOracle DBPassword — Le mot de passe RDS cible • TargetOracleDBPort— Le port de base de données RDS cible	

Tâche	Description	Compétences requises
	5. Dans Configuration du VPC, du sous-réseau et du groupe de sécurité, entrez les paramètres suivants : • VPCID — Le VPC pour l'instance de réplication • VPCSecurityGroupId— Le groupe de sécurité VPC pour l'instance de réplication • DMSSubnet1— Le sous-réseau de la zone de disponibilité 1 • DMSSubnet2— Le sous-réseau de la zone de disponibilité 2 6. Choisissez Suivant.	
Créez la pile.	1. Sur la page Configurer les options de pile, pour les balises, entrez des valeurs facultatives. 2. Choisissez Suivant. 3. Sur la page Révision, vérifiez les informations, puis choisissez Soumettre. Le provisionnement devrait être terminé en 5 à 10 minutes environ. Il est terminé lorsque la page AWS CloudFormation Stacks affiche CREATE_COMPLETE.	Administrateur cloud, DBA

Tâche	Description	Compétences requises
Configurez les points de terminaison.	1. Dans la console de gestion AWS, sélection nez Database Migration Services. 2. Sous Gestion des ressources, sélectionnez Instances de réplication. 3. Sous Gestion des ressources, sélectionnez Endpoints.	Administrateur cloud, DBA
Testez la connectivité.	Une fois que les points de terminaison source et cible ont affiché le statut Actif, testez la connectivité. Choisissez Exécuter le test pour chaque point de terminaison (source et cible) pour vous assurer que l'état indique que l'état est réussi.	Administrateur cloud, DBA

Exportez le PeopleSoft schéma depuis la base de données Oracle locale à l'aide d'Oracle Data Pump

Tâche	Description	Compétences requises
Générez le SCN.	Lorsque la base de données source est active et utilisée par l'application, lancez l'exportation des données avec Oracle Data Pump. Vous devez d'abord générer un numéro de modification du système (SCN) à partir de la base de données source	DBA

Tâche	Description	Compétences requises

	pour garantir la cohérence des données lors de l'exportation avec Oracle Data Pump et comme point de départ pour la capture des données de modification dans AWS DMS.
	
	Pour générer le SCN actuel à partir de votre base de données source, entrez l'instruction SQL suivante.
	
	`SQL> select name from v$database;`
	`SQL> select name from v$database;`
	`NAME`
	`---------`
	`PSFTDMO`
	`SQL> SELECT current_scn FROM v$database;`
	`CURRENT_SCN`
	`-----------`
	`23792008`
	
	Enregistrez le SCN généré pour l'utiliser lorsque vous exportez les données et pour créer la tâche de réplication AWS DMS.	

Tâche	Description	Compétences requises

Créez le fichier de paramètres.	Pour créer un fichier de paramètres pour exporter le schéma, vous pouvez utiliser le code suivant.
	`$ cat exp_datapmp.par`
	`userid=system/*******`
	`directory=DATA_P`
	`UMP_DIR`
	`logfile=export_dms_`
	`sample_user.log`
	`dumpfile=export_dms_`
	`sample_data_%U.dmp`
	`schemas=SYSADM`
	`flashback_scn=237920`
	`08`
	Note
	Vous pouvez également définir le vôtre `DATA_PUMP_DIR` en utilisant les commandes suivantes, en fonction de vos besoins.
	`SQL> CREATE OR REPLACE`
	`DIRECTORY DATA_PUMP`
	`_DIR AS '/opt/oracle/`
	`product/19c/dbhome_1/`
	`dmsdump/';`
	`Directory created.`
	`SQL> GRANT READ, WRITE`
	`ON DIRECTORY DATA_PUMP`
	`_DIR TO system;`
		DBA

Tâche	Description	Compétences requises
	Grant succeeded. SQL> SQL> SELECT owner, directory_name, directory_path FROM dba_directories WHERE directory_name='DA TA_PUMP_DIR'; OWNER DIRECTORY_NAME DIRECTORY_PATH ---------- ---------- ---------- ---------- ---------- ---------- SYS DATA_PUMP_DIR /opt/ oracle/product/19c/dbh ome_1/dmsdump/	

Tâche	Description	Compétences requises
Exportez le schéma.	Pour effectuer l'exportation, utilisez l'`expdp`utilitaire. `$ expdp parfile=e xp_datapmp.par .... Transferring the dump file with DBMS_FILE _TRANSFER to Target: . . exported "SYSADM". "PS_XML_TEMPLT_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_TEMPLT_LNK" 6.328 KB 0 rows . . exported "SYSADM". "PS_XML_XLATDEF_LNG" 6.320 KB 0 rows . . exported "SYSADM". "PS_XML_XLATITM_LNG" 7.171 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNCNTL" 7.601 KB 0 rows . . exported "SYSADM". "PS_XPQRYRUNPARM" 7.210 KB 0 rows . . exported "SYSADM". "PS_YE_AMOUNTS" 9.351 KB 0 rows . . exported "SYSADM". "PS_YE_DATA" 16.58 KB 0 rows . . exported "SYSADM". "PS_YE_EE" 6.75 KB 0 rows . . exported "SYSADM". "PS_YE_W2CP_AMOUNTS" 9.414 KB 0 rows`	DBA

Tâche	Description	Compétences requises
	. . exported "SYSADM". "PS_YE_W2CP_DATA" 20.94 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_AMOUNTS" 10.27 KB 0 rows . . exported "SYSADM". "PS_YE_W2C_DATA" 20.95 KB 0 rows . . exported "SYSADM". "PS_ZBD_JOBCODE_TBL" 14.60 KB 0 rows . . exported "SYSADM". "PTGRANTTBL" 5.468 KB 0 rows Master table "SYSTEM". "SYS_EXPORT_SCHEMA _01" successfully loaded/unloaded ** Dump file set for SYSTEM.SYS_EXPORT_ SCHEMA_01 is: /opt/oracle/pr oduct/19c/dbhome_1 /dmsdump/export_dm s_sample_data_01.dmp Job "SYSTEM"."SYS_EXPO RT_SCHEMA_01" successfully completed at Mon Dec 19 20:13:57 2022 elapsed 0 00:38:22	

Importez le PeopleSoft schéma dans la base de données Amazon RDS for Oracle à l'aide d'Oracle Data Pump

Tâche	Description	Compétences requises
Transférez le fichier de vidage vers l'instance cible.	Pour transférer vos fichiers à l'aide de`DBMS_FILE_TRANSFER`, vous devez créer un lien de base de données entre la base de données source et l'instance Amazon RDS for Oracle. Une fois le lien établi, vous pouvez utiliser l'utilitaire pour transférer les fichiers Data Pump directement vers l'instance RDS. Vous pouvez également transférer les fichiers Data Pump vers Amazon Simple Storage Service (Amazon S3), puis les importer dans l'instance Amazon RDS for Oracle. Pour plus d'informations sur cette option, consultez la section Informations supplémentaires. Pour créer un lien de base de données `ORARDSDB` qui se connecte à l'utilisateur principal Amazon RDS sur l'instance de base de données cible, exécutez les commandes suivantes sur la base de données source.	DBA

Tâche	Description	Compétences requises

	`$sqlplus / as sysdba`
	`$ SQL> create database link orardsdb connect to admin identified by "*****" using '(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = testpsft.*******.us-west-2.rds.amazonaws.com)(PORT = 1521))(CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = orcl)))';`
	`Database link created.`	

Testez le lien de base de données.	Testez le lien de base de données pour vous assurer que vous pouvez vous connecter via sqlplus à la base de données cible Amazon RDS for Oracle.
	`SQL>`
	`SQL> select name from v$database@orardsdb;`
	`NAME`
	`---------`
	`ORCL`
	`SQL>`
		DBA

Tâche	Description	Compétences requises

Transférez le fichier de vidage vers la base de données cible.	Pour copier le fichier de vidage dans la base de données Amazon RDS for Oracle, vous pouvez soit utiliser le répertoire `DATA_PUMP_DIR` par défaut, soit créer votre propre répertoire à l'aide du code suivant.
	`exec rdsadmin.rdsadmin_util.create_directory(p_directory_name => 'TARGET_PUMP_DIR') ;`
	Le script suivant copie un fichier de vidage nommé `export_dms_sample_data_01.dmp` depuis l'instance source vers une base de données Amazon RDS for Oracle cible à l'aide du lien `orardsdb` de base de données nommé.
	`$ sqlplus / as sysdba SQL> BEGIN DBMS_FILE_TRANSFER .PUT_FILE( source_directory_object => 'DATA_PUMP_DIR', source_file_name => 'export_dms_sample_data_01.dmp',`
		DBA

Tâche	Description	Compétences requises
	`destination_directory _object => 'TARGET_P UMP_DIR'', destination_file_name => 'export_dms_sample _data_01.dmp', destination_database => 'orardsdb' ); END; / PL/SQL procedure successfully completed .`	
Répertoriez le fichier de vidage dans la base de données cible.	Une fois la procédure PL/SQL terminée, vous pouvez répertorier le fichier de vidage de données dans la base de données Amazon RDS for Oracle en utilisant le code suivant. `SQL> select * from table (rdsadmin.rds_file _util.listdir(p_di rectory => 'TARGET_P UMP_DIR'));`	DBA

Tâche	Description	Compétences requises
Lancez l'importation sur la base de données cible.	Avant de commencer le processus d'importation, configurez les rôles, les schémas et les tablespac es sur la base de données Amazon RDS for Oracle cible à l'aide du fichier de vidage de données. Pour effectuer l'importa tion, accédez à la base de données cible avec le compte utilisateur principal Amazon RDS et utilisez le nom de la chaîne de connexion dans le `tnsnames.ora` fichier, qui inclut la base de données Amazon RDS for Oracle. `tns-entry` Si nécessaire, vous pouvez inclure une option de remappage pour importer le fichier de vidage de données dans un autre tablespace ou sous un autre nom de schéma. Pour démarrer l'importation, utilisez le code suivant. `impdp admin@orardsdb directory=TARGET_P UMP_DIR logfile=i mport.log dumpfile= export_dms_sample_ data_01.dmp`	DBA

Tâche	Description	Compétences requises
	Pour garantir le succès de l'importation, vérifiez que le fichier journal d'importation ne contient aucune erreur et vérifiez les détails tels que le nombre d'objets, le nombre de lignes et les objets non valides. Si des objets ne sont pas valides, recompilez-les. Comparez également les objets de base de données source et cible pour vérifier qu'ils correspondent.	

Créez une tâche de réplication AWS DMS à l'aide du CDC pour effectuer une réplication en direct

Tâche	Description	Compétences requises
Créez la tâche de réplication.	Créez la tâche de réplication AWS DMS en procédant comme suit : 1. Sur la console AWS DMS, sous Conversion et migration, sélectionnez Tâche de migration de base de données. 2. Sous Configuration des tâches, dans Identifiant de tâche, entrez votre identifiant de tâche. 3. Pour instance de réplication, choisissez l'instance de	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	réplication DMS que vous avez créée. 4. Pour Point de terminaison de base de données source, choisissez votre point de terminaison source. 5. Pour le point de terminaison de base de données cible, choisissez votre base de données Amazon RDS for Oracle cible. 6. Pour le type de migration , sélectionnez Répliquer uniquement les modifications de données. Si vous recevez un message indiquant que la journalisation supplémentaire doit être activée, suivez les instructions de la section Informations supplémentaires. 7. Sous Paramètres des tâches, sélectionnez Spécifier le numéro de séquence du journal. 8. Pour le numéro de modification du système, entrez le SCN de base de données Oracle que vous avez généré à partir de la base de données Oracle source.	

Tâche	Description	Compétences requises
	9. Choisissez Activer la validation. 10. Choisissez Activer CloudWatch les journaux. En activant cette fonctionn alité, vous pouvez valider les données et les CloudWatch journaux Amazon pour consulter les journaux des instances de réplication AWS DMS. 11. Sous Règles de sélection, complétez les informations suivantes : • Pour Schéma, choisissez Enter a schema. • Dans le champ Nom du schéma, entrez SYSADM. • Dans le champ Nom de la table, entrez %. • Pour Action, choisissez Inclure. 12. Sous Règles de transform ation, effectuez les opérations suivantes : • Pour Target, choisissez Table. • Pour Nom du schéma, choisissez Entrer un schéma.	

Tâche	Description	Compétences requises
	• Dans le champ Nom du schéma, entrez SYSADM. • Pour Action, choisissez Renommer en. 13. Choisissez Créer tâche. Après avoir créé la tâche, elle fait migrer le CDC vers l'instance de base de données Amazon RDS for Oracle à partir du SCN que vous avez fourni en mode de démarrage CDC. Vous pouvez également vérifier en consultant les CloudWatch journaux.	

Validez le schéma de base de données sur la base de données Amazon RDS for Oracle cible

Tâche	Description	Compétences requises
Validez le transfert de données.	Une fois la tâche AWS DMS lancée, vous pouvez consulter l'onglet Tableau des statistiq ues de la page Tâches pour voir les modifications apportées aux données. Vous pouvez surveiller l'état de la réplication en cours dans la console sur la page des tâches de migration de base de données.	Administrateur cloud, DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Validation des données AWS DMS.	

Découper

Tâche	Description	Compétences requises
Arrêtez la réplication.	Interrompez la procédure de réplication et arrêtez les services de l'application source.	Administrateur cloud, DBA
Lancez le niveau PeopleSoft intermédiaire.	Lancez l'application cible de niveau PeopleSoft intermédiaire dans AWS et dirigez-la vers la base de données Amazon RDS for Oracle récemment migrée. Lorsque vous accédez à l'application, vous devez remarquer que toutes les connexions de l'application sont désormais établies avec la base de données Amazon RDS for Oracle.	DBA, administrateur PeopleSoft
Éteignez la base de données source.	Une fois que vous avez confirmé qu'il n'y a plus de connexions à la base de données source, vous pouvez la désactiver.	DBA

Ressources connexes

- Commencer à utiliser AWS Database Migration Service
- Bonnes pratiques pour AWS Database Migration Service
- Migration des bases de données Oracle vers le cloud AWS

Informations supplémentaires

Transférer des fichiers à l'aide d'Amazon S3

Pour transférer les fichiers vers Amazon S3, vous pouvez utiliser l'AWS CLI ou la console Amazon S3. Après avoir transféré les fichiers vers Amazon S3, vous pouvez utiliser l'instance Amazon RDS for Oracle pour importer les fichiers Data Pump depuis Amazon S3.

Si vous choisissez de transférer le fichier de vidage en utilisant l'intégration Amazon S3 comme méthode alternative, effectuez les étapes suivantes :

1. Créez un compartiment S3.
2. Exportez les données de la base de données source à l'aide d'Oracle Data Pump.
3. Téléchargez les fichiers Data Pump dans le compartiment S3.
4. Téléchargez les fichiers Data Pump depuis le compartiment S3 vers la base de données Amazon RDS for Oracle cible.
5. Effectuez l'importation à l'aide des fichiers Data Pump.

> **Note**
>
> Pour transférer des fichiers de données volumineux entre des instances S3 et RDS, il est recommandé d'utiliser la fonctionnalité Amazon S3 Transfer Acceleration.

Activer la journalisation supplémentaire

Si vous recevez un message d'avertissement vous demandant d'activer la journalisation supplémentaire dans la base de données source pour une réplication continue, procédez comme suit.

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
```

```
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (FOREIGN KEY) COLUMNS;
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (UNIQUE) COLUMNS;
```

Migrer une base de données MySQL sur site vers Amazon RDS for MySQL

Créée par Lorenzo Mota (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données MySQL locale vers Amazon Relational Database Service (Amazon RDS) pour MySQL. Le modèle décrit l'utilisation de AWS Database Migration Service (AWS DMS) ou d'outils MySQL natifs tels que mysqldump pour une migration complète de base de données. Ce modèle est principalement destiné DBAs aux architectes de solutions. Il peut être utilisé dans des projets de petite ou de grande envergure en tant que procédure de test (nous recommandons au moins un cycle de test) ou en tant que procédure de migration finale.

Conditions préalables et limitations

Prérequis

- Un AWS compte actif
- Une base de données source MySQL dans un centre de données sur site

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- Versions de MySQL 5.5, 5.6, 5.7, 8.0. Pour obtenir la dernière liste des versions prises en charge, consultez MySQL sur Amazon RDS dans la AWS documentation. Si vous utilisez AWS DMS, consultez également Utiliser une base de données compatible MySQL comme cible pour les versions de AWS DMS MySQL actuellement prises en charge par. AWS DMS

Architecture

Pile technologique source

- Une base de données MySQL sur site

Pile technologique cible

- Une instance de base de données Amazon RDS exécutant MySQL

Architecture cible

Le schéma suivant montre l'implémentation cible d'Amazon RDS for MySQL après la migration.

AWS architecture de migration des données

En utilisant AWS DMS :

Le schéma suivant montre l'architecture de migration des données que vous utilisez AWS DMS pour envoyer des modifications complètes et incrémentielles jusqu'au passage. La connexion réseau depuis le site vers le réseau AWS dépend de vos besoins et n'est pas couverte par ce modèle.

À l'aide des outils MySQL natifs :

Le schéma suivant montre l'architecture de migration des données lorsque vous utilisez des outils MySQL natifs. Les fichiers de vidage d'exportation sont copiés sur Amazon Simple Storage Service (Amazon S3) et importés dans la base de données Amazon RDS for AWS MySQL avant le transfert. La connexion réseau depuis le site vers le réseau AWS dépend de vos besoins et n'est pas couverte par ce modèle.

Remarques :

- En fonction des besoins en temps d'arrêt et de la taille de la base de données, l'utilisation AWS DMS ou un outil de capture des données modifiées (CDC) permet de minimiser le temps de transition. AWS DMS peut aider à réduire au minimum le temps de transfert vers la nouvelle cible (généralement quelques minutes). Une stratégie hors ligne avec mysqldump peut suffire si la taille de la base de données et la latence du réseau permettent une courte période. (Nous vous recommandons de tester pour obtenir une durée approximative.)
- Habituellement, une stratégie du CDC telle que celle-ci AWS DMS nécessite plus de surveillance et de complexité que les options hors ligne.

Outils

- AWS services :AWS Database Migration Service (AWS DMS) vous aide à migrer les banques de données vers ou entre des combinaisons de configurations cloud et sur site. AWS Cloud Pour plus d'informations sur les bases de données source et cible MySQL prises en charge par AWS DMS, consultez Migration de bases de données compatibles MySQL vers. AWS Si votre base de données source n'est pas prise en charge par AWS DMS, vous devez choisir une autre méthode pour migrer vos données.
- Outils MySQL natifs : mysqldump
- Outils tiers : Percona XtraBackup

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions de base de données	Validez les versions de base de données source et cible.	DBA
Identifiez les exigences matérielles.	Identifiez la configuration matérielle requise pour le serveur cible.	DBA, administrateur système
Identifiez les besoins en matière de stockage.	Identifiez les exigences de stockage (telles que le type et la capacité de stockage) pour la base de données cible.	DBA, administrateur système
Choisissez le type d'instance.	Choisissez le type d'instanc e cible en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.	DBA, administrateur système
Identifiez les exigences en matière d'accès au réseau.	Identifiez les exigences de sécurité relatives à l'accès	DBA, administrateur système

Tâche	Description	Compétences requises
	au réseau pour les bases de données source et cible.	
Identifiez les objets non pris en charge.	Identifiez les objets non pris en charge (le cas échéant) et déterminez l'effort de migration .	DBA
Identifiez les dépendances.	Identifiez toute dépendanc e vis-à-vis des bases de données distantes.	DBA
Déterminez la stratégie de migration des applications.	Déterminez la stratégie de migration des applications clientes.	DBA, propriétaire de l'applica tion, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)	Configurez les tables de routage, la passerelle Internet, les passerelles NAT et les sous-réseaux. Pour plus d'informations, consultez VPCs Amazon RDS dans la documentation Amazon RDS.	Administrateur de systèmes
Créez des groupes de sécurité.	Configurez les ports et les plages d'adresses CIDR ou spécifiques IPs en fonction de vos besoins. Le port par défaut pour MySQL est 3306. Pour plus d'informations, consultez la section Contrôle	Administrateur de systèmes

Tâche	Description	Compétences requises
	de l'accès avec les groupes de sécurité dans la documentation Amazon RDS.	
Configurez et démarrez une instance de base de données Amazon RDS for MySQL.	Pour obtenir des instructions, consultez la section Création d'une instance de base de données Amazon RDS dans la documentation Amazon RDS. Vérifiez les versions prises en charge.	Administrateur de systèmes

Migrer les données – option 1 (à l'aide d'outils natifs)

Tâche	Description	Compétences requises
Utilisez des outils MySQL natifs ou des outils tiers pour migrer des objets et des données de base de données.	Pour obtenir des instructions, consultez la documentation des outils MySQL tels que mysqldump et Percona XtraBackup (pour la migration physique). Pour plus d'informations sur les options, consultez le billet de blog Options de migration pour MySQL vers Amazon RDS for MySQL ou Amazon Aurora MySQL.	DBA

Migrer les données – option 2 (en utilisant AWS DMS)

Tâche	Description	Compétences requises
Migrez les données avec AWS DMS.	Pour obtenir des instructi ons, consultez la AWS DMS documentation.	DBA

Effectuez des tâches préliminaires avant le passage au poste

Tâche	Description	Compétences requises
Corrigez les écarts dans le nombre d'objets.	Collectez le nombre d'objets à partir de la base de données source et de la nouvelle base de données cible. Corrigez les anomalies dans la base de données cible.	DBA
Vérifiez les dépendances.	Vérifiez si les dépendanc es (liens) vers et depuis d'autres bases de données sont valides et fonctionnent comme prévu.	DBA
Réaliser des tests.	S'il s'agit d'un cycle de test, effectuez des tests de requêtes, collectez des métriques et corrigez les problèmes.	DBA

Découper

Tâche	Description	Compétences requises
Basculez vers la base de données cible.	Basculez les applications clientes vers la nouvelle infrastructure.	DBA, propriétaire de l'application, administrateur système
Fournir une assistance en matière de tests.	Fournir une assistance pour les tests fonctionnels des applications.	DBA

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources.	Arrêtez les AWS ressources temporaires que vous avez créées pour la migration.	DBA, administrateur système
Validez les documents du projet.	Passez en revue et validez les documents du projet.	DBA, propriétaire de l'application, administrateur système
Collectez des statistiques.	Collectez des indicateurs tels que le temps de migration, le pourcentage d'efforts manuels par rapport aux efforts automatisés, les économies de coûts, etc.	DBA, propriétaire de l'application, administrateur système
Clôturez le projet.	Clôturez le projet et faites part de vos commentaires.	DBA, propriétaire de l'application, administrateur système
Désactivez la base de données source.	Lorsque toutes les tâches de migration et de transfert sont terminées, désactivez la base de données locale.	DBA, administrateur système

Ressources connexes

Références

- Migration strategy for relational databases
- AWS DMS website
- AWS DMS documentation
- Documentation Amazon RDS
- Tarification d’Amazon RDS
- Amazon VPC et Amazon RDS
- Déploiements multi-AZ d'Amazon RDS
- Migrez des bases de données MySQL sur site vers Aurora MySQL à l'aide de Percona, XtraBackup Amazon EFS et Amazon S3
- Stockage d'instance de base de données Amazon RDS

Didacticiels

- Commencer avec AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)

Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server

Créée par Henrique Lobao (AWS), Jonathan Pereira Cruz (AWS) et Vishal Singh (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données Microsoft SQL Server locale vers Amazon Relational Database Service (Amazon RDS) pour SQL Server. Il décrit deux options de migration : utiliser AWS Data Migration Service (AWS DMS) ou utiliser les outils natifs de Microsoft SQL Server tels que Copy Database Wizard.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Microsoft SQL Server source dans un centre de données sur site

Limites

- Limite de taille de base de données : 16 To

Versions du produit

- SQL Server 2014-2019, éditions Enterprise, Standard, Workgroup et Developer. Pour obtenir la dernière liste des versions et fonctionnalités prises en charge, consultez Microsoft SQL Server sur Amazon RDS dans la documentation AWS. Si vous utilisez AWS DMS, consultez également Utilisation d'une base de données Microsoft SQL Server comme cible pour les versions d'AWS DMS pour SQL Server prises en charge par AWS DMS.

Architecture

Pile technologique source

- Une base de données Microsoft SQL Server sur site

Pile technologique cible

- Une instance de base de données Amazon RDS pour SQL Server

Architecture source et cible

À l'aide d'AWS DMS :

À l'aide des outils SQL Server natifs :

Outils

- AWS DMS prend en charge plusieurs types de bases de données source et cible. Pour plus de détails, consultez les procédures pas à pas d'AWS DMS Step-by-Step. Si AWS DMS ne prend pas en charge la base de données source, sélectionnez une autre méthode pour migrer les données.
- Les outils natifs de Microsoft SQL Server incluent la sauvegarde et la restauration, l'assistant de copie de base de données, la copie et l'attachement de base de données.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez la version et le moteur de la base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, administrateur système
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, administrateur système
Choisissez le type d'instanc e approprié en fonction de la		DBA, administrateur système

Tâche	Description	Compétences requises
capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, administrateur système
Identifiez la stratégie de migration des applications.		DBA, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)		Administrateur de systèmes
Créez des groupes de sécurité.		Administrateur de systèmes
Configurez et démarrez une instance de base de données Amazon RDS.		DBA, administrateur système

Migrer les données - option 1

Tâche	Description	Compétences requises
Utilisez des outils SQL Server natifs ou des outils tiers pour migrer les objets et les données de base de données.		DBA

Migrer les données - option 2

Tâche	Description	Compétences requises
Migrez les données avec AWS DMS.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.		DBA, propriétaire de l'application, administrateur système

Découper

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, administrateur système
Passez en revue et validez les documents du projet.		DBA, propriétaire de l'application, administrateur système
Collectez des indicateurs tels que le temps de migration , le pourcentage de tâches		DBA, propriétaire de l'application, administrateur système

Tâche	Description	Compétences requises
manuelles par rapport aux tâches automatisées et les économies de coûts.		
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de l'application, administrateur système

Ressources connexes

Références

- Déploiement de Microsoft SQL Server sur Amazon Web Services
- Site Web AWS DMS
- Tarification d'Amazon RDS
- Produits Microsoft sur AWS
- Licences Microsoft sur AWS
- Microsoft SQL Server sur AWS
- Utilisation de l'authentification Windows avec une instance de base de données Microsoft SQL Server
- Déploiements multi-AZ d'Amazon RDS

Tutoriels et vidéos

- Commencer à utiliser AWS DMS
- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)
- AWS DMS (vidéo)
- Amazon RDS (vidéo)

Migrez les données de Microsoft Azure Blob vers Amazon S3 à l'aide de Rclone

Créée par Suhas Basavaraj (AWS), Aidan Keane (AWS) et Corey Lane (AWS)

Récapitulatif

Ce modèle décrit comment utiliser Rclone pour migrer des données depuis le stockage d'objets Microsoft Azure Blob vers un bucket Amazon Simple Storage Service (Amazon S3). Vous pouvez utiliser ce modèle pour effectuer une migration ponctuelle ou une synchronisation continue des données. Rclone est un programme de ligne de commande écrit en Go et utilisé pour déplacer des données entre différentes technologies de stockage proposées par des fournisseurs de cloud.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Données stockées dans le service de conteneur Azure Blob

Architecture

Pile technologique source

- Conteneur de stockage Azure Blob

Pile technologique cible

- Compartiment Amazon S3
- Instance Linux Amazon Elastic Compute Cloud (Amazon EC2)

Architecture

Outils

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Rclone est un programme de ligne de commande open source inspiré de rsync. Il est utilisé pour gérer les fichiers sur de nombreuses plateformes de stockage cloud.

Bonnes pratiques

Lorsque vous migrez des données d'Azure vers Amazon S3, tenez compte de ces considérations afin d'éviter des coûts inutiles ou des vitesses de transfert lentes :

- Créez votre infrastructure AWS dans la même région géographique que le compte de stockage Azure et le conteneur Blob, par exemple, la région AWS `us-east-1` (Virginie du Nord) et la région Azure. `East US`
- Évitez si possible d'utiliser la passerelle NAT, car elle entraîne des frais de transfert de données pour la bande passante d'entrée et de sortie.
- Utilisez un point de terminaison de passerelle VPC pour Amazon S3 afin d'améliorer les performances.
- Envisagez d'utiliser une EC2 instance basée sur le processeur AWS Graviton2 (ARM) pour réduire les coûts et améliorer les performances par rapport aux instances Intel x86. Rclone est fortement compilé de manière croisée et fournit un binaire ARM précompilé.

Épopées

Préparez les ressources du cloud AWS et Azure

Tâche	Description	Compétences requises
Préparez un compartiment S3 de destination.	Créez un nouveau compartiment S3 dans la région AWS appropriée ou choisissez un compartiment existant comme destination pour les données que vous souhaitez migrer.	Administrateur AWS
Créez un rôle d'instance IAM pour Amazon EC2.	Créez un nouveau rôle AWS Identity and Access Management (IAM) pour Amazon EC2. Ce rôle donne à votre EC2 instance un accès en écriture au compartiment S3 de destination.	Administrateur AWS

Tâche	Description	Compétences requises
Attachez une politique au rôle d'instance IAM.	Utilisez la console IAM ou l'interface de ligne de commande AWS (AWS CLI) pour créer une politique en ligne pour EC2 le rôle d'instance qui autorise les autorisations d'accès en écriture au compartiment S3 de destination. Pour un exemple de politique, consultez la section Informations supplémentaires.	Administrateur AWS
Lancez une EC2 instance.	Lancez une EC2 instance Amazon Linux configuré e pour utiliser le rôle de service IAM nouvellement créé. Cette instance devra également accéder aux points de terminaison de l'API publique Azure via Internet. **Note** Envisagez d'utiliser des EC2 instances basées sur AWS Graviton pour réduire les coûts. Rclone fournit des fichiers binaires compilés par ARM.	Administrateur AWS

Tâche	Description	Compétences requises
Créez un principal de service Azure AD.	Utilisez la CLI Azure pour créer un principal de service Azure Active Directory (Azure AD) disposant d'un accès en lecture seule au conteneur de stockage Azure Blob source. Pour obtenir des instructions, consultez la section Informations supplémentaires. Stockez ces informations d'identification sur votre EC2 instance à cet emplacement `~/azure-principal.json` .	Administrateur du cloud, Azure

Installation et configuration de Rclone

Tâche	Description	Compétences requises
Téléchargez et installez Rclone.	Téléchargez et installez le programme de ligne de commande Rclone. Pour les instructions d'installation, consultez la documentation d'installation de Rclone.	AWS général, administrateur du cloud
Configurez Rclone.	Copiez le fichier `rclone.conf` d'exemple suivant. `AZStorage Account` Remplacez-le par le nom de votre compte Azure Storage et `us-east-1` par la région AWS dans laquelle se trouve votre compartiment S3. Enregistrez ce fichier à	AWS général, administrateur du cloud

Tâche	Description	Compétences requises

	l'emplacement `~/.config/rclone/rclone.conf` de votre EC2 instance.
	
	`[AZStorageAccount]`
	`type = azureblob`
	`account = AZStorage Account`
	`service_principal_f ile = azure-pri ncipal.json`
	
	`[s3]`
	`type = s3`
	`provider = AWS`
	`env_auth = true`
	`region = us-east-1`	

Tâche	Description	Compétences requises

Vérifiez la configuration de Rclone.	Pour vérifier que Rclone est configuré et que les autorisations fonctionnent correctement, vérifiez que Rclone peut analyser votre fichier de configuration et que les objets de votre conteneur Azure Blob et de votre compartiment S3 sont accessibles. Consultez les exemples de commandes de validation suivants.
	• Répertoriez les télécommandes configurées dans le fichier de configuration. Cela garantira que votre fichier de configuration est correctement analysé. Vérifiez le résultat pour vous assurer qu'il correspond à votre `rclone.conf` fichier.
	`rclone listremotes`
	• Répertoriez les conteneurs Azure Blob dans le compte configuré. `AZStorage Account` Remplacez-le par le nom du compte de stockage que vous avez utilisé dans le `rclone.conf` fichier.
	`AZStorageAccount:`
	`s3:`
		AWS général, administrateur du cloud

Tâche	Description	Compétences requises

	<pre>rclone lsd AZStorage Account:
	2020-04-29 08:29:26 docs</pre>
	• Répertoriez les fichiers dans le conteneur Azure Blob. Remplacez les documents de cette commande par un véritable nom de conteneur Blob dans votre compte de stockage Azure.
	<pre>rclone ls AZStorage Account:docs
	824884 administr ator-en.a4.pdf</pre>
	• Répertoriez les buckets de votre compte AWS.
	<pre>[root@ip-10-0-20-157 ~]# rclone lsd s3:
	2022-03-07 01:44:40 amzn-s3-demo-bucket1
	2022-03-07 01:45:16 amzn-s3-demo-bucket2
	2022-03-07 02:12:07 amzn-s3-demo-bucket3</pre>
	• Répertoriez les fichiers du compartiment S3.
	<pre>[root@ip-10-0-20-1 57 ~]# rclone ls</pre>	

Tâche	Description	Compétences requises

	`s3:amzn-s3-demo-bucket1`
	`template0.yaml`
	`template1.yaml`	

Migrer les données à l'aide de Rclone

Tâche	Description	Compétences requises

Migrez les données de vos conteneurs.	Exécutez la commande de copie ou de synchronisation Rclone.
	
	Exemple : copie
	
	Cette commande copie les données du conteneur Azure Blob source vers le compartiment S3 de destination.
	
	`rclone copy AZStorageAccount:blob-container s3:amzn-s3-demo-bucket1`
	
	Exemple : synchronisation
	
	Cette commande synchronise les données entre le conteneur Azure Blob source et le compartiment S3 de destination.
	
	`rclone sync AZStorageAccount:blob-conta`
		AWS général, administrateur du cloud

Tâche	Description	Compétences requises
	`iner s3:amzn-s3-demo-bucket1` **Important** Lorsque vous utilisez la commande de synchronisation, les données absentes du conteneur source sont supprimées du compartiment S3 de destination.	
Synchronisez vos conteneurs.	Une fois la copie initiale terminée, exécutez la commande Rclone sync pour poursuivre la migration afin que seuls les nouveaux fichiers manquants dans le compartiment S3 de destination soient copiés.	AWS général, administrateur du cloud
Vérifiez que les données ont bien été migrées.	Pour vérifier que les données ont bien été copiées dans le compartiment S3 de destination, exécutez les commandes Rclone lsd et ls.	AWS général, administrateur du cloud

Ressources connexes

- Guide de l'utilisateur Amazon S3 (documentation AWS)
- Rôles IAM pour Amazon EC2 (documentation AWS)
- Création d'un conteneur Microsoft Azure Blob (documentation Microsoft Azure)

- Commandes Rclone (documentation Rclone)

Informations supplémentaires

Exemple de politique de rôle pour les EC2 instances

Cette politique donne à votre EC2 instance un accès en lecture et en écriture à un compartiment spécifique de votre compte. Si votre compartiment utilise une clé gérée par le client pour le chiffrement côté serveur, la politique peut nécessiter un accès supplémentaire à AWS Key Management Service (AWS KMS).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:DeleteObject",
                "s3:GetObject",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
              "arn:aws:s3:::amzn-s3-demo-bucket/*",
              "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": "arn:aws:s3:::*"
        }
    ]
}
```

Création d'un principal de service Azure AD en lecture seule

Un principal de service Azure est une identité de sécurité utilisée par les applications, les services et les outils d'automatisation des clients pour accéder à des ressources Azure spécifiques. Considérez-le comme une identité d'utilisateur (identifiant et mot de passe ou certificat) dotée d'un rôle spécifique

et d'autorisations étroitement contrôlées pour accéder à vos ressources. Pour créer un principal de service en lecture seule afin de respecter les autorisations du moindre privilège et de protéger les données dans Azure contre les suppressions accidentelles, procédez comme suit :

1. Connectez-vous au portail de votre compte cloud Microsoft Azure et lancez Cloud Shell PowerShell ou utilisez l'interface de ligne de commande (CLI) Azure sur votre poste de travail.
2. Créez un principal de service et configurez-le avec un accès en lecture seule à votre compte de stockage Azure Blob. Enregistrez le résultat JSON de cette commande dans un fichier local appelé`azure-principal.json`. Le fichier sera chargé sur votre EC2 instance. Remplacez les variables d'espace réservé indiquées entre accolades ({et}) par votre ID d'abonnement Azure, le nom du groupe de ressources et le nom de votre compte de stockage.

```
az ad sp create-for-rbac `
--name AWS-Rclone-Reader `
--role "Storage Blob Data Reader" `
--scopes /subscriptions/{Subscription ID}/resourceGroups/{Resource Group Name}/
providers/Microsoft.Storage/storageAccounts/{Storage Account Name}
```

Migrer du serveur Couchbase vers Couchbase Capella sur AWS

Créée par Battulga Purevragchaa (AWS), Mark Gamble et Saurabh Shanbhag (AWS)

Récapitulatif

Couchbase Capella est une base de données NoSQL en tant que service (DBaaS) entièrement gérée pour les applications critiques (par exemple, les profils utilisateurs ou les catalogues en ligne et la gestion des stocks). Couchbase Capella gère votre charge de travail DBaa S dans un compte Amazon Web Services (AWS) géré par Couchbase. Capella facilite l'exécution et la gestion de la réplication sur plusieurs clusters, plusieurs (région AWS, multicloud et cloud hybride) au sein d'une seule interface.

Couchbase Capella vous aide à faire évoluer instantanément vos applications Couchbase Server, en vous aidant à créer des clusters multi-nœuds en quelques minutes. Couchbase Capella prend en charge toutes les fonctionnalités de Couchbase Server, notamment SQL++, la recherche en texte intégral, le service d'événements et le service d'analyse. Il élimine également le besoin de gérer les installations, les mises à niveau, les sauvegardes et la maintenance générale des bases de données.

Ce modèle décrit les étapes et les meilleures pratiques pour migrer un environnement de serveur Couchbase autogéré vers le cloud AWS. Le modèle fournit un processus reproductible pour migrer les données et les index des clusters Couchbase Server, exécutés sur site ou dans le cloud, vers Couchbase Capella. Ces étapes vous permettent d'éviter les problèmes lors de votre migration et d'accélérer l'ensemble de votre processus de migration.

Ce modèle propose les deux options de migration suivantes :

- L'option 1 est appropriée si vous avez moins de 50 index à migrer.
- L'option 2 est appropriée si vous avez plus de 50 index à migrer.

Vous pouvez également configurer des exemples de données sur votre serveur Couchbase autogéré afin de suivre le guide de migration.

Si vous choisissez l'option de migration 2, ou si vous utilisez des étendues ou des collections autres que la valeur par défaut, vous devez utiliser l'exemple de fichier de configuration, qui se trouve dans la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un compte payant Couchbase Capella existant. Vous pouvez également créer un compte Couchbase Capella sur AWS et utiliser l'essai gratuit de Couchbase Capella, puis passer à un compte payant pour configurer votre cluster en vue de la migration. Pour commencer avec la version d'essai, suivez les instructions de la section Getting Started with Couchbase Capella.
- Un environnement Couchbase Server autogéré existant sur site ou déployé chez un fournisseur de services cloud.
- Pour l'option de migration 2, Couchbase Shell et un fichier de configuration. Pour créer le fichier de configuration, vous pouvez utiliser le fichier d'exemple qui se trouve dans la section Informations supplémentaires.
- Connaissance de l'administration de Couchbase Server et de Couchbase Capella.
- Connaissance de l'ouverture de ports TCP et de l'exécution de commandes dans une interface de ligne de commande (CLI).

Le processus de migration nécessite également les rôles et l'expertise décrits dans le tableau suivant.

Rôle	Expertise	Responsabilités
Administrateur Couchbase	• Connaissance de Couchbase Server et de Couchbase Capella • Des connaissances de base en ligne de commande sont utiles mais ne sont pas obligatoires	• Tâches spécifiques à Couchbase Server et Capella
Administrateur système, administrateur informatique	• Connaissance de l'environnement et de l'administration autogérés du système Couchbase Server	• Ouverture de ports et détermination des adresses IP sur les nœuds de cluster Couchbase Server autogérés

Limites

- Ce modèle est utilisé pour migrer les données, les index et les index Couchbase Full Text Search depuis Couchbase Server vers Couchbase Capella sur AWS. Le modèle ne s'applique pas à la migration de Couchbase Eventing Service ou à Couchbase Analytics.
- Couchbase Capella est disponible dans plusieurs régions AWS. Pour up-to-date plus d'informations sur les régions prises en charge par Capella, consultez Amazon Web Services dans la documentation de Couchbase.

Versions du produit

- Édition Couchbase Server (Community ou Enterprise) version 5.x ou ultérieure

Architecture

Pile technologique source

- Serveur Couchbase

Pile technologique cible

- Canapé Capella

Architecture cible

1. Vous accédez à Couchbase Capella en utilisant le plan de contrôle Capella. Vous pouvez utiliser le plan de contrôle Capella pour effectuer les opérations suivantes :
   - Contrôlez et surveillez votre compte.
   - Gérez les clusters et les données, les index, les utilisateurs et les groupes, les autorisations d'accès, la surveillance et les événements.
2. Des clusters sont créés.
3. Le plan de données Capella se trouve dans le compte AWS géré par Couchbase. Après avoir créé un nouveau cluster, Couchbase Capella le déploie dans plusieurs zones de disponibilité de la région AWS sélectionnée.

4. Vous pouvez développer et déployer des applications Couchbase dans un VPC de votre compte AWS. Généralement, ce VPC accède au plan de données Capella via le peering VPC.

Outils

- Couchbase Cross Data Center Replication (XDCR) permet de répliquer les données entre des clusters situés dans différents fournisseurs de cloud et différents centres de données. Il est utilisé pour migrer des données vers Couchbase Capella à partir de clusters Couchbase Server autogérés.

> **Note**
>
> XDCR ne peut pas être utilisé avec Couchbase Server Community Edition pour migrer vers Couchbase Capella. Au lieu de cela, vous pouvez utiliser cbexport. Pour plus d'informations, consultez l'épique Migrate data from Community Edition.

- Couchbase Shell est un shell en ligne de commande permettant à Couchbase Server et Couchbase Capella d'accéder aux clusters Couchbase locaux et distants. Dans ce modèle, Couchbase Shell est utilisé pour migrer les index.
- cbexport est un utilitaire Couchbase permettant d'exporter des données depuis le cluster Couchbase. Inclus dans les outils CLI de Couchbase Server.

Épopées

Préparer la migration

Tâche	Description	Compétences requises
Évaluez la taille du cluster de serveurs Couchbase autogéré.	Connectez-vous à la console Web Couchbase pour Couchbase Server et évaluez les nœuds et les compartiments de votre cluster autogéré. 1. Pour afficher la liste des nœuds du cluster, cliquez	Administrateur Couchbase

Tâche	Description	Compétences requises
	sur l'onglet Serveurs dans la barre de navigation. 2. Enregistrez le nombre de nœuds, puis choisissez chaque nœud dans la liste pour afficher ses propriété s. 3. Enregistrez la mémoire et le stockage pour chaque nœud individuel. 4. Cliquez sur l'onglet Buckets dans la barre de navigatio n, puis sélectionnez chaque bucket dans la liste pour afficher ses propriétés. Enregistrez le quota de RAM et le paramètre de résolution des conflits pour chaque compartiment. Vous utiliserez les configura tions de votre cluster Couchbase Server autogéré comme guide général pour le dimensionnement et la configuration du cluster cible sur Couchbase Capella. Pour obtenir de l'aide concernant un exercice plus détaillé de dimensionnement de Couchbase Capella, contactez Couchbase.	

Tâche	Description	Compétences requises
Enregistrez la distribut ion du service Couchbase sur le cluster de serveurs Couchbase autogéré.	1. Sur la console Web de Couchbase, choisisse z l'onglet Serveurs pour afficher la liste des nœuds du cluster. 2. Choisissez chaque nœud pour afficher ses propriétés, puis enregistrez la distribut ion du service Couchbase pour chaque nœud (service de données, service de requête, service d'index, service de recherche, service d'analyse et service d'événements).	Administrateur Couchbase
Enregistrez les adresses IP des nœuds du cluster Couchbase Server autogérés.	(Ignorez cette étape si vous utilisez Community Edition.) Enregistrez l'adresse IP de chaque nœud de votre cluster. Ils seront ajoutés ultérieurement à la liste des autorisations de votre cluster Couchbase Capella.	Administrateur Couchbase, administrateur système

Déployez et configurez des ressources sur Couchbase Capella

Tâche	Description	Compétences requises
Choisir un modèle.	1. Connectez-vous à votre plan de contrôle Couchbase Capella, choisissez l'onglet Tableau de bord ou l'onglet Clusters dans la navigation	Administrateur Couchbase

Tâche	Description	Compétences requises
	principale, puis choisissez Create Cluster. 2. À l'aide des informations que vous avez enregistr ées lors de l'évaluation de votre cluster Couchbase Server autogéré, choisisse z le modèle de cluster qui répond aux exigences de la configuration. Si vous ne trouvez pas de modèle approprié, choisisse z Modèle personnalisé dans l'éditeur de dimension nement des clusters.	

Tâche	Description	Compétences requises
Choisissez et configurez les nœuds.	Choisissez et configurez les nœuds en fonction de votre environnement de cluster Couchbase Server autogéré, notamment en ce qui concerne le nombre de nœuds, la distribution des services, le calcul ou la RAM et le stockage. Couchbase Capella utilise les meilleures pratiques de mise à l'échelle multidimensionnelle. Les services et les nœuds ne peuvent être choisis qu'en fonction des meilleures pratiques de déploiement. Cela peut signifier que vous ne pouvez pas correspondre exactement aux configurations de votre cluster Couchbase Server autogéré.	Administrateur Couchbase

Tâche	Description	Compétences requises
Déployez le cluster.	Choisissez une zone de support et un package de support, puis déployez le cluster. Pour obtenir des instructions et des étapes détaillées, consultez la section Création d'un cluster dans la documentation de Couchbase. **Important** Si vous utilisez l'essai gratuit de Couchbase Capella, vous devez le convertir en compte payant avant de commencer votre migration. Pour convertir votre compte, ouvrez la section Facturation du plan de contrôle Couchbase Capella, puis choisisse z Ajouter un identifia nt d'activation. L'identif iant d'activation est envoyé à votre adresse e-mail de contact de facturati on une fois que vous avez conclu un contrat d'achat avec Couchbase Sales ou après avoir effectué	Administrateur Couchbase

Tâche	Description	Compétences requises
	un achat via AWS Marketplace.	

Tâche	Description	Compétences requises
Créez un utilisateur d'identification de base de données.	Un utilisateur d'identification de base de données est spécifique à un cluster et comprend un nom d'utilisateur, un mot de passe et un ensemble de privilèges de compartiment. Cet utilisateur est requis pour créer des compartiments et accéder aux données des compartiments. Dans le plan de contrôle Couchbase Capella, créez un identifiant de base de données pour le nouveau cluster en suivant les instructions de la section Configurer les informations d'identification de base de données dans la documentation Couchbase Capella. **Note** Les utilisateurs d'une organisation ont besoin que les informations d'identification relatives au rôle organisationnel leur soient attribuées pour accéder aux données des compartiments d'un cluster en particulier,	Administrateur Couchbase

Tâche	Description	Compétences requises
	soit à distance, soit via l'interface utilisateur de Couchbase Capella. Cela est distinct des informations d'identification de base de données, qui sont généralement utilisées par les applications et les intégrations. La création de l'utilisateur organisationnel vous permet de créer et de gérer les buckets cibles sur votre cluster Couchbase Capella.	

Tâche	Description	Compétences requises
Si vous utilisez l'option de migration 2, installez Couchbase Shell.	Vous pouvez installer Couchbase Shell sur n'importe quel système disposant d'un accès réseau à la fois à votre serveur Couchbase autogéré et aux clusters Couchbase Capella. Pour plus d'informations, consultez Installer Couchbase Shell version 1.0.0-beta.5 dans la documentation de Couchbase Shell. Vérifiez que Couchbase Shell est installé en testant une connexion à votre cluster autogéré dans un terminal de ligne de commande.	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
Autoriser les adresses IP.	1. Dans le plan de contrôle Couchbase Capella, choisissez Clusters, puis choisissez votre cluster cible. 2. Choisissez l'onglet Connect pour le cluster et enregistrez le point de terminaison de connexion de votre cluster qui est répertorié sous Gérer les adresses IP autorisées. 3. Pour ajouter l'adresse IP du système sur lequel vous avez installé Couchbase Shell et l'adresse IP de vos instances de cluster Couchbase Server autogérées en tant qu'adresses IP autorisées, procédez comme suit : a. Sous Réseau étendu, choisissez Gérer les adresses IP autorisées. b. Choisissez Ajouter une adresse IP autorisée, entrez l'adresse IP du système sur lequel vous avez installé Couchbase Shell, puis choisissez Ajouter une adresse IP. c. Répétez l'étape précédente pour ajouter	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
	l'adresse IP de votre instance de cluster Couchbase Server autogérée. Pour plus d'informations sur les adresses IP autorisées, consultez Configurer les adresses IP autorisées dans la documentation de Couchbase.	

Tâche	Description	Compétences requises
Configurez les certificats.	1. Pour télécharger le certificat racine de votre cluster, sous Certificat racine, choisissez Télécharger. 2. Enregistrez le certificat racine à l'aide de l'extension de fichier .pem dans un dossier du système qui exécutera Couchbase Shell. 3. Ensuite, connectez-vous à votre console Web Couchbase Server autogérée, choisissez Sécurité dans la barre de navigation de gauche, puis choisissez l'onglet Certificats. 4. Copiez le certificat racine de votre cluster Couchbase Server autogéré et enregistrez-le sous forme de fichier .pem dans le dossier où vous avez enregistré le fichier de certificat racine de votre cluster Couchbase Capella. Pour plus d'informations sur le certificat racine, consultez la section Certificat racine dans la documentation du serveur Couchbase.	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
Créez le fichier de configuration pour Couchbase Shell.	Créez un fichier point de configuration dans le répertoire personnel de l'installation de Couchbase Shell (par exemple,). `/<HOME_DIRECTORY>/.cbsh/config` Pour plus d'informations, consultez Config dotfiles dans la documentation de Couchbase. Ajoutez les propriétés de connexion pour les clusters source et cible au fichier de configuration. Vous pouvez utiliser l'exemple de fichier de configuration qui se trouve dans la section Informations supplémentaires et modifier les paramètres de vos clusters. Enregistrez le fichier de configuration avec les paramètres mis à jour `.cbsh` dans le dossier (par exemple,`/<HOME_DIRECTORY>/.cbsh/config`).	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
Créez des compartiments cibles.	Pour chaque bucket source, créez un bucket cible dans votre cluster Couchbase Capella en suivant les instructions de la section Créer un bucket dans la documentation Couchbase. Les configurations de vos compartiments cibles doivent correspondre aux noms des compartiments, aux paramètres de mémoire et aux paramètres de résolution des conflits des compartiments de votre cluster Couchbase Server autogéré.	Administrateur Couchbase

Tâche	Description	Compétences requises

Créez des étendues et des collections.	Chaque compartiment contient une étendue et une collection par défaut avec le keyspace. `_default._default` Si vous utilisez d'autres espaces clés pour votre portée et votre collection, vous devez créer des espaces clés identiques dans le cluster Capella cible.
	1. Ouvrez le terminal de ligne de commande sur le système sur lequel vous avez installé Couchbase Shell.
	2. Pour démarrer Couchbase Shell, exécutez la commande suivante.
	`./cbsh`
	3. Pour chaque compartiment que vous souhaitez migrer, créez des étendues et des collections dans le cluster Capella en exécutant les commandes suivantes . Assurez-vous de le remplacer <BUCKET_NAME>par le nom du compartiment que vous souhaitez migrer.
	`scopes --clusters "On-Prem-Cluster" --bucket`
		Administrateur Couchbase

Tâche	Description	Compétences requises
	<BUCKET_NAME> | select scope | where scope != "_default" | each { |it| scopes create $it.scope --clusters "Capella-Cluster" } collections --clusters "On-Prem-Cluster" --bucket <BUCKET_NAME> | select scope collection | where $it.scope != "_default" | where $it.collection != "_default" | each { |it| collections create $it.collection --clusters "Capella-Cluster" --bucket <BUCKET_NAME> --scope $it.scope }	

Migrer les données depuis Enterprise Edition

Tâche	Description	Compétences requises
Ouvrez les ports TCP sur les nœuds du cluster Couchbase Server autogérés.	Assurez-vous que les ports appropriés sont ouverts pour la communication XDCR sur les nœuds du cluster Couchbase Server autogéré. Pour plus d'informations, consultez la documentation sur les ports du serveur Couchbase.	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
Si vous utilisez Couchbase Server Enterprise Edition, configurez Couchbase XDCR.	1. Dans la navigation principale du plan de contrôle Couchbase Capella, choisissez Clusters, puis choisissez le cluster cible pour la migration. 2. Sous Certificat racine, choisissez Copier. 3. Connectez-vous à votre console Web Couchbase Server autogérée et, dans la navigation principale, choisissez XDCR. Choisissez ensuite Ajouter une télécommande. 4. Définissez les paramètres suivants : • Nom du cluster : nom de la connexion au cluster Capella • IP/nom d'hôte — Le point de connexion pour votre cluster Couchbase Capella • Nom d'utilisateur pour le cluster distant — L'utilisateur de base de données pour votre cluster Couchbase Capella • Mot de passe — Le mot de passe utilisateur de la base de données pour	Administrateur Couchbase

Tâche	Description	Compétences requises
	votre cluster Couchbase Capella • Activer la connexion sécurisée : sélectionné • Complet (mot de passe et données chiffrés TLS) — Sélectionné 5. Collez le certificat racine du cluster Capella que vous avez copié précédemment, puis choisissez Enregistrer.	

Tâche	Description	Compétences requises
Démarrez Couchbase XDCR.	1. Dans votre console Web Couchbase Server autogérée, choisissez XDCR dans la navigation principale, puis choisissez Ajouter une réplication. 2. Définissez les paramètres suivants : • Répliquer depuis un compartiment : sélectionnez le compartiment source pour la migration. • Compartiment distant : entrez le nom du compartiment cible. • Cluster distant : sélectionnez le cluster cible que vous avez créé précédemment. 3. Choisissez Enregistrer la réplication. Le processus de réplication devrait commencer dans quelques secondes.	Administrateur Couchbase

Migrez les index à l'aide de l'option 1

Tâche	Description	Compétences requises
Migrez les index de clusters autogérés vers Couchbase Capella.	⚠ Important Nous recommandons cette procédure si	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
	vous avez moins de 50 index à migrer. Si vous avez plus de 50 index à migrer, nous vous recommandons d'utiliser l'option de migration 2. 1. Sur la console Web de Couchbase, choisissez Indexes. 2. Dans la liste des index, choisissez le premier index que vous souhaitez migrer. La définition de l'index est ensuite affichée. 3. Copiez la définition de l'index à l'aide de l'`CREATE`instruction, mais ne la copiez pas`WITH { "defer_build":true }` . Par exemple, à partir de l'exemple de définition d'index suivant, vous ne devez copier que`CREATE INDEX `cityindex` ON `travel-sample`(`city`)` . `CREATE INDEX `cityindex` ON `travel-sample`(`city`)`	

Tâche	Description	Compétences requises
	WITH { "defer_bu ild":true } 4. Dans le plan de contrôle Couchbase Capella, choisissez Clusters, puis choisissez le cluster cible. 5. Dans la liste déroulant e Outils, sélectionnez Query Workbench. Collez l'CREATEinstruction que vous avez copiée précédemment dans l'éditeur de requête, puis choisissez Execute. Cela crée et construit l'index. 6. Pour confirmer la création de l'index, choisissez Index dans la liste déroulant e Outils. La liste indique que l'index a été créé et construit. 7. Répétez ce processus pour chaque index qui doit être migré.	

Migrez les index à l'aide de l'option 2

Tâche	Description	Compétences requises
Migrez les définitions d'index.	⚠ Important Nous recommand ons cette procédure	Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises

	si vous avez plus de 50 index à migrer. Si vous avez moins de 50 index à migrer, nous vous recommandons d'utiliser l'option de migration 1.
	
	1. Ouvrez le terminal de ligne de commande sur le système sur lequel vous avez installé Couchbase Shell.
	2. Pour démarrer Couchbase Shell, exécutez la commande suivante.
	
	`./cbsh`
	
	3. Pour vous connecter au cluster Couchbase Server autogéré, exécutez la commande suivante.
	
	`cb-env cluster On-Prem-Cluster`
	
	4. Pour migrer les définitions d'index du cluster Couchbase Server autogéré vers le cluster Couchbase Capella, exécutez la commande suivante pour chaque bucket que vous souhaitez migrer. Assurez-	

Tâche	Description	Compétences requises
	vous de le <BUCKET_NAME> remplacer par le nom du bucket correspondant aux index que vous souhaitez migrer. Cette option de migration nécessite que les noms de vos compartiments cibles soient identiques à ceux des compartiments source. `query indexes --definitions | where bucket =~ <BUCKET_NAME>| get definition | each { |it| query $it --clusters Capella-Cluster }`	

Tâche	Description	Compétences requises

Créez les définitions d'index.	1. Pour passer du contexte au cluster Couchbase Capella, exécutez la commande suivante :
	`cb-env cluster Capella-Cluster`
	2. Pour créer les définitions d'index qui ont été migrées vers le cluster Couchbase Capella, exécutez la commande suivante, en les <BUCKET_NAME> remplaçant par le nom du bucket correspondant aux index que vous souhaitez créer.
	`query 'SELECT RAW CONCAT("BUILD INDEX ON ", k , "(['", CONCAT2 ("','", inames), "']);") FROM system:indexes AS s LET bid = CONCAT("` ",s.bucket_id, "`"), sid = CONCAT("`", s.scope_id, "`"), kid = CONCAT("` ", s.keyspace_id, "`"), k = NVL2(bid, CONCAT2(".", bid, sid, kid), kid) WHERE s.namespa ce_id = "default" AND s.bucket_id = "" GROUP BY k LETTING`
		Administrateur Couchbase, administrateur système

Tâche	Description	Compétences requises
	inames = ARRAY_AGG (s.name) FILTER (WHERE s.state = 'deferred') HAVING ARRAY_LENGTH(iname s) > 0;' | each { | it| query $it } 3. Répétez l'opération pour chaque seau.	

Migrer les index de recherche en texte intégral

Tâche	Description	Compétences requises
Migrez les index de recherche en texte intégral des clusters autogérés vers Couchbase Capella.	1. Dans la console Web de Couchbase, choisissez Rechercher. 2. Dans la liste des index de recherche en texte intégral (FTS), choisissez le premier index FTS que vous souhaitez migrer, choisissez Afficher la définition d'index JSON, puis Copier dans le presse-papiers. Notez le nom de l'index et le bucket auquel il appartient. 3. Dans le plan de contrôle Couchbase Capella, choisissez Clusters, puis choisissez le cluster cible. 4. Dans la liste déroulant e Outils, sélectionnez	Administrateur Couchbase

Tâche	Description	Compétences requises
	Recherche en texte intégral. 5. Choisissez Importer un index, puis collez la définitio n de l'index FTS. 6. Entrez le nom de l'index, sélectionnez le compartim ent approprié, comme indiqué sur le cluster autogéré, puis choisissez Create. 7. Répétez ce processus pour chaque index FTS qui doit être migré.	

Migrer les données depuis Couchbase Community Edition

Tâche	Description	Compétences requises
Exportez des données depuis l'édition communautaire autogérée de Couchbase Server.	Le XDCR crypté n'est pas disponible dans Couchbase Community Edition. Vous pouvez exporter des données depuis Couchbase Community Edition, puis les importer manuellement dans Couchbase Capella. Pour exporter des données depuis le compartiment source, utilisez `cbexport` la ligne de commande.	Administrateur Couchbase

Tâche	Description	Compétences requises
	La commande suivante est fournie à titre d'exemple. `cbexport json \ --cluster localhost \ --bucket <SOURCE BUCKET NAME> \ --format lines \ --username <USERNAME> \ --password <PASSWORD> \ --include-key cbkey \ --scope-field cbscope \ --collection-field cbcoll \ --output cbexported_data.json` Notez que `cbkey`, `cbscope` et `cbcoll` sont des libellés arbitraires. Ils seront référencés plus tard dans le processus, donc si vous choisissez de les nommer différemment, prenez-en note.	

Tâche	Description	Compétences requises
Importez des données dans Couchbase Capella.	1. Dans le plan de contrôle Couchbase Capella, choisissez Clusters, puis choisissez le cluster cible. 2. Dans la liste déroulant e Outils, sélectionnez Importer. Cela ouvrira un assistant avec les six étapes suivantes : a. Bucket — Choisissez le bucket cible. b. Fichier — Choisisse z JSON, choisissez Lignes, puis choisissez Utiliser votre navigateu r Web. Si vous disposez d'une grande quantité de données, vous pouvez explorer l'option Manuellement. Sélection nez le fichier créé par `cbexport`. c. Collections — Choisissez un mappage de collectio n personnalisé. Si votre base de données Community Edition n'utilise ni étendues ni collectio ns, ou si elle utilise uniquement _default, vous pouvez plutôt choisir l'option Sélection	Administrateur Couchbase

Tâche	Description	Compétences requises
	ner une collection unique. Pour Collection Mapping Expressio n, entrez`%cbscope %.%cbcoll%` . Pour vérifier que cette expression fonctionn e correctement, vous pouvez coller des exemples de données, tels que les suivants. `{ "cbscope" :"inventory", "cbcoll":"landmark ", "cbkey":" landmark_3991" }` d. Clé — Choisissez Customer Generatio n. (Si la préservation des clés des données que vous importez ne vous intéresse pas, vous pouvez plutôt sélection ner l'UUID généré automatiquement et passer à l'étape 5.) Pour Key Name Generator Expression, entrez %cbkey%. Pour vérifier que cette expression fonctionne correctem	

Tâche	Description	Compétences requises
	ent, collez quelques exemples de données. e. Configurations — Choisissez Ignorer les champs, puis saisissez cbscope, cbcoll, cbkey. Ces champs contiennent des informations transitoires qui ne doivent pas nécessairement se trouver dans le compartiment cible après une importation. Conservez les valeurs par défaut des autres paramètres. f. Importer — Vérifiez et choisissez Importer lorsque vous êtes prêt. Attendez le téléchargement et l'importation des données. Pour les fichiers volumineux, Couchbase Capella prend en charge l'importation en ligne de commande à l'aide de cURL. Vous pouvez explorer les options d'importation plus en détail dans la section Importer des données dans la documentation de Couchbase Capella.	

Tester et vérifier la migration

Tâche	Description	Compétences requises
Vérifiez la migration des données.	1. Dans le plan de contrôle Couchbase Capella, choisissez Clusters, puis choisissez le cluster cible dans votre liste de clusters. 2. Choisissez l'onglet Buckets pour votre cluster cible. Vérifiez que le nombre d'éléments (document s) dans le compartim ent cible correspond au nombre d'éléments dans le compartiment source. 3. Dans le cluster cible, dans la liste déroulante Outils, sélectionnez Documents . Vérifiez que tous les documents ont été migrés. 4. (Facultatif) Une fois toutes les données migrées, vous pouvez arrêter la réplication en les suppriman t. Pour plus d'informa tions, consultez Supprimer une réplication dans la documentation de Couchbase.	Administrateur Couchbase
Vérifiez la migration de l'index.	Dans le plan de contrôle Couchbase Capella, dans la liste déroulante Outils de votre cluster cible, choisissez	Administrateur Couchbase

Tâche	Description	Compétences requises
	Indexes. Vérifiez que les index sont migrés et créés.	
Vérifiez les résultats de la requête.	1. Dans le plan de contrôle Couchbase Capella, dans la liste déroulante Outils de votre cluster cible, choisissez Query Workbench. 2. Exécutez un exemple de requête N1QL ou une requête utilisée dans votre application. Assurez-vous de recevoir les mêmes résultats que lorsque vous exécutez la requête dans votre cluster Couchbase Server autogéré.	Administrateur Couchbase
Vérifiez les résultats de recherche en texte intégral (applicable si vous avez migré des index FTS).	1. Dans le plan de contrôle Couchbase Capella, dans la liste déroulante Outils de votre cluster cible, choisissez Recherche en texte intégral. 2. Sélectionnez un index FTS en choisissant son nom. 3. Choisissez Rechercher. 4. Entrez un exemple de requête de recherche, puis choisissez Rechercher. 5. Vérifiez que les résultats sont les mêmes que lorsque vous lancez la recherche sur votre cluster autogéré.	Administrateur Couchbase

Ressources connexes

Préparer la migration

- Commencez avec l'essai gratuit de Couchbase Capella
- Exigences relatives aux fournisseurs de cloud pour Couchbase Capella
- Directives relatives aux tailles de Couchbase Capella

Migrer les données et les index

- Canapé XDCR
- Documentation de Couchbase Shell

Couchbase SLAs Capella et assistance

- Contrats de niveau de service Couchbase Capella () SLAs
- Politique de support du service Couchbase Capella

Informations supplémentaires

Le code suivant est un exemple de fichier de configuration pour Couchbase Shell.

```
Version = 1

[[clusters]]
identifier = "On-Prem-Cluster"
hostnames = ["<SELF_MANAGED_COUCHBASE_CLUSTER>"]
default-bucket = "travel-sample"
username = "<SELF_MANAGED_ADMIN>"
password = "<SELF_MANAGED_ADMIN_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"

[[clusters]]
identifier = "Capella-Cluster"
hostnames = ["<COUCHBASE_CAPELLA_ENDPOINT>"]
default-bucket = "travel-sample"
username = "<CAPELLA_DATABASE_USER>"
```

```
password = "<CAPELLA_DATABASE_USER_PWD>"
tls-cert-path = "/<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>"
data-timeout = "2500ms"
connect-timeout = "7500ms"
query-timeout = "75s"
```

Avant d'enregistrer le fichier de configuration, utilisez le tableau suivant pour vous assurer que vous avez ajouté vos propres informations de cluster source et cible.

<SELF_MANAGED_COUCHBASE_CLUSTER>	Utilisez l'adresse IP de votre cluster Couchbase Server autogéré.
<SELF_MANAGED_ADMIN>	Utilisez l'utilisateur administrateur pour votre cluster Couchbase Server autogéré.
<ABSOLUTE_PATH_TO_SELF_MANAGED_ROOT_CERT>	Utilisez le chemin absolu vers le fichier de certificat racine enregistré pour votre cluster Couchbase Server autogéré.
<COUCHBASE_CAPELLA_ENDPOINT>	Utilisez le point de connexion de votre cluster Couchbase Capella.
<CAPELLA_DATABASE_USER>	Utilisez l'utilisateur de base de données pour votre cluster Couchbase Capella.
<CAPELLA_DATABASE_USER_PWD>	Utilisez le mot de passe utilisateur de la base de données pour votre cluster Couchbase Capella.
<ABSOLUTE_PATH_TO_COUCHBASE_CAPELLA_ROOT_CERT>	Utilisez le chemin absolu vers le fichier de certificat racine enregistré pour votre cluster Couchbase Capella.

Migrer d'un serveur WebSphere d'applications IBM vers Apache Tomcat sur Amazon EC2

Créée par Neal Ardeljan (AWS) et Afroz Khan (AWS)

Récapitulatif

Ce modèle explique les étapes de migration d'un système Red Hat Enterprise Linux (RHEL) 6.9 ou version ultérieure sur site exécutant IBM WebSphere Application Server (WAS) vers RHEL 8 exécutant Apache Tomcat sur une instance Amazon Elastic Compute Cloud (Amazon). EC2

Le modèle peut être appliqué aux versions source et cible suivantes :

- WebSphere Serveur d'applications 7.x vers Apache Tomcat 8 (avec Java 7 ou version ultérieure)
- WebSphere Serveur d'applications 8.x vers Apache Tomcat 8 (avec Java 7 ou version ultérieure)
- WebSphere Serveur d'applications 8.5.5.x vers Apache Tomcat 9 (avec Java 8 ou version ultérieure)
- WebSphere Serveur d'applications 8.5.5.x vers Apache Tomcat 10 (avec Java 8 ou version ultérieure)

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Code Java source, avec les hypothèses suivantes :
  - Utilise la version Java Development Kit (JDK) de Java 7 ou version ultérieure
  - Utilise le framework Spring ou Apache Struts
  - N'utilise pas le framework Enterprise Java Beans (EJB) ni aucune autre fonctionnalité de WebSphere serveur qui n'est pas facilement disponible pour Tomcat
  - Utilise principalement des servlets ou des pages de serveur Java () JSPs
  - Utilise les connecteurs Java Database Connectivity (JDBC) pour se connecter aux bases de données
- Source : IBM WebSphere Application Server version 7.x ou ultérieure
- Target Apache Tomcat version 8.5 ou supérieure

Architecture

Pile technologique source

- Une application Web créée à l'aide du framework Apache Struts Model-View-Controller (MVC)
- Une application Web exécutée sur IBM WebSphere Application Server version 7.x ou 8.x
- Application Web qui utilise un connecteur LDAP (Lightweight Directory Access Protocol) pour se connecter à un annuaire LDAP (iPlanet/eTrust)
- Une application qui utilise la connectivité IBM Tivoli Access Manager (TAM) pour mettre à jour le mot de passe utilisateur TAM (dans l'implémentation actuelle, les applications utilisent PD.jar)

Bases de données sur site

- Oracle Database 21c (21.0.0.0)
- Oracle Database 19c (19.0.0.0)
- Oracle Database 12c version 2 (12.2.0.1)
- Oracle Database 12c version 1 (12.1.0.2)

Pile technologique cible

- Apache Tomcat version 8 (ou version ultérieure) exécuté sur RHEL sur une instance EC2
- Amazon Relational Database Service (Amazon RDS) pour Oracle

Pour plus d'informations sur les versions d'Oracle prises en charge par Amazon RDS, consultez le site Web Amazon RDS for Oracle.

Architecture cible

Outils

- Niveau d'application : reconstruction de l'application Java dans un fichier WAR.
- Niveau de base de données : sauvegarde et restauration natives d'Oracle.
- Outil de migration Apache Tomcat pour Jakarta EE. Cet outil utilise une application Web écrite pour Java EE 8 qui s'exécute sur Apache Tomcat 9 et la convertit automatiquement pour qu'elle s'exécute sur Apache Tomcat 10, qui implémente Jakarta EE 9.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Terminez la découverte des applications, l'empreinte de l'état actuel et les performan ces de référence.		BA, responsable de la migration
Validez les versions de base de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l' EC2 instance de serveur cible.		DBA, SysAdmin
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, SysAdmin
Choisissez le type d' EC2 instance approprié en fonction de la capacité, des fonctionn alités de stockage et des fonctionnalités réseau.		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, SysAdmin
Identifiez la stratégie et les outils de migration des applications.		DBA, responsable de la migration

Tâche	Description	Compétences requises
Complétez le guide de conception et de migration de l'application.		Responsable de la création, responsable de la migration
Terminez le runbook de migration des applications.		Responsable du développement, responsable du transfert, responsable des tests, responsable de la migration

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)		SysAdmin
Créez les groupes de sécurité.		SysAdmin
Configurez et démarrez Amazon RDS pour Oracle.		DBA, SysAdmin

Migrer les données

Tâche	Description	Compétences requises
Créez ou obtenez l'accès aux points de terminaison pour récupérer les fichiers de sauvegarde de la base de données.		DBA
Utilisez le moteur de base de données natif ou un outil tiers pour migrer les objets et les données de base de données.	Pour plus de détails, consultez la section « Migration des objets et des données de base	DBA

Tâche	Description	Compétences requises
	de données » dans la section Informations supplémentaires.	

Migrer l'application

Tâche	Description	Compétences requises
Déposez la demande de modification (CR) pour la migration.		Plomb de découpe
Obtenez l'approbation du CR pour la migration.		Plomb de découpe
Suivez la stratégie de migration des applications décrite dans le runbook de migration des applications.	Pour plus de détails, reportez-vous à la section « Configuration du niveau d'application » dans la section Informations supplémentaires.	DBA, ingénieur en migration, propriétaire de l'application
Mettez à niveau l'application (si nécessaire).		DBA, ingénieur en migration, propriétaire de l'application
Effectuez les tests fonctionnels, non fonctionnels, de validation des données, de SLA et de performance.		Responsable des tests, propriétaire de l'application, utilisateurs de l'application

Découper

Tâche	Description	Compétences requises
Obtenez l'approbation du propriétaire de l'application ou du propriétaire de l'entreprise.		Plomb de découpe

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, ingénieur en migration, propriétaire de l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, ingénieur en migration, SysAdmin
Passez en revue et validez les documents du projet.		Responsable de la migration
Collectez des indicateurs tels que le temps de migration , le pourcentage de tâches manuelles par rapport aux tâches automatisées et les économies de coûts.		Responsable de la migration
Clôturez le projet et faites part de vos commentaires.		Responsable de la migration, propriétaire de l'application

Ressources connexes

Références

- Documentation d'Apache Tomcat 10.0
- Documentation d'Apache Tomcat 9.0
- Documentation d'Apache Tomcat 8.0
- Guide d'installation d'Apache Tomcat 8.0
- Documentation JNDI d'Apache Tomcat
- Site Web Amazon RDS for Oracle

- Tarification d'Amazon RDS
- Oracle et Amazon Web Services
- Oracle sur Amazon RDS
- Déploiements multi-AZ d'Amazon RDS

Tutoriels et vidéos

- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)

Informations supplémentaires

Migration d'objets et de données de base de données

Par exemple, si vous utilisez les utilitaires de sauvegarde/restauration natifs d'Oracle :

1. Créez la sauvegarde Amazon Simple Storage Service (Amazon S3) pour les fichiers de sauvegarde de base de données (facultatif).
2. Sauvegardez les données Oracle DB dans le dossier partagé du réseau.
3. Connectez-vous au serveur de préparation de la migration pour mapper le dossier de partage réseau.
4. Copiez les données du dossier de partage réseau vers le compartiment S3.
5. Demandez un déploiement Amazon RDS Multi-AZ pour Oracle.
6. Restaurez la sauvegarde de base de données sur site sur Amazon RDS for Oracle.

Configuration du niveau d'application

1. Installez Tomcat 8 (ou 9/10) depuis le site Web d'Apache Tomcat.
2. Package de l'application et des bibliothèques partagées dans un fichier WAR.
3. Déployez le fichier WAR dans Tomcat.
4. Surveillez le journal de démarrage pour détecter `Linux cat` toutes les bibliothèques partagées manquantes à partir de WebSphere.
5. Regardez l'enregistrement de démarrage de `Linux cat` toute extension de descripteur de déploiement WebSphere spécifique.
6. Collectez toutes les bibliothèques Java dépendantes manquantes sur le WebSphere serveur.

7. Modifiez les éléments WebSphere du descripteur de déploiement spécifiques avec des équivalents compatibles avec Tomcat.
8. Reconstruisez le fichier WAR avec les bibliothèques Java dépendantes et les descripteurs de déploiement mis à jour.
9. Mettez à jour la configuration LDAP, la configuration de la base de données et testez les connexions (consultez le manuel de configuration du domaine et le mode d'emploi de la source de données JNDI dans la documentation d'Apache Tomcat).
10. Testez l'application installée par rapport à la base de données Amazon RDS for Oracle restaurée.
11. Créez une Amazon Machine Image (AMI) pour Linux à partir de l' EC2 instance.
12. Lancez l'architecture complète avec le groupe Application Load Balancer et Auto Scaling.
13. Mettez à jour le URLs (en utilisant la jonction WebSEAL) pour qu'il pointe vers l'Application Load Balancer.
14. Mettez à jour la base de données de gestion de configuration (CMDB).

Migrez d'IBM WebSphere Application Server vers Apache Tomcat sur Amazon EC2 avec Auto Scaling

Créée par Kevin Yung (AWS) et Afroz Khan (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une application Java d'IBM WebSphere Application Server vers Apache Tomcat sur une instance Amazon Elastic Compute Cloud EC2 (Amazon) avec Amazon EC2 Auto Scaling activé.

En utilisant ce modèle, vous pouvez obtenir :

- Réduction des coûts de licence IBM
- Haute disponibilité grâce au déploiement multi-AZ
- Résilience des applications améliorée avec Amazon EC2 Auto Scaling

Conditions préalables et limitations

Prérequis

- Applications Java (version 7). x ou 8. x) doit être développé dans des piles LAMP.
- L'état cible est d'héberger des applications Java sur des hôtes Linux. Ce modèle a été implémenté avec succès dans un environnement Red Hat Enterprise Linux (RHEL) 7. D'autres distributions Linux peuvent suivre ce modèle, mais la configuration de la distribution Apache Tomcat doit être référencée.
- Vous devez comprendre les dépendances de l'application Java.
- Vous devez avoir accès au code source de l'application Java pour apporter des modifications.

Limitations et modifications apportées à la replateforme

- Vous devez comprendre les composants d'archivage d'entreprise (EAR) et vérifier que toutes les bibliothèques sont regroupées dans les fichiers WAR des composants Web. Vous devez configurer le plug-in Apache Maven WAR et produire des artefacts de fichiers WAR.
- Lors de l'utilisation d'Apache Tomcat 8, il existe un conflit connu entre le fichier servlet-api.jar et les fichiers jar intégrés au package de l'application. Pour résoudre ce problème, supprimez le fichier servlet-api.jar du package de l'application.

- Vous devez configurer WEB-INF/Resources situé dans le chemin de classe de la configuration d'Apache Tomcat. Par défaut, les bibliothèques JAR ne sont pas chargées dans le répertoire. Vous pouvez également déployer toutes les ressources ci-dessous src/main/resources.
- Vérifiez la présence de racines de contexte codées en dur dans l'application Java et mettez à jour la nouvelle racine de contexte d'Apache Tomcat.
- Pour définir les options d'exécution de la JVM, vous pouvez créer le fichier de configuration setenv.sh dans le dossier bin d'Apache Tomcat ; par exemple, JAVA_OPTS, JAVA_HOME, etc.
- L'authentification est configurée au niveau du conteneur et est configurée en tant que domaine dans les configurations Apache Tomcat. L'authentification est établie pour l'un des trois domaines suivants :
  - Le domaine de base de données JDBC recherche les utilisateurs dans une base de données relationnelle accessible par le pilote JDBC.
  - DataSource Database Realm recherche les utilisateurs dans une base de données à laquelle JNDI accède.
  - Le domaine du répertoire JNDI recherche les utilisateurs dans le répertoire LDAP (Lightweight Directory Access Protocol) auquel le fournisseur JNDI accède. Les recherches nécessitent :
    - Détails de la connexion LDAP : base de recherche utilisateur, filtre de recherche, base de rôles, filtre de rôles
    - Le domaine clé du répertoire JNDI : se connecte au LDAP, authentifie les utilisateurs et récupère tous les groupes dont un utilisateur est membre
- Autorisation : dans le cas d'un conteneur doté d'une autorisation basée sur les rôles qui vérifie les contraintes d'autorisation dans le fichier web.xml, les ressources Web doivent être définies et comparées aux rôles définis dans les contraintes. Si LDAP ne dispose pas de mappage des rôles de groupe, vous devez définir l'attribut < security-role-ref > dans le fichier web.xml pour réaliser le mappage des rôles de groupe. Pour voir un exemple de document de configuration, consultez la documentation Oracle.
- Connexion à la base de données : créez une définition de ressource dans Apache Tomcat avec une URL de point de terminaison Amazon Relational Database Service (Amazon RDS) et les détails de connexion. Mettez à jour le code de l'application pour qu'il fasse référence à un en DataSource utilisant la recherche JNDI. Une connexion à la base de données existante définie dans ne WebSphere fonctionnerait pas, car elle utilise les WebSphere noms JNDI. Vous pouvez ajouter une <resource-ref>entrée dans le fichier web.xml avec le nom JNDI et la définition du DataSource type. Pour consulter un exemple de document de configuration, consultez la documentation d'Apache Tomcat.

- Journalisation : par défaut, Apache Tomcat se connecte à la console ou à un fichier journal. Vous pouvez activer le suivi au niveau du domaine en mettant à jour logging.properties (voir Logging in Tomcat). Si vous utilisez Apache Log4j pour ajouter des journaux à un fichier, vous devez télécharger tomcat-juli et l'ajouter au chemin de classe.
- Gestion des sessions : si vous conservez IBM WebSeal pour l'équilibrage de charge des applications et la gestion des sessions, aucune modification n'est requise. Si vous utilisez un Application Load Balancer ou un Network Load Balancer sur AWS pour remplacer le composant IBM WebSEAL, vous devez configurer la gestion de session en utilisant une instance ElastiCache Amazon avec un cluster Memcached et configurer Apache Tomcat pour utiliser la gestion de session open source.
- Si vous utilisez le proxy de transfert IBM WebSEAL, vous devez configurer un nouveau Network Load Balancer sur AWS. Utilisez celui IPs fourni par le Network Load Balancer pour les configurations de jonction WebSEAL.
- Configuration SSL : nous vous recommandons d'utiliser le protocole SSL (Secure Sockets Layer) pour les end-to-end communications. Pour configurer une configuration de serveur SSL dans Apache Tomcat, suivez les instructions de la documentation d'Apache Tomcat.

Architecture

Pile technologique source

- Serveur WebSphere d'applications IBM

Pile technologique cible

- L'architecture utilise Elastic Load Balancing (version 2). Si vous utilisez IBM WebSeal pour la gestion des identités et l'équilibrage de charge, vous pouvez sélectionner un Network Load Balancer sur AWS à intégrer au proxy inverse IBM WebSeal.
- Les applications Java sont déployées sur un serveur d'applications Apache Tomcat, qui s'exécute sur une EC2 instance d'un groupe Amazon EC2 Auto Scaling. Vous pouvez définir une politique de dimensionnement basée sur les CloudWatch indicateurs Amazon tels que l'utilisation du processeur.
- Si vous arrêtez d'utiliser IBM WebSeal pour l'équilibrage de charge, vous pouvez utiliser Amazon for Memcached ElastiCache pour la gestion des sessions.

- Pour la base de données principale, vous pouvez déployer la haute disponibilité (Multi-AZ) pour Amazon RDS et sélectionner un type de moteur de base de données.

Architecture cible

Outils

- AWS CloudFormation
- Interface de ligne de commande AWS (AWS CLI)
- Apache Tomcat (version 7). x ou 8. x)
- RHEL 7 ou Centos 7
- Déploiement multi-AZ d'Amazon RDS
- Amazon ElastiCache pour Memcached (facultatif)

Épopées

Configuration du VPC

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)		
Créez des sous-réseaux.		
Créez des tables de routage si nécessaire.		
Créez des listes de contrôle d'accès réseau (ACLs).		
Configurez AWS Direct Connect ou une connexion VPN d'entreprise.		

Replateformage de l'application

Tâche	Description	Compétences requises
Refactorisez la configura tion Maven de la version de l'application pour générer les artefacts WAR.		
Refactorisez les sources de données de dépendance des applications dans Apache Tomcat.		
Refactorisez les codes sources de l'application pour utiliser les noms JNDI dans Apache Tomcat.		
Déployez les artefacts WAR dans Apache Tomcat.		
Terminez les validations et les tests des applications.		

Configuration du réseau

Tâche	Description	Compétences requises
Configurez le pare-feu d'entreprise pour autoriser la connexion aux services de dépendance.		
Configurez le pare-feu de l'entreprise pour autoriser l'accès des utilisateurs finaux		

Tâche	Description	Compétences requises
à Elastic Load Balancing on AWS.		

Création de l'infrastructure d'applications

Tâche	Description	Compétences requises
Créez et déployez l'application sur une EC2 instance.		
Créez un cluster Amazon ElastiCache for Memcached pour la gestion des sessions.		
Créez une instance Amazon RDS Multi-AZ pour la base de données principale.		
Créez des certificats SSL et importez-les dans AWS Certificate Manager (ACM).		
Installez des certificats SSL sur les équilibreurs de charge.		
Installez des certificats SSL pour les serveurs Apache Tomcat.		
Terminez les validations et les tests des applications.		

Découper

Tâche	Description	Compétences requises
Arrêtez l'infrastructure existante.		
Restaurez la base de données de production vers Amazon RDS.		
Réduisez l'application en modifiant le DNS.		

Ressources connexes

Références

- Documentation d'Apache Tomcat 7.0
- Guide d'installation d'Apache Tomcat 7.0
- Documentation JNDI d'Apache Tomcat
- Déploiements multi-AZ d'Amazon RDS
- Amazon ElastiCache pour Memcached

Tutoriels et vidéos

- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)

Migrer une application .NET de Microsoft Azure App Service vers AWS Elastic Beanstalk

Créée par Raghavender Madamshitti (AWS)

Récapitulatif

Ce modèle décrit comment migrer une application Web .NET hébergée sur Microsoft Azure App Service vers AWS Elastic Beanstalk. Il existe deux méthodes pour migrer des applications vers Elastic Beanstalk :

- Utiliser AWS Toolkit for Visual Studio : ce plugin pour l'IDE Microsoft Visual Studio constitue le moyen le plus simple et le plus direct de déployer des applications .NET personnalisées sur AWS. Vous pouvez utiliser cette approche pour déployer du code .NET directement sur AWS et pour créer des ressources de support, telles qu'Amazon Relational Database Service (Amazon RDS) pour les bases de données SQL Server, directement depuis Visual Studio.
- Téléchargement et déploiement sur Elastic Beanstalk : chaque service d'application Azure inclut un service d'arrière-plan appelé Kudu, utile pour capturer les vidages de mémoire et les journaux de déploiement, consulter les paramètres de configuration et accéder aux packages de déploiement. Vous pouvez utiliser la console Kudu pour accéder au contenu d'Azure App Service, extraire le package de déploiement, puis télécharger le package sur Elastic Beanstalk en utilisant l'option de téléchargement et de déploiement de la console Elastic Beanstalk.

Ce modèle décrit la deuxième approche (téléchargement de votre application vers Elastic Beanstalk via Kudu). Le modèle utilise également les services AWS suivants : AWS Elastic Beanstalk, Amazon Virtual Private Cloud (Amazon VPC), Amazon, Amazon Elastic Compute Cloud (CloudWatchAmazon EC2) Auto Scaling, Amazon Simple Storage Service (Amazon S3) et Amazon Route 53.

L'application Web .NET est déployée sur AWS Elastic Beanstalk, qui s'exécute dans un groupe Amazon EC2 Auto Scaling. Vous pouvez définir une politique de dimensionnement basée sur les CloudWatch indicateurs Amazon tels que l'utilisation du processeur. Pour une base de données, vous pouvez utiliser Amazon RDS dans un environnement multi-AZ, ou Amazon DynamoDB, en fonction de votre application et des exigences commerciales.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif

- Une application Web .NET exécutée dans Azure App Service
- Autorisation d'utiliser la console Azure App Service Kudu

Versions du produit

- .NET Core (x64) 1.0.1, 2.0.0 ou version ultérieure, ou .NET Framework 4.x, 3.5 (voir l'historique de la plateforme .NET sur Windows Server)
- Internet Information Services (IIS) version 8.0 ou ultérieure, s'exécutant sur Windows Server 2012 ou version ultérieure
- .NET 2.0 ou 4.0 Runtime.

Architecture

Pile technologique source

- Application développée à l'aide de .NET Framework 3.5 ou version ultérieure, ou .NET Core 1.0.1, 2.0.0 ou version ultérieure, et hébergée sur Azure App Service (application Web ou application API)

Pile technologique cible

- AWS Elastic Beanstalk exécuté dans un groupe Amazon EC2 Auto Scaling

Architecture de migration

Flux de travail de déploiement

Outils

Outils

- .NET Core ou .NET Framework
- C#
- IIS
- Console Kudu

Services et fonctionnalités AWS

- AWS Elastic Beanstalk — Elastic Beanstalk est un service de déploiement et de mise à l' easy-to-useéchelle d'applications Web .NET. Elastic Beanstalk gère automatiquement le provisionnement des capacités, l'équilibrage de charge et le dimensionnement automatique.
- Groupe Amazon EC2 Auto Scaling — Elastic Beanstalk inclut un groupe Auto Scaling qui gère les instances Amazon EC2 dans l'environnement. Dans un environnement à instance unique, le groupe Auto Scaling s'assure qu'il y a toujours une instance en cours d'exécution. Dans un environnement à charge équilibrée, vous pouvez configurer le groupe avec une série d'instances à exécuter, et Amazon EC2 Auto Scaling ajoute ou supprime des instances selon les besoins, en fonction de la charge.
- Elastic Load Balancing : lorsque vous activez l'équilibrage de charge dans AWS Elastic Beanstalk, cela crée un équilibreur de charge qui répartit le trafic EC2 entre les instances de l'environnement.
- Amazon CloudWatch — Elastic Beanstalk CloudWatch utilise automatiquement Amazon pour fournir des informations sur les ressources de votre application et de votre environnement. Amazon CloudWatch prend en charge les métriques standard, les métriques personnalisées et les alarmes.
- Amazon Route 53 — Amazon Route 53 est un service Web de système de noms de domaine (DNS) cloud hautement disponible et évolutif. Vous pouvez utiliser les enregistrements d'alias Route 53 pour mapper des noms de domaine personnalisés aux environnements AWS Elastic Beanstalk.

Épopées

Configurez un VPC

Tâche	Description	Compétences requises
Configurez un cloud privé virtuel (VPC).	Dans votre compte AWS, créez un VPC avec les informations requises.	Administrateur système
Créez des sous-réseaux.	Créez au moins deux sous-réseaux dans votre VPC.	Administrateur système
Créez une table de routage.	Créez une table de routage en fonction de vos besoins.	Administrateur système

Configurer Elastic Beanstalk

Tâche	Description	Compétences requises
Accédez à la console Azure App Service Kudu.	Accédez à Kudu via le portail Azure en accédant au tableau de bord App Service, puis en choisissant Advanced Tools, Go. Ou, vous pouvez modifier l'URL d'Azure App Service comme suit :`https://<appservicename>.scm.azurewebsites.net` .	Développeur d'applications, administrateur système
Téléchargez le package de déploiement depuis Kudu.	Accédez à Windows PowerShell en choisissant l'DebugConsoleoption. Cela ouvrira la console Kudo. Accédez au `wwwroot` dossier et téléchargez-le. Cela téléchargera le package de déploiement d'Azure App Service sous forme de fichier zip. Pour un exemple, voir la pièce jointe.	Développeur d'applications, administrateur système
Créez un package pour Elastic Beanstalk.	Décompressez le package de déploiement que vous avez téléchargé depuis Azure App Service. Créez un fichier JSON appelé `aws-windows-deployment-manifest.json` (ce fichier n'est requis que pour les applications .NET Core). Créez un fichier zip qui inclut `aws-windows-deployment-`	Développeur d'applications, administrateur système

Tâche	Description	Compétences requises
	`manifest.json` le fichier du package de déploiement Azure App Service. Pour un exemple, voir la pièce jointe.	
Créez une nouvelle application Elastic Beanstalk.	Ouvrez la console Elastic Beanstalk. Choisissez une application existante ou créez-en une nouvelle.	Développeur d'applications, administrateur système
Création de l'environnement	Dans le menu Actions de la console Elastic Beanstalk, choisissez Create environment. Sélectionnez l'environnement du serveur Web et la plate-forme .NET/IIS. Pour le code de l'application, choisissez Upload. Téléchargez le fichier zip que vous avez préparé pour Elastic Beanstalk, puis choisissez Create Environment.	Développeur d'applications, administrateur système
Configurez Amazon CloudWatch.	Par défaut, la CloudWatch surveillance de base est activée. Si vous souhaitez modifier la configuration, dans l'assistant Elastic Beanstalk, choisissez l'application publiée, puis choisissez Monitoring.	Administrateur système

Tâche	Description	Compétences requises
Vérifiez que le package de déploiement se trouve dans Amazon S3.	Lorsque l'environnement d'application a été créé, vous pouvez trouver le package de déploiement dans le compartiment S3.	Développeur d'applications, administrateur système
Testez l'application.	Une fois l'environnement créé, utilisez l'URL fournie dans la console Elastic Beanstalk pour tester l'application.	Administrateur système

Ressources connexes

- Concepts d'AWS Elastic Beanstack (documentation Elastic Beanstalk)
- Commencer à utiliser .NET sur Elastic Beanstalk (documentation Elastic Beanstalk)
- Console Kudu () GitHub
- Utilisation de « Kudu » pour gérer les applications Web Azure (article du GS Lab)
- Déploiements ASP.NET Core Elastic Beanstalk personnalisés (guide de l'utilisateur d'AWS Toolkit pour Visual Studio)
- Documentation sur Elastic Load Balancing
- Plateformes prises en charge par AWS Elastic Beanstalk (documentation Elastic Beanstalk)
- Déployer une application Web sur AWS (article C# Corner)
- Dimensionnement de la taille de votre groupe Auto Scaling (EC2 documentation Amazon)
- Haute disponibilité (multi-AZ) pour Amazon RDS (documentation Amazon RDS)

Informations supplémentaires

Remarques

- Si vous migrez une base de données locale ou Azure SQL Server vers Amazon RDS, vous devez également mettre à jour les informations de connexion à la base de données.
- À des fins de test, un exemple d'application de démonstration est joint.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer d'Oracle WebLogic vers Apache Tomcat (ToMee) sur Amazon ECS

Créée par Anya Epishcheva (AWS) et Harshad Gohil (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'un système Oracle Solaris SPARC sur site exécutant Oracle WebLogic vers une installation basée sur des conteneurs Docker exécutant Apache ToMee (Apache Tomcat avec support de conteneur supplémentaire) avec Amazon Elastic Container Service (Amazon ECS).

Pour plus d'informations sur la migration des bases de données associées aux applications que vous migrez d'Oracle WebLogic vers Tomcat, consultez les modèles de migration de base de données de ce catalogue.

Bonnes pratiques

Les étapes de migration des applications Web Java et Java Enterprise Edition (Java EE) varient en fonction du nombre de ressources spécifiques au conteneur utilisées par l'application. Les applications basées sur Spring sont généralement plus faciles à migrer, car elles ne dépendent que d'un petit nombre de fois par rapport au conteneur de déploiement. En revanche, les applications Java EE qui utilisent Enterprise JavaBeans (EJBs) et des ressources de conteneur gérées telles que les pools de threads, le service d'authentification et d'autorisation Java (JAAS) et la persistance gérée par conteneur (CMP) nécessitent plus d'efforts.

Les applications développées pour Oracle Application Server utilisent fréquemment la suite Oracle Identity Management. Les clients qui migrent vers des serveurs d'applications open source choisissent souvent de réimplémenter la gestion des identités et des accès à l'aide de la fédération basée sur le protocole SAML. D'autres utilisent Oracle HTTP Server Webgate dans les cas où la migration depuis la suite Oracle Identity Management n'est pas une option.

Les applications Web Java et Java EE sont d'excellentes candidates pour le déploiement sur des services AWS basés sur Docker, tels que AWS Fargate et Amazon ECS. Les clients choisissent souvent une image Docker avec la dernière version du serveur d'applications cible (tel que ToMee) et le kit de développement Java (JDK) préinstallés. Ils installent leurs applications au-dessus de l'image Docker de base, la publient dans leur registre Amazon Elastic Container Registry (Amazon ECR) et l'utilisent pour le déploiement évolutif de leurs applications sur AWS Fargate ou Amazon ECS.

Idéalement, le déploiement des applications est élastique, c'est-à-dire que le nombre d'instances d'application augmente ou diminue en fonction du trafic ou de la charge de travail. Cela signifie que

les instances d'application doivent être mises en ligne ou mises hors service pour ajuster la capacité à la demande.

Lorsque vous déplacez une application Java vers AWS, pensez à la rendre apatride. Il s'agit d'un principe architectural clé de l'AWS Well-Architected Framework qui permettra une mise à l'échelle horizontale à l'aide de la conteneurisation. Par exemple, la plupart des applications Web basées sur Java stockent les informations de session utilisateur localement. Pour éviter la fermeture d'une instance d'application en raison du dimensionnement automatique dans Amazon Elastic Compute Cloud (Amazon EC2) ou pour d'autres raisons, les informations de session utilisateur doivent être stockées dans le monde entier afin que les utilisateurs des applications Web puissent continuer à travailler de manière fluide et transparente sans se reconnecter ou se reconnecter à une application Web. Il existe plusieurs options architecturales pour cette approche, notamment Amazon ElastiCache pour Redis ou le stockage de l'état de session dans une base de données globale. Les serveurs d'applications tels que TomEE disposent de plug-ins qui permettent le stockage et la gestion des sessions via Redis, des bases de données et d'autres magasins de données mondiaux.

Utilisez un outil de journalisation et de débogage commun et centralisé qui s'intègre facilement à Amazon CloudWatch et AWS X-Ray. La migration permet d'améliorer les fonctionnalités du cycle de vie des applications. Par exemple, vous souhaiterez peut-être automatiser le processus de création afin que les modifications soient facilement apportées à l'aide d'un pipeline d'intégration et de livraison continues (CI/CD). Cela peut nécessiter des modifications de l'application afin qu'elle puisse être déployée sans interruption.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Code source Java et JDK
- Application source créée avec Oracle WebLogic
- Solution définie pour la gestion des identités et des accès (SAML ou Oracle Webgate)
- Solution définie pour la gestion des sessions d'application (transfert like-for-like ou utilisation d'Amazon ElastiCache, ou mise en état de l'application si nécessaire)
- Comprendre si l'équipe doit refactoriser les bibliothèques spécifiques à J2EE pour la portabilité vers Apache ToMee (voir État de l'implémentation de Java EE 7 sur le site Web d'Apache)
- Image TomEee renforcée en fonction de vos exigences de sécurité
- Image du conteneur avec ToMee cible préinstallée

- Corrections d'applications convenues et mises en œuvre si nécessaire (par exemple, journalisation, débogage, construction, authentification)

Versions du produit

- Oracle WebLogic OC4 J, 9i, 10 g
- Tomcat 7 (avec Java 1.6 ou version ultérieure)

Architecture

Pile technologique source

- Application Web créée à l'aide d'Oracle WebLogic
- Application Web utilisant l'authentification Oracle Webgate ou SAML
- Applications Web connectées à Oracle Database version 10g et ultérieure

Pile technologique cible

- TomEE (Apache Tomcat avec prise en charge des conteneurs ajoutée) s'exécutant sur Amazon ECS (voir également Déploiement d'applications Web Java et de microservices Java sur Amazon ECS)
- Amazon Relational Database Service (Amazon RDS) pour Oracle ; pour les versions d'Oracle prises en charge par Amazon RDS, consultez Amazon RDS pour Oracle

Architecture cible

Outils

Pour fonctionner sur TomEE, une application Java doit être reconstruite dans un fichier .war. Dans certains cas, des modifications d'application peuvent être nécessaires pour faire fonctionner l'application sur ToMee ; vous devez vérifier que les options de configuration et les propriétés d'environnement nécessaires sont correctement définies.

En outre, les recherches JNDI (Java Naming and Directory Interface) et les espaces de noms JavaServer Pages (JSP) doivent être définis correctement. Pensez à vérifier les noms de fichiers

utilisés par l'application pour éviter les collisions de noms avec les bibliothèques T intégrées. Par exemple, persistence.xml est un nom de fichier utilisé par le framework Apache OpenJPA (qui est fourni avec OpenEJB dans TomEE) à des fins de configuration. Le fichier persistence.xml du PUI contient les déclarations de bean du framework Spring.

TomEE version 7.0.3 et versions ultérieures (Tomcat 8.5.7 et versions ultérieures) renvoie une réponse HTTP 400 (mauvaise requête) pour le format brut (non codé) avec des caractères spéciaux. URLs La réponse du serveur apparaît sous forme de page blanche à l'utilisateur final. Les versions antérieures de Tomee et Tomcat autorisaient l'utilisation de certains caractères spéciaux non codés URLs ; toutefois, cela est considéré comme dangereux, comme indiqué sur le site Web CVE-2016-6816. Pour résoudre le problème d'encodage des URL, les URLs informations transmises directement au navigateur via JavaScript doivent être codées avec la méthode encodeURI () au lieu d'être utilisées sous forme de chaînes brutes.

Après avoir déployé le fichier .war dans ToMee, surveillez le journal de démarrage sur Linux cat pour détecter les bibliothèques partagées manquantes et les extensions spécifiques à Oracle afin d'ajouter les composants manquants dans les bibliothèques Tomcat.

Procédure générale

- Configurez l'application sur TomEE.
- Identifiez et reconfigurez les fichiers de configuration et les ressources spécifiques au serveur d'applications, du format source au format cible.
- Identifiez et reconfigurez les ressources JNDI.
- Ajustez l'espace de noms et les recherches EJB au format requis par le serveur d'applications cible (le cas échéant).
- Reconfigurez les rôles de sécurité et les mappages principaux spécifiques au conteneur d'applications JAAS (le cas échéant).
- Package de l'application et des bibliothèques partagées dans un fichier .war.
- Déployez le fichier .war dans Tomee à l'aide du conteneur Docker fourni.
- Surveillez le journal de démarrage pour identifier les extensions de bibliothèque partagée et de descripteur de déploiement manquantes. Si vous en trouvez, revenez à la première tâche.
- Testez l'application installée par rapport à la base de données Amazon RDS restaurée.
- Lancez l'architecture complète avec un équilibreur de charge et un cluster Amazon ECS en suivant les instructions de la section Déployer des conteneurs Docker.

- Mettez à jour le URLs pour qu'il pointe vers l'équilibreur de charge.
- Mettez à jour la base de données de gestion de configuration (CMDB).

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Effectuez la découverte des applications (empreinte de l'état actuel et référence de performances).		BA, responsable de la migration
Validez les versions et les moteurs des bases de données source et cible.		DBA
Validez la conception de l'application source et cible (gestion des identités et des sessions).		DBA, ingénieur en migration, propriétaire de l'application
Identifiez les exigences matérielles et de stockage pour l'instance de serveur cible.		DBA, SysAdmin
Choisissez le type d'instanc e approprié en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		DBA, SysAdmin
Identifiez les exigences de sécurité d'accès réseau pour les bases de données source et cible.		DBA, SysAdmin

Tâche	Description	Compétences requises
Identifiez la stratégie et les outils de migration des applications.		DBA, responsable de la migration
Complétez le guide de conception et de migration de l'application.		Responsable de la création, responsable de la migration
Terminez le runbook de migration des applications.		Responsable du développement, responsable du transfert, responsable des tests, responsable de la migration

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)		SysAdmin
Créez des groupes de sécurité.		SysAdmin
Configurez et démarrez l'instance de base de données Amazon RDS.		DBA, SysAdmin
Configurez le déploiement d'Amazon ECS.		SysAdmin
Package de votre application sous forme d'image Docker.		SysAdmin
Transférez l'image vers le registre Amazon ECR (ou ignorez cette étape et		SysAdmin

Tâche	Description	Compétences requises
transférez-la vers le cluster Amazon ECS).		
Configurez la définition de tâche pour l'application et les options de service Amazon ECS.		SysAdmin
Configurez votre cluster, passez en revue les paramètres de sécurité et définissez les rôles AWS Identity and Access Management (IAM).		SysAdmin
Lancez votre installation et exécutez les tests conformément au manuel de migration de votre application.		SysAdmin

Migrer les données

Tâche	Description	Compétences requises
Obtenez l'autorisation de votre équipe d'assurance sécurité pour transférer les données de production vers AWS.		DBA, ingénieur en migration, propriétaire de l'application
Créez et obtenez l'accès à des points de terminaison pour récupérer les fichiers de sauvegarde de la base de données.		DBA

Tâche	Description	Compétences requises
Utilisez le moteur de base de données natif ou des outils tiers pour migrer les objets et les données de base de données.		DBA
Exécutez les tests nécessaires depuis le runbook de migration des applications pour confirmer la réussite de la migration des données.		DBA, ingénieur en migration, propriétaire de l'application

Migrer l'application

Tâche	Description	Compétences requises
Créez une demande de modification (CR) pour la migration.		Plomb de découpe
Obtenez l'approbation du CR pour la migration.		Plomb de découpe
Suivez la stratégie de migration des applications décrite dans le runbook de migration des applications.		DBA, ingénieur en migration, propriétaire de l'application
Mettez à niveau l'application (si nécessaire).		DBA, ingénieur en migration, propriétaire de l'application
Effectuez des tests fonctionnels, non fonctionnels, de validation des données, de SLA et de performance.		Responsable des tests, propriétaire de l'application, utilisateurs de l'application

Découper

Tâche	Description	Compétences requises
Obtenez l'approbation de l'application ou du propriétaire de l'entreprise.		Plomb de découpe
Exécutez un exercice sur le thème d'un tableau pour suivre toutes les étapes du runbook de transition.		DBA, ingénieur en migration, propriétaire de l'application
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, ingénieur en migration, propriétaire de l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		DBA, ingénieur en migration, SysAdmin
Passez en revue et validez les documents du projet.		Responsable de la migration
Collectez des indicateu rs concernant le délai de migration, le pourcentage de manuel par rapport à l'outil, les économies de coûts, etc.		Responsable de la migration
Clôturez le projet et faites part de vos commentaires.		Responsable de la migration, propriétaire de l'application

Ressources connexes

Références

- Documentation d'Apache Tomcat 7.0
- Guide d'installation d'Apache Tomcat 7.0
- Documentation JNDI d'Apache Tomcat
- Documentation d'Apache ToMee
- Amazon RDS for Oracle
- Tarification d’Amazon RDS
- Oracle et AWS
- Documentation Oracle sur Amazon RDS
- Déploiements multi-AZ d'Amazon RDS
- Commencer à utiliser Amazon ECS
- Mise en route avec Amazon RDS

Tutoriels et vidéos

- Meilleures pratiques pour exécuter des bases de données Oracle sur Amazon RDS (présentation re:Invent 2018)

Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for Oracle à l'aide d'AWS DMS

Créée par Chethan Gangadharaiah (AWS) et Brian Motzer (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'une base de données Oracle sur Amazon Elastic Compute Cloud (Amazon EC2) vers Amazon Relational Database Service (Amazon RDS) pour Oracle à l'aide d'AWS Database Migration Service (AWS DMS). Le modèle utilise également Oracle SQL Developer ou SQL *Plus pour se connecter à votre instance de base de données Oracle, et inclut un CloudFormation modèle AWS qui automatise certaines tâches.

La migration vers Amazon RDS for Oracle vous permet de vous concentrer sur votre activité et vos applications, tandis qu'Amazon RDS s'occupe des tâches d'administration des bases de données telles que le provisionnement des bases de données, la sauvegarde et la restauration, les correctifs de sécurité, les mises à niveau des versions et la gestion du stockage.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une image machine Amazon (AMI) pour la base de données Oracle sur Amazon EC2

Versions du produit

- AWS DMS prend en charge les versions 11g (versions 11.2.0.3.v1 et ultérieures), 12c et 18c d'Oracle pour les bases de données d'instances Amazon RDS pour les éditions Enterprise, Standard, Standard One et Standard Two. Pour obtenir les dernières informations sur les versions prises en charge, consultez la section Utilisation d'une base de données Oracle comme cible pour AWS DMS dans la documentation AWS. (Les CloudFormation modèles AWS joints utilisent la version 12c d'Oracle comme base de données source.)
- Développeur Oracle SQL 4.0.3

Architecture

Architecture de la source

- Base de données Oracle sur Amazon EC2

Architecture cible

- Amazon RDS for Oracle

Architecture de migration

Outils

- AWS DMS — AWS Database Migration Service (AWS DMS) vous aide à migrer des bases de données vers AWS rapidement et en toute sécurité. Il prend en charge les migrations homogènes et hétérogènes. Pour plus d'informations sur les versions et éditions de base de données Oracle prises en charge, consultez les sections Utilisation d'une base de données Oracle comme source pour AWS DMS et Utilisation d'une base de données Oracle comme cible pour AWS DMS dans la documentation AWS.
- Oracle SQL Developer ou SQL *Plus : ces outils vous permettent de vous connecter à l'instance de base de données Amazon RDS for Oracle.

Épopées

Configuration de votre base de données cible

Tâche	Description	Compétences requises
Créez une instance de base de données Amazon RDS for Oracle.	Connectez-vous à AWS Management Console et ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/. Créez une instance de base de données Oracle en sélectionnant le moteur, le modèle, le paramètre d'identification de base de données, le type d'instance, le stockage,	Developer

Tâche	Description	Compétences requises
	les paramètres multi-AZ, le cloud privé virtuel (VPC) et la configuration appropriés, les informations d'identification de connexion et les paramètres supplémentaires pour la base de données Oracle. Pour obtenir des instructions, consultez les liens dans la section « Ressources connexes ». Vous pouvez également utiliser le CloudFormation modèle AWS (Create_RDS.yaml) dans la pièce jointe pour créer l'instance de base de données Amazon RDS for Oracle.	

Tâche	Description	Compétences requises
Connectez-vous à Amazon RDS et accordez des privilèges à l'utilisateur Oracle.	Modifiez le groupe de sécurité pour ouvrir les ports appropriés pour vous connecter à partir de la machine locale et de l'instance de réplication AWS DMS. Lorsque vous configurez la connectivité, assurez-vous que l'option « Accessible au public » est sélectionnée afin de pouvoir vous connecter à la base de données depuis l'extérieur du VPC. Connectez-vous à Amazon RDS avec Oracle SQL Developer ou SQL *Plus en utilisant les informations de connexion, créez un utilisateur AWS DMS et accordez les privilèges requis à l'utilisateur AWS DMS pour modifier la base de données.	Developer

Configurer le groupe de sécurité de l' EC2 instance source

Tâche	Description	Compétences requises
Vérifiez si la base de données Oracle est opérationnelle.	Utilisez Secure Shell (SSH) pour vous connecter à l' EC2 instance et essayez de vous connecter à la base de données Oracle à l'aide de SQL *Plus.	Developer

Tâche	Description	Compétences requises
Modifiez le groupe de sécurité.	Modifiez le groupe de sécurité de l' EC2 instance pour ouvrir les ports appropriés, afin de pouvoir vous connecter depuis votre machine locale et l'instance de réplication AWS DMS.	Developer

Configuration d'AWS DMS

Tâche	Description	Compétences requises
Créez une instance de réplication AWS DMS.	Dans AWS DMS, créez une instance de réplication dans le même VPC que votre instance de base de données Amazon RDS for Oracle. Spécifiez le nom et la description de l'instance de réplication, choisissez la classe d'instanc e et la version du moteur de réplication (utilisez la valeur par défaut), choisissez le VPC dans lequel vous avez créé l'instance de base de données Amazon RDS, définisse z les paramètres multi-AZ si nécessaire, allouez du stockage, spécifiez la zone de disponibilité et configurez des paramètres supplémentaires. Vous pouvez également utiliser le CloudFormation modèle AWS (DMS.yaml	DBA

Tâche	Description	Compétences requises
	) dans la pièce jointe pour implémenter cette étape.	
Connectez-vous aux points de terminaison de la base de données source et cible.	Créez les points de terminaison de base de données source et cible en spécifiant l'identifiant du point de terminaison, le moteur, le serveur, le port, les informations de connexion et les attributs de connexion supplémentaires. Pour le serveur source, utilisez le DNS public de l' EC2 instance qui héberge la base de données Oracle. Pour le serveur cible, utilisez le point de terminaison d'Amazon RDS for Oracle. Effectuez un test pour vérifier que les connexions source et cible fonctionnent. Vous pouvez également utiliser le CloudFormation modèle AWS (DMS.yaml) dans la pièce jointe pour implémenter cette étape.	DBA

Tâche	Description	Compétences requises
Créez une tâche AWS DMS.	Créez une tâche AWS DMS pour migrer les données du point de terminaison source vers le point de terminaison cible, pour configurer la réplication entre le point de terminaison source et le point de terminaison de destination, ou les deux. Lors de la création de la tâche AWS DMS, spécifiez l'instance de réplication, le point de terminaison source, le point de terminaison cible, le type de migration (données uniquement, réplication uniquement, ou les deux), le mappage des tables et le filtre. Exécutez la tâche AWS DMS, surveillez-la, consultez les statistiques du tableau et consultez les journaux sur Amazon CloudWatch. Vous pouvez également utiliser le CloudFormation modèle AWS (DMS.yaml) dans la pièce jointe pour implémenter cette étape.	DBA

Ressources connexes

- Création d'une instance de base de données Amazon RDS
- Connexion à une instance de base de données exécutant le moteur de base de données Oracle
- Documentation AWS DMS

- Procédures pas à pas d'AWS DMS Step-by-Step
- Migration des bases de données Oracle vers le cloud AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer une base de données Oracle sur site vers Amazon OpenSearch Service à l'aide de Logstash

Créée par Aditya Goteti (AWS)

Récapitulatif

Ce modèle décrit comment déplacer des données d'une base de données Oracle sur site vers Amazon OpenSearch Service à l'aide de Logstash. Il inclut des considérations architecturales ainsi que certaines compétences et recommandations requises. Les données peuvent provenir d'une seule table ou de plusieurs tables dans lesquelles une recherche en texte intégral devra être effectuée.

OpenSearch Le service peut être configuré dans un cloud privé virtuel (VPC), ou il peut être placé publiquement avec des restrictions basées sur l'IP. Ce modèle décrit un scénario dans lequel le OpenSearch service est configuré au sein d'un VPC. Logstash est utilisé pour collecter les données de la base de données Oracle, les analyser au format JSON, puis les introduire dans Service. OpenSearch

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Java 8 (requis par Logstash 6.4.3)
- Connectivité entre les serveurs de base de données sur site et les instances Amazon Elastic Compute Cloud (Amazon EC2) dans un VPC, établie à l'aide du réseau privé virtuel AWS (AWS VPN)
- Une requête pour récupérer les données requises à envoyer au OpenSearch Service à partir de la base de données
- Pilotes Oracle Java Database Connectivity (JDBC)

Limites

- Logstash ne peut pas identifier les enregistrements supprimés définitivement de la base de données

Versions du produit

- Oracle Database 12c
- OpenSearch Service 6.3
- Logstash 6.4.3

Architecture

Pile technologique source

- Base de données Oracle sur site
- VPN AWS sur site

Pile technologique cible

- VPC
- EC2 instance
- OpenSearch Service
- Logstash
- Passerelle NAT (pour les mises à jour du système d'exploitation sur les EC2 instances et pour installer Java 8, Logstash et les plugins)

Architecture de migration des données

Outils

- Logstash 6.4.3
- Plug-in d'entrée JDBC (téléchargement et informations supplémentaires)
- Plug-in de sortie Logstash (_es) logstash-output-amazon
- Pilotes Oracle JDBC

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Identifiez la taille des données sources.	La taille des données source est l'un des paramètres que vous utilisez pour déterminer le nombre de partitions à configurer dans un index.	DBA, développeur de bases de données
Analysez les types de données de chaque colonne et les données correspondantes.	OpenSearch Le service mappe dynamiquement le type de données lorsqu'un champ invisible est trouvé dans le document. Si certains types ou formats de données spécifiques (par exemple, les champs de date) doivent être explicitement déclarés, identifiez les champs et définissez le mappage de ces champs lors de la création de l'index.	Propriétaire de l'application, développeur, développeur de base de données
Déterminez s'il existe des colonnes avec des clés primaires ou uniques.	Pour éviter la duplication des enregistrements dans Amazon OpenSearch Service lors des mises à jour ou des insertions, vous devez configurer le `document_id` paramètre dans la section de sortie du `amazon_es` plugin (par exemple, `document_id => "%{customer_id}"` où se `customer_id` trouve une clé primaire).	Propriétaire de l'application, développeur

Tâche	Description	Compétences requises
Analysez le nombre et la fréquence des nouveaux enregistrements ajoutés ; vérifiez la fréquence à laquelle les enregistrements sont supprimés.	Cette tâche est nécessaire pour comprendre le taux de croissance des données sources. Si les données sont lues de manière intensive et que les insertions sont rares, vous pouvez avoir un seul index. Si de nouveaux enregistrements sont insérés fréquemment et qu'il n'y a aucune suppression, la taille de la partition peut facilement dépasser la taille maximale recommandée de 50 Go. Dans ce cas, vous pouvez créer un index de manière dynamique en configurant des modèles d'index dans Logstash et dans le code auquel vous pouvez accéder à l'aide d'un alias.	Propriétaire de l'application, développeur
Déterminez le nombre de répliques nécessaires.		Propriétaire de l'application, développeur
Déterminez le nombre de partitions à configurer sur l'index.		Propriétaire de l'application, développeur
Identifiez les types d'instances pour les nœuds maîtres dédiés, les nœuds de données et l' EC2 instance.	Pour plus d'informations, consultez la section Ressources connexes.	Propriétaire de l'application, développeur

Tâche	Description	Compétences requises
Déterminez le nombre de nœuds maîtres et de nœuds de données dédiés requis.	Pour plus d'informations, consultez la section Ressources connexes.	

Migrer les données

Tâche	Description	Compétences requises
Lancez une EC2 instance.	Lancez une EC2 instance au sein du VPC auquel le VPN AWS est connecté.	Constructions Amazon VPC, AWS VPN
Installez Logstash sur l'instanc e. EC2		Developer
Installez les plugins Logstash.	Installez les plugins `jdbc-input` Logstash requis et. `logstash-output-am azon_es`	Developer
Configurez Logstash.	Créez le keystore Logstash pour stocker des informations sensibles telles que les clés AWS Secrets Manager et les informations d'identification de base de données, puis placez les références dans un fichier de configuration Logstash.	Developer
Configurez la file d'attente des lettres mortes et la file d'attente persistante.	Par défaut, lorsque Logstash rencontre un événement qu'il ne peut pas traiter en raison d'une erreur de mappage ou d'un autre problème, le pipeline Logstash bloque	Developer

Tâche	Description	Compétences requises
	ou supprime l'événeme nt infructueux. Pour vous protéger contre la perte de données dans ce cas, vous pouvez configurer Logstash pour qu'il inscrive les événements infructueux dans une file d'attente lettre morte au lieu de les supprimer. Pour se protéger contre la perte de données lors d'une interrupt ion anormale, Logstash dispose d'une fonction de file d'attente persistante qui permet de stocker la file de messages sur le disque. Les files d'attente persistantes garantissent la durabilité des données dans Logstash.	

Tâche	Description	Compétences requises
Créez le domaine Amazon OpenSearch Service.	Créez le domaine Amazon OpenSearch Service avec une politique d'accès qui n'exige pas de signer les demandes avec les informations d'identification AWS Identity and Access Management (IAM). Le domaine Amazon OpenSearch Service doit être créé au sein du même VPC. Vous devez également sélectionner les types d'instances et définir le nombre de nœuds dédiés et maîtres en fonction de votre analyse.	Developer
Configurez les journaux Amazon OpenSearch Service requis.	Pour plus d'informations, consultez la documentation du OpenSearch service.	
Créez l'index.		Developer
Lancez Logstash.	Exécutez Logstash en tant que service d'arrière-plan. Logstash exécute la requête SQL configurée, extrait les données, les convertit au format JSON et les transmet au OpenSearch Service. Pour le chargement initial, ne configurez pas le planificateur dans le fichier de configuration de Logstash.	Developer

Tâche	Description	Compétences requises
Vérifiez les documents.	Vérifiez le nombre de documents figurant dans l'index et vérifiez si tous les documents sont présents dans la base de données source. Lors du chargement initial, ils sont ajoutés à l'index et utilisés pour arrêter Logstash. Modifiez la configuration de Logstash pour ajouter un planificateur qui s'exécute à intervalles fixes en fonction des besoins du client, puis redémarrez Logstash. Logstash sélectionne uniquement les enregistr ements qui ont été mis à jour ou ajoutés après la dernière exécution, et l'horodatage de la dernière exécution est stocké dans le fichier configuré avec la propriété `last_run_metadata_ path => “/usr/sha re/logstash/.logst ash_jdbc_last_run”` du fichier de configuration Logstash.	Developer

Ressources connexes

- CloudWatch Alarmes recommandées
- Nœuds OpenSearch principaux Amazon Service dédiés

- Dimensionnement des domaines Amazon OpenSearch Service
- Documentation de Logstash
- Plug-in d'entrée JDBC
- Plug-in de sortie Logstash
- Site Web Amazon OpenSearch Service

Migrer une base de données Oracle sur site vers Amazon RDS for Oracle

Créée par Baji Shaik (AWS) et Pavan Pusuluri (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration des bases de données Oracle locales vers Amazon Relational Database Service (Amazon RDS) pour Oracle. Dans le cadre du processus de migration, vous créez un plan de migration et vous tenez compte des facteurs importants concernant votre infrastructure de base de données cible en fonction de votre base de données source. Vous pouvez choisir l'une des deux options de migration en fonction des besoins de votre entreprise et de votre cas d'utilisation :

- AWS Database Migration Service (AWS DMS) : vous pouvez utiliser AWS DMS pour migrer des bases de données vers le cloud AWS rapidement et en toute sécurité. Votre base de données source reste pleinement opérationnelle pendant la migration, ce qui minimise les interruptions de service pour les applications qui dépendent de la base de données. Vous pouvez réduire le temps de migration en utilisant AWS DMS pour créer une tâche qui capture les modifications en cours après avoir effectué une migration initiale complète via un processus appelé capture des données de modification (CDC).
- Outils Oracle natifs : vous pouvez migrer des bases de données à l'aide d'outils Oracle natifs, tels qu'Oracle et Data Pump Export et Data Pump Import with Oracle GoldenGate for CDC. Vous pouvez également utiliser des outils Oracle natifs tels que l'utilitaire d'exportation et l'utilitaire d'importation d'origine pour réduire le temps de chargement complet.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données Oracle sur site
- Une instance de base de données Oracle (DB) Amazon RDS

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- Versions Oracle 11g (versions 11.2.0.3.v1 et ultérieures) et versions 12.2 et 18c supérieures. Pour obtenir la dernière liste des versions et éditions prises en charge, consultez Amazon RDS for Oracle dans la documentation AWS. Pour les versions d'Oracle prises en charge par AWS DMS, consultez la section Utilisation d'une base de données Oracle comme source pour AWS DMS dans la documentation AWS DMS.

Architecture

Pile technologique source

- Bases de données Oracle sur site

Pile technologique cible

- Amazon RDS for Oracle

Architecture source et cible

Le schéma suivant montre comment migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'AWS DMS.

Le schéma suivant illustre le flux de travail suivant :

1. Créez ou utilisez un utilisateur de base de données existant, accordez les autorisations AWS DMS requises à cet utilisateur, activez le mode ARCHIVELOG, puis configurez une journalisation supplémentaire.
2. Configurez la passerelle Internet entre le réseau sur site et le réseau AWS.
3. Configurez les points de terminaison source et cible pour AWS DMS.
4. Configurez les tâches de réplication AWS DMS pour migrer les données de la base de données source vers la base de données cible.
5. Effectuez les activités post-migration sur la base de données cible.

Le schéma suivant montre comment migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'outils Oracle natifs.

Le schéma suivant illustre le flux de travail suivant :

1. Créez ou utilisez un utilisateur de base de données existant et accordez les autorisations requises pour sauvegarder la base de données Oracle à l'aide des utilitaires Oracle Export (`exp`) et Import (`imp`).
2. Configurez la passerelle Internet entre le réseau sur site et le réseau AWS.
3. Configurez le client Oracle sur l'hôte Bastion pour qu'il prenne la base de données de sauvegarde.
4. Chargez la base de données de sauvegarde dans un compartiment Amazon Simple Storage Service (Amazon S3).
5. Restaurez la sauvegarde de base de données depuis Amazon S3 vers une base de données Amazon RDS for Oracle.
6. Configurez Oracle GoldenGate pour CDC.
7. Effectuez les activités post-migration sur la base de données cible.

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site.
- Les outils Oracle natifs vous aident à effectuer une migration homogène. Vous pouvez utiliser Oracle Data Pump pour faire migrer les données entre vos bases de données source et cible. Ce modèle utilise Oracle Data Pump pour effectuer le chargement complet de la base de données source vers la base de données cible.
- Oracle vous GoldenGate aide à effectuer une réplication logique entre deux bases de données ou plus. Ce modèle est utilisé GoldenGate pour reproduire les modifications du delta après le chargement initial à l'aide d'Oracle Data Pump.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Créez des documents de projet et enregistrez les détails de la base de données.	1. Documentez vos objectifs de migration, vos exigences en matière de migration	DBA

Tâche	Description	Compétences requises
	, les principales parties prenantes du projet, les étapes clés du projet, les indicateurs clés, les risques liés à la migration et les plans d'atténuation des risques. 2. Documentez les informations critiques concernant votre base de données source, notamment la RAM, les IOPS et CPUs. Vous utiliserez ultérieurement ces informations pour déterminer l'instance de base de données cible appropriée. 3. Validez les versions de vos bases de données source et cible.	

Tâche	Description	Compétences requises
Identifiez les besoins en matière de stockage.	Identifiez et documentez vos besoins en matière de stockage, notamment les suivants : 1. Calculez le stockage alloué à l'instance de base de données source. 2. Rassemblez les mesures de croissance historiques à partir de l'instance de base de données source. 3. Forecast future la croissance de l'instance de base de données cible. **Note** Pour les volumes SSD à usage général (gp2), vous bénéficiez de trois IOPS pour 1 Go de stockage. Allouez le stockage en calculant le nombre total d'IOPS en lecture et en écriture sur la base de données source.	DBA, SysAdmin

Tâche	Description	Compétences requises
Choisissez le type d'instance approprié en fonction des exigences de calcul.	1. Déterminez les exigences de calcul de l'instance de base de données cible. 2. Identifiez les problèmes de performance. 3. Tenez compte des facteurs permettant de déterminer le type d'instance approprié : • Utilisation du processeur de l'instance de base de données source • IOPS (lecture et écriture) pour l'instance de base de données source • Empreinte mémoire sur l'instance de base de données source	SysAdmin
Identifiez les exigences de sécurité d'accès au réseau.	1. Identifiez et documentez les exigences de sécurité d'accès au réseau pour vos bases de données source et cible. 2. Configurez les groupes de sécurité appropriés pour permettre à l'application de communiquer avec la base de données.	DBA, SysAdmin

Tâche	Description	Compétences requises
Identifiez la stratégie de migration des applications.	1. Déterminez et documente z la stratégie de transition vers la migration. 2. Déterminez et documente z l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO) de votre application, puis planifiez le passage en conséquence.	DBA, propriétaire de SysAdmin l'application

Tâche	Description	Compétences requises
Identifiez les risques liés à la migration.	Évaluez les risques et les mesures d'atténuation spécifiques à la migration des bases de données et des documents. Par exemple : • Identifiez les tables sans journalisation et mettez en évidence le risque de perte de données en cas de restauration. • Extrayez les utilisateurs et les privilèges de la base de données source, et mettez en évidence les conflits avec les privilèges Amazon RDS. • Consultez le journal des alertes pour détecter les erreurs et les avertisse ments spécifiques à Oracle. • Identifiez les fonctionnalités prises en charge et non prises en charge de l'instanc e de base de données cible. • Passez en revue les fonctionnalités obsolètes du moteur de version de base de données cible.	DBA

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un VPC.	Créez un nouvel Amazon Virtual Private Cloud (Amazon VPC) pour l'instance de base de données cible.	SysAdmin
Créez des groupes de sécurité.	Créez un groupe de sécurité dans votre nouveau VPC pour autoriser les connexions entrantes vers l'instance de base de données.	SysAdmin
Créez une instance de base de données Amazon RDS for Oracle.	Créez l'instance de base de données cible avec le nouveau VPC et le nouveau groupe de sécurité, puis démarrez l'instance.	SysAdmin

Option 1 : utiliser des outils natifs d'Oracle ou des outils tiers pour migrer les données

Tâche	Description	Compétences requises
Préparez la base de données source.	1. Créez un répertoire Data Pump ou utilisez-en un existant. 2. Créez un utilisateur de migration et accordez les autorisations nécessaires pour effectuer l'extrait de Data Pump. 3. Extrayez les rôles, les utilisateurs et les tablespaces de la base de données	DBA, SysAdmin

Tâche	Description	Compétences requises
	source sous forme de script SQL. 4. Transférez le dump Data Pump extrait vers le `data pump` répertoire de l'instance de base de données cible.	

Tâche	Description	Compétences requises
Préparez la base de données cible.	1. Vérifiez que toutes les options de base de données (par exemple, texte et Java) sont installées ou activées sur l'instance de base de données Amazon RDS for Oracle cible. 2. Créez un répertoire Data Pump ou utilisez-en un existant. 3. Créez un utilisateur de migration et accordez les autorisations nécessaires pour effectuer l'importation de Data Pump. 4. Créez les tablespaces, les utilisateurs et les rôles requis sur l'instance de base de données cible. 5. Importez le dump d'exportation Data Pump transféré dans la base de données cible. 6. Créez tous les index exclus lors de l'importation ou de la création d'objets. 7. Créez toutes les contraintes exclues lors de l'importation. 8. Validez ou recompilez les objets non valides.	DBA, SysAdmin

Tâche	Description	Compétences requises
	9. Reconstruisez les index non valides. 10. Validez le nombre d'objets de base de données entre les bases de données source et cible. 11. Résolvez les écarts constatés entre le nombre d'objets.	

Option 2 - Utiliser AWS DMS pour migrer les données

Tâche	Description	Compétences requises
Préparez les données.	1. Nettoyez les données de la base de données source. 2. Créez une instance de réplication. 3. Créez un point de terminaison source et un point de terminaison cible. 4. Identifiez le nombre de tables et d'objets à migrer.	DBA
Migrez les données.	1. Supprimez les contraintes et les déclencheurs de clé étrangère sur la base de données cible. 2. Supprimez les index secondaires de la base de données cible. 3. Configurez les paramètres des tâches de chargemen	DBA

Tâche	Description	Compétences requises
	t complet d'AWS DMS de la base de données source vers la base de données cible. 4. Activez les clés étrangères. 5. Permettez à AWS DMS CDC de répliquer les modifications en cours. 6. Activez les déclencheurs. 7. Mettez à jour les séquences . 8. Validez les données source et cible.	

Passez à la base de données cible

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.	1. Arrêtez tous les services applicatifs et les connexions clients pointant vers Oracle. 2. Exécutez les tâches AWS DMS. 3. Configurez une tâche de restauration (par exemple, inversez le CDC de la base de données Amazon RDS vers la base de données Oracle locale). 4. Validez les données. 5. Démarrez les services d'application sur la nouvelle	DBA, propriétaire de SysAdmin l'application

Tâche	Description	Compétences requises
	base de données cible en configurant Amazon Route 53 sur la nouvelle instance de base de données Amazon RDS for Oracle. 6. Ajoutez Amazon CloudWatch Monitoring à votre nouvelle instance de base de données Amazon RDS for Oracle.	
Mettez en œuvre votre plan de rollback.	1. Arrêtez tous les services d'application pointant vers l'instance de base de données Amazon RDS for Oracle. 2. Annulez les modifications apportées à la base de données Oracle source sur site à l'aide d'une tâche AWS DMS. 3. Arrêtez les tâches AWS DMS exécutées depuis la base de données Oracle sur site vers la base de données Amazon RDS for Oracle. 4. Reconfigurez les applications sur la base de données Oracle source. 5. Vérifiez que le déploiement de la restauration est terminé.	DBA, propriétaire de l'application

Clôturer le projet de migration

Tâche	Description	Compétences requises
Nettoyez les ressources.	Arrêtez ou supprimez les ressources AWS temporaires, telles que l'instance de réplication AWS DMS et le compartiment S3.	DBA, SysAdmin
Passez en revue les documents du projet.	Passez en revue vos documents et objectifs de planification de migration, puis confirmez que vous avez effectué toutes les étapes de migration requises.	DBA, propriétaire de SysAdmin l'application
Collectez des statistiques.	Enregistrez les principaux indicateurs de migration, notamment le temps nécessaire pour terminer la migration, le pourcentage de tâches manuelles par rapport aux tâches basées sur des outils, les économies de coûts et les autres indicateurs pertinents.	DBA, propriétaire de SysAdmin l'application
Clôturez le projet.	Clôturez le projet de migration et recueillez des commentaires sur les efforts déployés.	DBA, propriétaire de SysAdmin l'application

Ressources connexes

Références

- Migration de bases de données Oracle vers le cloud AWS (AWS Prescriptive Guidance)
- Service de migration de base de données AWS (documentation AWS DMS)

- Tarification Amazon RDS (documentation Amazon RDS)

Tutoriels et vidéos

- Mise en route avec AWS Database Migration Service (documentation AWS DMS)
- Ressources Amazon RDS (documentation Amazon RDS)
- Service de migration de base de données AWS (DMS) (YouTube)

Migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'Oracle Data Pump

Créée par Mohan Annam (AWS) et Brian Motzer (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Oracle d'un centre de données sur site vers une instance de base de données Amazon Relational Database Service (Amazon RDS) pour Oracle à l'aide d'Oracle Data Pump.

Le modèle implique la création d'un fichier de vidage de données à partir de la base de données source, le stockage du fichier dans un bucket Amazon Simple Storage Service (Amazon S3), puis la restauration des données sur une instance de base de données Amazon RDS for Oracle. Ce modèle est utile lorsque vous rencontrez des difficultés lors de l'utilisation d'AWS Database Migration Service (AWS DMS) pour la migration.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Les autorisations requises pour créer des rôles dans AWS Identity and Access Management (IAM) et pour un téléchargement partitionné sur Amazon S3
- Les autorisations requises pour exporter des données depuis la base de données source
- Interface de ligne de commande (AWS CLI) (AWS CLI) installée et configurée

Versions du produit

- Oracle Data Pump est uniquement disponible pour Oracle Database 10g version 1 (10.1) et versions ultérieures.

Architecture

Pile technologique source

- Bases de données Oracle sur site

Pile technologique cible

- Amazon RDS for Oracle
- Client SQL (développeur Oracle SQL)
- Compartiment S3

Architecture source et cible

Outils

Services AWS

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser. Dans ce modèle, IAM est utilisé pour créer les rôles et les politiques nécessaires à la migration des données d'Amazon S3 vers Amazon RDS for Oracle.
- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le cloud AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Oracle Data Pump vous aide à déplacer des données et des métadonnées d'une base de données à une autre à grande vitesse. Dans ce modèle, Oracle Data Pump est utilisé pour exporter le fichier de vidage de données (.dmp) vers le serveur Oracle et pour l'importer dans Amazon RDS for Oracle. Pour plus d'informations, consultez la section Importation de données dans Oracle sur Amazon RDS dans la documentation Amazon RDS.
- Oracle SQL Developer est un environnement de développement intégré qui simplifie le développement et la gestion des bases de données Oracle dans les déploiements traditionnels et basés sur le cloud. Il interagit à la fois avec la base de données Oracle sur site et avec Amazon RDS for Oracle pour exécuter les commandes SQL nécessaires à l'exportation et à l'importation de données.

Épopées

Création d’un compartiment S3

Tâche	Description	Compétences requises
Créer le compartiment.	Pour créer le compartiment S3, suivez les instructions de la documentation AWS.	Administrateur système AWS

Création du rôle IAM et attribution de politiques

Tâche	Description	Compétences requises
Configurez les autorisations IAM.	Pour configurer les autorisations, suivez les instructions de la documentation AWS.	Administrateur système AWS

Créez l'instance de base de données Amazon RDS for Oracle cible et associez le rôle d'intégration Amazon S3

Tâche	Description	Compétences requises
Créez l'instance de base de données Amazon RDS for Oracle cible.	Pour créer l'instance Amazon RDS for Oracle, suivez les instructions de la documentation AWS.	Administrateur système AWS
Associez le rôle à l'instance de base de données.	Pour associer le rôle à l'instance, suivez les instructions de la documentation AWS.	DBA

Création de l'utilisateur de base de données sur la base de données cible

Tâche	Description	Compétences requises

Créez l'utilisateur.	Connectez-vous à la base de données Amazon RDS for Oracle cible depuis Oracle SQL Developer ou SQL*Plus, puis exécutez la commande SQL suivante pour créer l'utilisateur dans lequel importer le schéma.
	`create user SAMPLE_SCHEMA identified by <PASSWORD>;`
	`grant create session, resource to <USER NAME>;`
	`alter user <USER NAME> quota 100M on users;`
		DBA

Créez le fichier d'exportation à partir de la base de données Oracle source

Tâche	Description	Compétences requises

Créez un fichier de vidage de données.	Pour créer un fichier de vidage nommé `sample.dmp` dans le `DATA_PUMP_DIR` répertoire d'exportation de l'`SAMPLE_SCHEMA` utilisateur, utilisez le script suivant.
	`DECLARE`
	`hdnl NUMBER;`
	`BEGIN`
		DBA

Tâche	Description	Compétences requises

	`hdnl := dbms_datapump.open(operation => 'EXPORT', job_mode => 'SCHEMA', job_name => NULL);`
	
	`dbms_datapump.add_file( handle => hdnl, filename => 'sample.dmp', directory => 'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_dump_file);`
	
	`dbms_datapump.add_file(handle => hdnl, filename => 'export.log', directory => 'DATA_PUMP_DIR', filetype => dbms_datapump.ku$_file_type_log_file);`
	
	`dbms_datapump.metadata_filter(hdnl, 'SCHEMA_EXPR', 'IN (''SAMPLE_SCHEMA'')');`	

Tâche	Description	Compétences requises

	`dbms_datapump.start_job(hdnl);`
	`END;`
	`/`
	
	Vérifiez les détails de l'exportation en consultant le `export.log` fichier dans votre `DATA_PUMP_DIR` répertoire local.	

Téléchargez le fichier de vidage dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le fichier de vidage de données de la source vers le compartiment S3.	À l'aide de l'AWS CLI, exécutez la commande suivante. `aws s3 cp sample.dmp s3://<bucket_created_epic_1>/`	DBA

Téléchargez le fichier d'exportation depuis le compartiment S3 vers l'instance RDS

Tâche	Description	Compétences requises
Téléchargez le fichier de vidage de données sur Amazon RDS	Pour copier le fichier `sample.dmp` de vidage du compartiment S3 vers la base de données Amazon RDS for Oracle, exécutez la commande SQL suivante. Dans cet exemple, le	Administrateur système AWS

Tâche	Description	Compétences requises

	`sample.dmp` fichier est téléchargé depuis le compartiment S3 `my-s3-integration1` vers le répertoire Oracle`DATA_PUMP_DIR` . Assurez-vous que l'espace disque alloué à votre instance RDS est suffisant pour accueillir à la fois la base de données et le fichier d'exportation.
	
	`-- If you want to download all the files in the S3 bucket remove the p_s3_prefix line.`
	
	`SELECT rdsadmin.rdsadmin_s3_tasks.download_from_s3( p_bucket_name => 'my-s3-integration', p_s3_prefix => 'sample.dmp', p_directory_name => 'DATA_PUMP_DIR') AS TASK_ID FROM DUAL;`
	
	La commande précédente génère un identifiant de tâche. Pour vérifier l'état du téléchargement en consultant les données contenues dans l'ID de tâche, exécutez la commande suivante.	

Tâche	Description	Compétences requises

	`SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('BDUMP','dbtask-<task_id>.log'));`
	
	Pour voir les fichiers du `DATA_PUMP_DIR` répertoire, exécutez la commande suivante.
	
	`SELECT filename, type,filesize/1024/1024 size_megs ,to_char(mtime,'DD-MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => upper('DATA_PUMP_DIR'))) order by 4;`	

Importez le fichier de vidage dans la base de données cible

Tâche	Description	Compétences requises
Restaurez le schéma et les données sur Amazon RDS.	Pour importer le fichier de vidage dans le schéma `sample_schema` de base de données, exécutez la commande SQL suivante depuis SQL Developer ou SQL*Plus.	DBA

Tâche	Description	Compétences requises
	`DECLARE hdnl NUMBER; BEGIN hdnl := DBMS_DATA PUMP.OPEN(operation => 'IMPORT', job_mode => 'SCHEMA', job_name= >null); DBMS_DATAPUMP.ADD_ FILE(handle => hdnl, filename => 'sample.d mp', directory => 'DATA_PUMP_DIR', filetype => dbms_data pump.ku$_file_type _dump_file); DBMS_DATAPUMP.ADD_FILE (handle => hdnl, filename => 'import.l og', directory => 'DATA_PUMP_DIR', filetype => dbms_data pump.ku$_file_type _log_file); DBMS_DATAPUMP. METADATA_FILTER(hd nl,'SCHEMA_EXPR',' IN (''SAMPLE_SCHEMA'')'); DBMS_DATAPUMP.START_J OB(hdnl); END; /`	

Tâche	Description	Compétences requises
	Pour consulter le fichier journal de l'importation, exécutez la commande suivante. `SELECT text FROM table(rdsadmin.rds_file_util.read_text_file('DATA_PUMP_DIR','import.log'));`	

Supprimez le fichier de vidage du répertoire DATA_PUMP_DIR

Tâche	Description	Compétences requises

Répertoriez et nettoyez les fichiers d'exportation.	Répertoriez et supprimez les fichiers d'exportation dans le `DATA_PUMP_DIR` répertoire, exécutez les commandes suivantes.
	`-- List the files SELECT filename, type,filesize/1024/1024 size_megs,to_char(mtime,'DD-MON-YY HH24:MI:SS') timestamp FROM TABLE(rdsadmin.rds_file_util.listdir(p_directory => upper('DATA_PUMP_DIR'))) order by 4;`
	`-- Remove the files`
		Administrateur système AWS

Tâche	Description	Compétences requises
	`EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','sample.dmp');` `EXEC UTL_FILE.FREMOVE('DATA_PUMP_DIR','import.log');`	

Ressources connexes

- Intégration avec Amazon S3
- Création d'une instance de base de données
- Importation de données dans Oracle sur Amazon RDS
- Documentation Amazon S3
- Documentation IAM
- Documentation Amazon RDS
- Documentation Oracle Data Pump
- Oracle SQL Developer

Migrez de PostgreSQL sur EC2 Amazon vers Amazon RDS pour PostgreSQL à l'aide de pglogical

Créée par Rajesh Madiwale (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration d'une base de données PostgreSQL (version 9.5 et ultérieure) d'Amazon Elastic Compute Cloud (Amazon) vers Amazon Relational Database Service (EC2Amazon RDS) pour PostgreSQL à l'aide de l'extension pglogical PostgreSQL. Amazon RDS prend désormais en charge l'extension pglogical pour PostgreSQL version 10.

Conditions préalables et limitations

Prérequis

- Choisissez le bon type d'instance Amazon RDS. Pour plus d'informations, consultez la section Types d'instances Amazon RDS.
- Assurez-vous que les versions source et cible de PostgreSQL sont identiques.
- Installez et intégrez l'extension pglogical à PostgreSQL sur Amazon. EC2

Versions du produit

- PostgreSQL version 10 et versions ultérieures sur Amazon RDS, avec les fonctionnalités prises en charge par Amazon RDS (voir PostgreSQL sur Amazon RDS dans la documentation AWS). Ce modèle a été testé lors de la migration de PostgreSQL 9.5 vers PostgreSQL version 10 sur Amazon RDS, mais il s'applique également aux versions ultérieures de PostgreSQL sur Amazon RDS.

Architecture

Architecture de migration des données

Outils

- extension pglogical
- utilitaires natifs de PostgreSQL : pg_dump et pg_restore

Épopées

Migrer les données à l'aide de l'extension pglogical

Tâche	Description	Compétences requises
Créez une instance de base de données Amazon RDS PostgreSQL.	Configurez une instance de base de données PostgreSQL dans Amazon RDS. Pour obtenir des instructions, consultez la documentation Amazon RDS for PostgreSQL.	DBA
Obtenez un dump de schéma à partir de la base de données PostgreSQL source et restaurez-le dans la base de données PostgreSQL cible.	1. Utilisez l'utilitaire pg_dump avec l'`-s`option permettant de générer un fichier de schéma à partir de la base de données source. 2. Utilisez l'utilitaire psql avec l'`-f`option permettant de charger le schéma dans la base de données cible.	DBA
Activez le décodage logique.	Dans le groupe de paramètres de base de données Amazon RDS, définissez le paramètre `rds.logical_replication` statique sur 1. Pour obtenir des instructions, consultez la documentation Amazon RDS.	DBA
Créez l'extension pglogical sur les bases de données source et cible.	1. Créez l'`pglogical` extension sur la base de données PostgreSQL source :	DBA

Tâche	Description	Compétences requises

	`psql -h <amazon-ec2-endpoint> -d target-dbname -U target-dbuser -c "create extension pglogical ;"`
	2. Créez l'`pglogical` extension sur la base de données PostgreSQL cible :
	`psql -h <amazon-rds-endpoint> -d source-dbname -U source-dbuser -c "create extension pglogical ;"`	

Créez un éditeur sur la base de données PostgreSQL source.	Pour créer un éditeur, exécutez : `psql -d dbname -p 5432 <<EOF SELECT pglogical .create_node( node_name := 'provider1', dsn := 'host=<ec2-endpoint> port=5432 dbname=source-dbname user=source-dbuser' ); EOF`	DBA

Tâche	Description	Compétences requises

Créez un ensemble de réplication, ajoutez des tables et des séquences.	Pour créer un jeu de réplication dans la base de données PostgreSQL source et pour ajouter des tables et des séquences au jeu de réplication, exécutez :
	`psql -d dbname -p 5432 <<EOF`
	`SELECT pglogical.replication_set_add_all_tables('default', '{public}'::text[],synchronize_data := true);`
	`EOF`
		DBA

Créez un abonné.	Pour créer un abonné sur la base de données PostgreSQL cible, exécutez :
	`psql -h <rds-endpoint> -d target-dbname -U target-dbuser <<EOF`
	`SELECT pglogical.create_node(`
	`node_name := 'subscriber1',`
	`dsn := 'host=<rds-endpoint> port=5432 dbname=target-dbname password=postgres user=target-dbuser'`
	`);`
	`EOF`
		DBA

Tâche	Description	Compétences requises
Créez un abonnement.	Pour créer un abonnement sur la base de données PostgreSQL cible, exécutez : `psql -h <rds-endpoint> -d target -U postgres <<EOF SELECT pglogical.create_subscription( subscription_name := 'subscription1', replication_sets := array['default'], provider_dsn := 'host=<ec2-endpoint> port=5432 dbname=<source-dbname> password=<password> user=source-dbuser' );`	DBA

Validez vos données

Tâche	Description	Compétences requises
Vérifiez les bases de données source et cible.	Vérifiez les bases de données source et cible pour vous assurer que les données sont correctement répliquées. Vous pouvez effectuer une validation `select count(1)` de base en utilisant les tables source et cible.	DBA

Ressources connexes

- Amazon RDS
- Réplication logique pour PostgreSQL sur Amazon RDS (documentation Amazon RDS)
- pglogical (GitHub dépôt)
- Limites de pglogical (fichier README GitHub du dépôt)
- Migration de PostgreSQL sur site ou d'Amazon vers Amazon RDS EC2 à l'aide de la réplication logique (blog de base de données AWS)

Migrer une base de données PostgreSQL locale vers Aurora PostgreSQL

Créée par Baji Shaik (AWS) et Jitender Kumar (AWS)

Récapitulatif

L'édition compatible avec Amazon Aurora PostgreSQL associe les performances et la disponibilité des bases de données commerciales haut de gamme à la simplicité et à la rentabilité des bases de données open source. Aurora offre ces avantages en étendant le stockage sur trois zones de disponibilité dans la même région AWS et en prenant en charge jusqu'à 15 instances de réplication en lecture pour augmenter les charges de travail de lecture et fournir une haute disponibilité au sein d'une même région. En utilisant une base de données globale Aurora, vous pouvez répliquer des bases de données PostgreSQL dans un maximum de cinq régions pour un accès en lecture à distance et une reprise après sinistre en cas de défaillance d'une région. Ce modèle décrit les étapes de migration d'une base de données source PostgreSQL locale vers une base de données compatible Aurora PostgreSQL. Le modèle inclut deux options de migration : à l'aide d'AWS Data Migration Service (AWS DMS) ou à l'aide d'outils PostgreSQL natifs (tels que pg_dump, pg_restore et psql) ou d'outils tiers.

Les étapes décrites dans ce modèle s'appliquent également aux bases de données PostgreSQL cibles sur les instances Amazon Relational Database Service (Amazon RDS) et Amazon Elastic Compute Cloud (Amazon). EC2

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source PostgreSQL dans un centre de données sur site
- Une instance de base de données compatible avec Aurora PostgreSQL ou une instance de base de données Amazon RDS for PostgreSQL

Limites

- Les limites de taille des bases de données sont de 64 To pour Amazon RDS pour PostgreSQL et de 128 To pour les bases de données compatibles avec Aurora PostgreSQL.
- Si vous utilisez l'option de migration AWS DMS, consultez les limites d'AWS DMS relatives à l'utilisation d'une base de données PostgreSQL comme source.

Versions du produit

- Pour la prise en charge des versions majeures et mineures de PostgreSQL dans Amazon RDS, consultez les mises à jour d'Amazon RDS for PostgreSQL dans la documentation Amazon RDS.
- Pour la prise en charge de PostgreSQL dans Aurora, consultez les mises à jour d'Amazon Aurora PostgreSQL dans la documentation Aurora.
- Si vous utilisez l'option de migration AWS DMS, consultez les versions de PostgreSQL prises en charge dans la documentation AWS DMS.

Architecture

Pile technologique source

- Base de données PostgreSQL locale

Pile technologique cible

- Instance de base de données compatible avec Aurora PostgreSQL

Architecture de la source

Architecture cible

Architecture de migration des données

Utilisation d'AWS DMS

Utilisation des outils PostgreSQL natifs

Outils

- AWS Database Migration Service (AWS DMS) vous aide à migrer des magasins de données vers le cloud AWS ou entre des combinaisons de configurations cloud et sur site. Ce service prend en charge différentes sources et bases de données cibles. Pour plus d'informations sur la façon

de valider les versions et éditions des bases de données source et cible PostgreSQL prises en charge pour une utilisation avec AWS DMS, consultez la section Utilisation d'une base de données PostgreSQL comme source AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités.

- Les outils natifs de PostgreSQL incluent pg_dump, pg_restore et psql.

Épopées

Analyser la migration

Tâche	Description	Compétences requises
Validez les versions de base de données source et cible.	Si vous utilisez AWS DMS, assurez-vous que vous utilisez une version compatible de PostgreSQL.	DBA
Identifiez le type de stockage et les exigences en matière de capacité.	1. Calculez le stockage alloué à l'instance de base de données source. 2. Rassemblez les mesures de croissance historiques pour l'instance de base de données source. 3. Anticipez les prévision s de croissance futures pour l'instance de base de données cible. 4. Allouez le stockage en calculant le nombre total d'IOPS en lecture et en écriture sur la base de données source. Un volume SSD à usage général (gp2) fournit 3 IOPS pour chaque Go de stockage.	DBA, administrateur système

Tâche	Description	Compétences requises
Choisissez le type d'instance, la capacité, les fonctionnalités de stockage et les fonctionn alités réseau appropriés.	Déterminez les exigences de calcul de l'instance de base de données cible. Passez en revue les problèmes de performances connus susceptibles de nécessiter une attention supplémentaire. Tenez compte des facteurs suivants pour déterminer le type d'instance approprié : • Utilisation du processeur de l'instance de base de données source • IOPS (opérations de lecture et d'écriture) pour l'instance de base de données source • Empreinte mémoire sur l'instance de base de données source Pour plus d'informations, consultez les classes d'instanc e de base de données Aurora dans la documentation Aurora.	DBA, administrateur système
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.	Déterminez les groupes de sécurité appropriés qui permettraient à l'application de communiquer avec la base de données.	DBA, administrateur système

Tâche	Description	Compétences requises
Identifiez la stratégie de migration des applications.	• Déterminez la stratégie de migration en fonction de la complexité de votre application. • Déterminez l'objectif de temps de restauration (RTO) et l'objectif de point de restauration (RPO) pour l'application, et planifiez le passage en conséquence.	DBA, propriétaire de l'application, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créez un VPC.	Créez un nouveau cloud privé virtuel (VPC) pour l'instance de base de données cible.	Administrateur de systèmes
Créez des groupes de sécurité.	Créez un groupe de sécurité au sein du VPC (comme indiqué dans l'épopée précédente) pour autoriser les connexions entrantes à l'instance de base de données.	Administrateur de systèmes
Configurez et démarrez le cluster de base de données Aurora.	Créez l'instance de base de données cible avec le nouveau VPC et le nouveau groupe de sécurité, puis démarrez l'instance.	Administrateur de systèmes

Migrer les données – option 1 (à l'aide d'AWS DMS)

Tâche	Description	Compétences requises
Effectuez les étapes préalables à la migration.	1. Nettoyez les données de la base de données source. 2. Créez une instance de réplication. 3. Créez des points de terminaison source et cible. 4. Identifiez le nombre de tables et d'objets disponibles à migrer.	DBA
Terminez les étapes de migration.	1. Supprimez les contraintes et les déclencheurs de clé étrangère sur la base de données cible. 2. Supprimez les index secondaires de la base de données cible. 3. Utilisez une tâche de chargement complet pour migrer les données de la base de données source vers la base de données cible. 4. Activez les clés étrangères. 5. Si vous utilisez la migration instantanée et que votre application nécessite un temps d'arrêt minimal, activez la capture des données relatives aux modifications (CDC) pour	DBA

Tâche	Description	Compétences requises
	répliquer les modifications en cours 6. Activez les déclencheurs. 7. Mettez à jour les séquences . 8. Validez les données source et cible.	
Validez les données.	Pour vous assurer que vos données ont été migrées correctement de la source vers la cible, suivez les étapes de validation des données décrites dans la documenta tion AWS DMS.	DBA

Migrer les données – option 2 (en utilisant pg_dump et pg_restore)

Tâche	Description	Compétences requises
Préparez la base de données source.	1. Créez un répertoire pour stocker la sauvegarde pg_dump si elle n'existe pas déjà. 2. Créez un utilisateur de migration autorisé à exécuter pg_dump sur des objets de base de données. 3. Connectez-vous à l' EC2 instance et exécutez la sauvegarde pg_dump.	DBA

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la documentation pg_dump et la procédure pas à pas dans la documentation AWS DMS.	
Préparez la base de données cible.	1. Créez un utilisateur de migration autorisé à utiliser pg_restore sur les objets de base de données. 2. Importez le dump de la base de données à l'aide de pg_restore. Pour plus d'informations, consultez la documentation pg_restore et la procédure pas à pas dans la documentation AWS DMS.	DBA
Validez les données.	1. Comparez le nombre d'objets de base de données entre les bases de données source et cible. 2. Résolvez les écarts constatés entre le nombre d'objets.	DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.	Mettez en œuvre la stratégie de migration des applications	DBA, propriétaire de l'application, administrateur système

Tâche	Description	Compétences requises
	que vous avez créée dans le premier épisode épique.	

Passez à la base de données cible

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.	1. Arrêtez tous les services applicatifs et les connexions client qui pointent vers la base de données PostgreSQL locale. 2. Exécutez les tâches AWS DMS. 3. Configurez une tâche de restauration (inverse CDC de la base de données compatible Aurora PostgreSQL à la base de données PostgreSQL locale) si nécessaire. 4. Validez les données. 5. Démarrez les services d'application sur la nouvelle cible en configurant Amazon Route 53 sur la nouvelle instance de base de données compatible Aurora PostgreSQL. 6. Ajoutez la surveillance d'Amazon CloudWatch et de Performance Insights à votre nouvelle instance de	DBA, propriétaire de l'application, administrateur système

Tâche	Description	Compétences requises
	base de données compatibl e Aurora PostgreSQL.	
Si vous devez annuler la migration.	1. Arrêtez tous les services d'application qui pointent vers la base de données compatible Aurora PostgreSQL. 2. Annulez les modifications apportées à la base de données PostgreSQL locale source à l'aide de la tâche AWS DMS que vous avez créée dans l'article précédent. 3. Arrêtez les tâches AWS DMS exécutées depuis la base de données PostgreSQL locale vers la base de données compatibl e Aurora PostgreSQL. 4. Configurez l'application de manière à ce qu'elle pointe vers la base de données PostgreSQL locale source. 5. Vérifiez que tous les déploiements de restaurat ion sont terminés.	DBA, propriétaire de l'applica tion

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources.	Arrêtez les ressources AWS temporaires.	DBA, administrateur système
Validez les documents.	Passez en revue et validez les documents du projet.	DBA, propriétaire de l'application, administrateur système
Collectez des statistiques.	Collectez des indicateurs concernant le délai de migration, le pourcentage d'économies réalisées manuellement par rapport aux coûts liés aux outils, etc.	DBA, propriétaire de l'application, administrateur système
Fermez le projet.	Clôturez le projet et faites part de vos commentaires.	DBA, propriétaire de l'application, administrateur système

Ressources connexes

Références

- Service de migration de données AWS
- VPCs et Amazon Aurora
- Tarification d'Amazon Aurora
- Utilisation d'une base de données PostgreSQL comme source AWS DMS
- Comment créer une instance de réplication AWS DMS
- Comment créer des points de terminaison source et cible à l'aide d'AWS DMS

Ressources supplémentaires

- Commencer à utiliser AWS DMS
- Tutoriels sur la migration des step-by-step données
- Ressources Amazon Aurora

Migrer une base de données Microsoft SQL Server sur site vers Microsoft SQL Server sur Amazon EC2 exécutant Linux

Créée par Tirumala Dasari (AWS)

Récapitulatif

Ce modèle décrit comment migrer d'une base de données Microsoft SQL Server sur site exécutée sous Microsoft Windows vers Microsoft SQL Server sur une instance Linux Amazon Elastic Compute Cloud (Amazon EC2) à l'aide d'utilitaires de sauvegarde et de restauration.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- AMI Amazon EC2 Linux (Amazon Machine Image) avec Microsoft SQL Server
- AWS Direct Connect entre Windows sur site et Microsoft SQL Server sur l'instance Linux EC2

Architecture

Pile technologique source

- Base de données Microsoft SQL Server locale

Pile technologique cible

- EC2 Instance Linux avec une base de données Microsoft SQL Server

Architecture de migration de base de données

Outils

- WinSCP - Cet outil permet aux utilisateurs de Windows de partager facilement des fichiers avec des utilisateurs de Linux.
- Sqlcmd - Cet utilitaire de ligne de commande vous permet d'envoyer des instructions ou des lots T-SQL à des instances locales et distantes de SQL Server. Cet utilitaire est extrêmement utile pour les tâches de base de données répétitives telles que le traitement par lots ou les tests unitaires.

Épopées

Préparation de l'instance EC2 Linux avec SQL Server

Tâche	Description	Compétences requises
Sélectionnez une AMI qui fournit le système d'exploit ation Linux et inclut Microsoft SQL Server.		Administrateur système
Configurez l'AMI pour créer une EC2 instance.		Administrateur système
Créez des règles entrantes et sortantes pour les groupes de sécurité.		Administrateur système
Configurez l' EC2 instance Linux pour une base de données Microsoft SQL Server.		DBA
Créez des utilisateurs et accordez des autorisations comme dans la base de données source.		Propriétaire, DBA
Installez les outils SQL Server et l'utilitaire sqlcmd sur l'instance Linux. EC2		DBA

Sauvegardez la base de données et déplacez le fichier de sauvegarde vers une EC2 instance Linux

Tâche	Description	Compétences requises
Sauvegardez la base de données SQL Server locale.		DBA

Tâche	Description	Compétences requises
Installez WinSCP sur Microsoft SQL Server.		DBA
Déplacez le fichier de sauvegarde vers l' EC2 instance Linux exécutant Microsoft SQL Server.		DBA

Restaurez la base de données sur une EC2 instance Linux exécutant SQL Server

Tâche	Description	Compétences requises
Restaurez la base de données à partir du fichier de sauvegarde de la base de données à l'aide de l'utilitaire sqlcmd.		DBA
Validez les objets et les données de base de données.		Développeur, ingénieur de test

Passer de Windows SQL Server à une EC2 instance Windows SQL Server sur Linux

Tâche	Description	Compétences requises
Validez les objets et les données de base de données.		Développeur, ingénieur de test
Passez de la base de données Microsoft SQL Server locale à l' EC2 instance Linux exécutant Microsoft SQL Server.		DBA

Ressources connexes

- Comment configurer SQL Server 2017 sur Amazon Linux et Ubuntu AMIs
- Installation d'outils SQL sur une instance Linux
- Backup et restauration depuis une base de données Microsoft SQL Server locale vers Microsoft SQL Server sur une instance Linux EC2

Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de serveurs liés

Créée par Kevin Yung (AWS), Vishal Singh (AWS) et Viqash Adwani (AWS)

Récapitulatif

Les serveurs liés permettent à Microsoft SQL Server d'exécuter des instructions SQL sur d'autres instances de serveurs de base de données. Ce modèle décrit comment vous pouvez migrer votre base de données Microsoft SQL Server locale vers Amazon Relational Database Service (Amazon RDS) pour Microsoft SQL Server afin de réduire les coûts et d'augmenter la disponibilité. Actuellement, Amazon RDS pour Microsoft SQL Server ne prend pas en charge les connexions en dehors d'un réseau Amazon Virtual Private Cloud (Amazon VPC).

Vous pouvez utiliser ce modèle pour atteindre les objectifs suivants :

- Migrer Microsoft SQL Server vers Amazon RDS pour Microsoft SQL Server sans interrompre les fonctionnalités du serveur lié.
- Prioriser et migrer Microsoft SQL Server lié en différentes vagues.

Conditions préalables et limitations

Prérequis

- Vérifiez si Microsoft SQL Server sur Amazon RDS prend en charge les fonctionnalités dont vous avez besoin.
- Assurez-vous que vous pouvez utiliser Amazon RDS pour Microsoft SQL Server avec des classements par défaut ou des classements définis par rapport aux niveaux de base de données.

Architecture

Pile technologique source

- Bases de données locales (Microsoft SQL Server)

Pile technologique cible

- Amazon RDS for SQL Server

Architecture de l'état source

Architecture de l'état cible

Dans l'état cible, vous migrez Microsoft SQL Server vers Amazon RDS for Microsoft SQL Server à l'aide de serveurs liés. Cette architecture utilise un Network Load Balancer pour transférer le trafic d'Amazon RDS pour Microsoft SQL Server vers des serveurs sur site exécutant Microsoft SQL Server. Le schéma suivant montre la fonctionnalité de proxy inverse pour le Network Load Balancer.

Outils

- AWS CloudFormation
- Network Load Balancer
- Amazon RDS pour SQL Server dans plusieurs zones de disponibilité (AZsmulti-zones)
- Service de migration de base de données AWS (AWS DMS)

Épopées

Création d'une zone d'atterrissage (VPC)

Tâche	Description	Compétences requises
Créez l'allocation CIDR.		AWS SysAdmin
Créer un cloud privé virtuel (VPC)		AWS SysAdmin
Créez les sous-réseaux VPC.		AWS SysAdmin

Tâche	Description	Compétences requises
Créez les listes de contrôle d'accès aux sous-réseaux (ACLs).		AWS SysAdmin
Créez les tables de routage des sous-réseaux.		AWS SysAdmin
Créez une connexion avec AWS Direct Connect ou le réseau privé virtuel (VPN) AWS.		AWS SysAdmin

Migrer la base de données vers Amazon RDS

Tâche	Description	Compétences requises
Créez une instance de base de données Amazon RDS pour Microsoft SQL Server.		AWS SysAdmin
Créez une instance de réplication AWS DMS.		AWS SysAdmin
Créez les points de terminaison de base de données source et cible dans AWS DMS.		AWS SysAdmin
Créez la tâche de migration et définissez la réplication continue sur ON après un chargement complet.		AWS SysAdmin
Demandez une modification du pare-feu afin de permettre à Amazon RDS for Microsoft		AWS SysAdmin

Tâche	Description	Compétences requises
SQL Server d'accéder aux bases de données SQL Server locales.		
Créez un Network Load Balancer.		AWS SysAdmin
Créez un groupe cible qui cible les serveurs de base de données de votre centre de données	Nous vous recommandons d'utiliser des noms d'hôte dans la configuration cible pour intégrer les événements de basculement du centre de données (DC).	AWS SysAdmin
Exécutez l'instruction SQL pour la configuration du serveur lié.	Exécutez les instructions SQL pour ajouter un serveur lié à l'aide de l'outil de gestion Microsoft SQL sur l'instance de base de données Amazon RDS for Microsoft SQL Server. Dans l'instruction SQL, définissez @datasrc pour qu'il utilise le nom d'hôte Network Load Balancer. Ajoutez des informations de connexion au serveur liées en utilisant l'outil de gestion Microsoft SQL sur l'instance de base de données Amazon RDS for Microsoft SQL Server.	AWS SysAdmin
Testez et validez les fonctions de SQL Server.		AWS SysAdmin
Créez un découpage.		AWS SysAdmin

Ressources connexes

- Tâches de gestion courantes pour Microsoft SQL Server sur Amazon RDS
- Collations et jeux de caractères pour Microsoft SQL Server
- Documentation sur le Network Load Balancer
- Implémenter des serveurs liés avec Amazon RDS pour Microsoft SQL Server (article de blog)

Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de méthodes de sauvegarde et de restauration natives

Créée par Tirumala Dasari (AWS), David Queiroz (AWS) et Vishal Singh (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Microsoft SQL Server sur site vers une instance de base de données Amazon Relational Database Service (Amazon RDS) pour SQL Server (migration homogène). Le processus de migration est basé sur les méthodes de sauvegarde et de restauration natives de SQL Server. Il utilise SQL Server Management Studio (SSMS) pour créer un fichier de sauvegarde de base de données et un bucket Amazon Simple Storage Service (Amazon S3) pour stocker le fichier de sauvegarde avant de le restaurer dans Amazon RDS for SQL Server.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Politiques de rôle AWS Identity and Access Management (IAM) pour accéder au compartiment S3 et à l'instance de base de données Amazon RDS for SQL Server.

Limites

- Le processus décrit dans ce modèle migre uniquement la base de données. Les connexions SQL ou les utilisateurs de base de données, y compris les tâches de l'agent SQL Server, ne sont pas migrés car ils nécessitent des étapes supplémentaires.

Versions du produit

- SQL Server 2012-2017. Pour obtenir la dernière liste des versions et fonctionnalités prises en charge, consultez Microsoft SQL Server sur Amazon RDS dans la documentation AWS.

Architecture

Pile technologique source

- Une base de données Microsoft SQL Server sur site

Pile technologique cible

- Instance de base de données Amazon RDS pour SQL Server

Architecture de migration des données

Outils

- Microsoft SQL Server Management Studio (SSMS) est un environnement intégré de gestion de l'infrastructure SQL Server. Il fournit une interface utilisateur et un groupe d'outils dotés d'éditeurs de script riches qui interagissent avec SQL Server.

Épopées

Création d'une instance de base de données Amazon RDS for SQL Server

Tâche	Description	Compétences requises
Sélectionnez SQL Server comme moteur de base de données dans Amazon RDS for SQL Server.		DBA
Choisissez l'édition SQL Server Express.		DBA
Spécifiez les informations de base de données.	Pour plus d'informations sur la création d'une instance de base de données, consultez la documentation Amazon RDS.	DBA, propriétaire de l'application

Création d'un fichier de sauvegarde à partir de la base de données SQL Server locale

Tâche	Description	Compétences requises
Connectez-vous à la base de données SQL Server locale via SSMS.		DBA
Créez une sauvegarde de la base de données.	Pour obtenir des instructions, consultez la documentation SSMS.	DBA, propriétaire de l'application

Chargez le fichier de sauvegarde sur Amazon S3

Tâche	Description	Compétences requises
Créez un compartiment dans Amazon S3.	Pour plus d'informations, consultez la documentation Amazon S3.	DBA
Téléchargez le fichier de sauvegarde dans le compartiment S3.	Pour plus d'informations, consultez la documentation Amazon S3.	SysOps administrateur

Restaurez la base de données dans Amazon RDS for SQL Server

Tâche	Description	Compétences requises
Ajoutez le groupe d'options à Amazon RDS.	1. Ouvrez la console Amazon RDS à l'adresse https://console.aws.amazon.com/rds/. 2. Dans le volet de navigation, choisissez Groupes d'options, puis Créer un groupe.	SysOps administrateur

Tâche	Description	Compétences requises
	3. Complétez les informations relatives au groupe d'options, puis choisissez Create. 4. Ajoutez l'`SQLSERVER_BACKUP_RESTORE` option au groupe d'options, puis choisissez Ajouter une option. Pour plus d'informations, consultez la documentation Amazon RDS.	
Restaurez la base de données.	1. Connectez-vous à Amazon RDS pour SQL Server via SSMS. 2. Appelez la procédure `msdb.dbo.rds_restore_database` stockée pour restaurer la base de données.	DBA

Valider la base de données cible

Tâche	Description	Compétences requises
Validez les objets et les données.	Validez les objets et les données entre la base de données source et Amazon RDS for SQL Server.	Propriétaire de l'application, DBA

Tâche	Description	Compétences requises
	Note Cette tâche fait uniquement migrer la base de données. Les connexions et les tâches ne seront pas migrées.	

Découper

Tâche	Description	Compétences requises
Redirigez le trafic des applications.	Après validation, redirigez le trafic de l'application vers l'instance de base de données Amazon RDS for SQL Server.	Propriétaire de l'application, DBA

Ressources connexes

- Documentation Amazon S3
- Documentation Amazon RDS pour SQL Server
- Options pour le moteur de base de données Microsoft SQL Server

Migrer une base de données Microsoft SQL Server vers Aurora MySQL à l'aide d'AWS DMS et d'AWS SCT

Créée par Mark Szalkiewicz (AWS) et Pavan Pusuluri (AWS)

Récapitulatif

Ce modèle décrit comment migrer une base de données Microsoft SQL Server sur site ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2) vers Amazon Aurora MySQL. Le modèle utilise AWS Database Migration Service (AWS DMS) et AWS Schema Conversion Tool (AWS SCT) pour la migration des données et la conversion de schéma.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source Microsoft SQL Server dans un centre de données local ou sur une instance EC2
- Pilotes de connectivité de base de données Java (JDBC) pour les connecteurs AWS SCT, installés sur une machine locale ou une instance sur EC2 laquelle AWS SCT est installé

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- Microsoft SQL Server 2008, 2008R2, 2012, 2014, 2016 et 2017 pour les éditions Enterprise, Standard, Workgroup et Developer. Les éditions Web et Express ne sont pas prises en charge par AWS DMS. Pour obtenir la dernière liste des versions prises en charge, consultez Utilisation d'une base de données Microsoft SQL Server comme source pour AWS DMS. Nous vous recommandons d'utiliser la dernière version d'AWS DMS pour bénéficier du support le plus complet en termes de versions et de fonctionnalités. Pour plus d'informations sur les versions de Microsoft SQL Server prises en charge par AWS SCT, consultez la documentation AWS SCT.
- MySQL versions 5.5, 5.6 et 5.7. Pour obtenir la dernière liste des versions prises en charge, consultez Utilisation d'une base de données compatible MySQL comme cible pour AWS DMS.

Architecture

Pile technologique source

L'un des éléments suivants :

- Une base de données Microsoft SQL Server sur site
- Une base de données Microsoft SQL Server sur une EC2 instance

Pile technologique cible

- Aurora MySQL

Architecture de migration des données

- À partir d'une base de données Microsoft SQL Server exécutée dans le cloud AWS

- À partir d'une base de données Microsoft SQL Server exécutée dans un centre de données local

Outils

- AWS DMS - AWS Data Migration Service (AWS DMS) vous aide à migrer vos données vers et depuis des bases de données commerciales et open source largement utilisées, notamment Oracle, SQL Server, MySQL et PostgreSQL. Vous pouvez utiliser AWS DMS pour migrer vos données dans le cloud AWS, entre plusieurs instances sur site (via une configuration AWS Cloud) ou entre différentes combinaisons de configurations cloud et sur site.
- AWS SCT - AWS Schema Conversion Tool (AWS SCT) facilite les migrations de bases de données hétérogènes en convertissant automatiquement le schéma de base de données source et la majorité du code personnalisé dans un format compatible avec la base de données cible.

Épopées

Préparez-vous à la migration

Tâche	Description	Compétences requises
Validez la version et le moteur de la base de données source et cible.		DBA
Créez un groupe de sécurité sortant pour les bases de données source et cible.		SysAdmin
Créez et configurez une EC2 instance pour AWS SCT, si nécessaire.		DBA
Téléchargez la dernière version d'AWS SCT et des pilotes associés.		DBA
Ajoutez et validez les utilisateurs et les autorisations requis dans la base de données source.		DBA
Créez un projet AWS SCT pour la charge de travail et connectez-vous à la base de données source.		DBA
Générez un rapport d'évaluation et évaluez la faisabilité.		DBA

Préparation de la base de données cible

Tâche	Description	Compétences requises
Créez une instance de base de données Amazon RDS cible en utilisant Amazon Aurora comme moteur de base de données.		DBA
Extrayez la liste des utilisateurs, des rôles et des autorisations à partir de la source.		DBA
Mappez les utilisateurs de base de données existants aux nouveaux utilisateurs de base de données.		Propriétaire de l'application
Créez des utilisateurs dans la base de données cible.		DBA
Appliquez les rôles de l'étape précédente à la base de données cible.		DBA
Passez en revue les options de base de données, les paramètres, les fichiers réseau et les liens de base de données dans la base de données source, puis évaluez leur applicabilité à la base de données cible.		DBA
Appliquez tous les paramètres pertinents à la cible.		DBA

Transférer des objets

Tâche	Description	Compétences requises
Configurez la connectivité AWS SCT à la base de données cible.		DBA
Convertissez le schéma à l'aide d'AWS SCT.	AWS SCT convertit automatiquement le schéma de base de données source et la majeure partie du code personnalisé dans un format compatible avec la base de données cible. Tout code que l'outil ne peut pas convertir automatiquement est clairement indiqué afin que vous puissiez le convertir vous-même.	DBA
Passez en revue le rapport SQL généré et enregistrez les erreurs et les avertissements éventuels.		DBA
Appliquez des modifications de schéma automatisées à la cible ou enregistrez-les sous forme de fichier .sql.		DBA
Vérifiez qu'AWS SCT a créé les objets sur la cible.		DBA
Réécrivez, rejetez ou redessinez manuellement tous les éléments dont la conversion automatique n'a pas échoué.		DBA

Tâche	Description	Compétences requises
Appliquez le rôle et les autorisations d'utilisateur générés et passez en revue les exceptions.		DBA

Migrer les données

Tâche	Description	Compétences requises
Déterminez la méthode de migration.		DBA
Créez une instance de réplication à partir de la console AWS DMS.	Pour obtenir des informations détaillées sur l'utilisation d'AWS DMS, consultez les liens de la section « Ressources associées ».	DBA
Créez les points de terminaison source et cible.		DBA
Créez une tâche de réplication.		DBA
Lancez la tâche de réplication et surveillez les journaux.		DBA

Migrer l'application

Tâche	Description	Compétences requises
Utilisez AWS SCT pour analyser et convertir les éléments SQL du code de l'application.	Lorsque vous convertissez votre schéma de base de données à partir d'un moteur à un autre, vous	Propriétaire de l'application

Tâche	Description	Compétences requises
	devez également mettre à jour le code SQL dans vos applications pour interagir avec le nouveau moteur de base de données au lieu de l'ancien. Vous pouvez afficher, analyser, modifier et enregistrer le code SQL converti. Pour obtenir des informations détaillées sur l'utilisation d'AWS SCT, consultez les liens de la section « Ressources associées ».	
Créez les nouveaux serveurs d'applications sur AWS.		Propriétaire de l'application
Migrez le code de l'application vers les nouveaux serveurs.		Propriétaire de l'application
Configurez le serveur d'applications pour la base de données cible et les pilotes.		Propriétaire de l'application
Corrigez tout code spécifique au moteur de base de données source de l'application.		Propriétaire de l'application
Optimisez le code de l'application pour le moteur cible.		Propriétaire de l'application

Découper

Tâche	Description	Compétences requises
Appliquez les nouveaux utilisateurs, les autorisations et les modifications de code à la cible.		DBA
Verrouillez l'application pour toute modification.		Propriétaire de l'application
Vérifiez que toutes les modifications ont été propagées à la base de données cible.		DBA
Pointez le nouveau serveur d'applications vers la base de données cible.		Propriétaire de l'application
Revérifiez tout.		Propriétaire de l'application
Passez en direct.		Propriétaire de l'application

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires (instance de réplication AWS DMS et EC2 instance utilisée pour AWS SCT).		DBA, propriétaire de l'application
Mettez à jour les commentaires sur le processus AWS		DBA, propriétaire de l'application

Tâche	Description	Compétences requises
DMS destinés aux équipes internes.		
Révisez le processus AWS DMS et améliorez le modèle si nécessaire.		DBA, propriétaire de l'application
Passez en revue et validez les documents du projet.		DBA, propriétaire de l'application
Collectez des indicateurs concernant le délai de migration, le pourcentage d'économies réalisées manuellement par rapport aux coûts liés aux outils, etc.		DBA, propriétaire de l'application
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de l'application

Ressources connexes

Références

- Guide de l'utilisateur d'AWS DMS
- Guide de l'utilisateur d'AWS SCT
- Tarification d'Amazon Aurora

Tutoriels et vidéos

- Commencer à utiliser AWS Database Migration Service
- Commencer à utiliser l'outil AWS Schema Conversion Tool
- Ressources Amazon RDS
- Procédures pas à pas d'AWS DMS Step-by-Step

Migrer une base de données MariaDB sur site vers Amazon RDS for MariaDB à l'aide d'outils natifs

Créée par Shyam Sunder Rakhecha (AWS)

Récapitulatif

Ce modèle fournit des conseils pour la migration d'une base de données MariaDB sur site vers Amazon Relational Database Service (Amazon RDS) pour MariaDB à l'aide d'outils natifs. Si des outils MySQL sont installés, vous pouvez utiliser mysql et mysqldump. Si des outils MariaDB sont installés, vous pouvez utiliser mariadb et mariadb-dump. Les outils MySQL et MariaDB ont la même origine, mais il existe des différences mineures entre les versions 10.6 et ultérieures de MariaDB.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une base de données source MariaDB dans un centre de données sur site

Limites

- Limite de taille de base de données : 64 To

Versions du produit

- Versions 10.0-10.6 de MariaDB (pour la dernière liste des versions prises en charge, consultez MariaDB sur Amazon RDS dans la documentation AWS)

Architecture

Pile technologique source

- Base de données MariaDB dans un centre de données sur site

Pile technologique cible

- Instance de base de données Amazon RDS pour MariaDB

Architecture cible

Architecture de migration des données

Outils

- Outils MySQL natifs : mysql et mysqldump
- Outils natifs de MariaDB : mariadb et mariadb-dump

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez les versions et les moteurs des bases de données source et cible.		DBA
Identifiez la configuration matérielle requise pour l'instance de serveur cible.		DBA, administrateur système
Identifiez les exigences de stockage (type et capacité de stockage).		DBA, administrateur système
Choisissez le type d'instanc e approprié en fonction de la capacité, des fonctionnalités de stockage et des fonctionn alités réseau.		DBA, administrateur système
Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.		DBA, administrateur système

Tâche	Description	Compétences requises
Identifiez la stratégie de migration des applications.		DBA, propriétaire de l'application, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)		Administrateur de systèmes
Créez des groupes de sécurité.		Administrateur de systèmes
Configurez et démarrez une instance de base de données Amazon RDS exécutant MariaDB.		Administrateur de systèmes

Migrer les données

Tâche	Description	Compétences requises
Utilisez des outils natifs pour migrer les objets et les données de base de données.	Dans la base de données source, utilisez mysqldump ou mariadb-dump pour créer un fichier de sortie contenant des objets et des données de base de données. Dans la base de données cible, utilisez mysql ou mariadb pour restaurer les données.	DBA
Validez les données.	Vérifiez les bases de données source et cible pour vous	DBA

Tâche	Description	Compétences requises
	assurer que la migration des données a bien été effectuée.	

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie de migration des applications.		DBA, propriétaire de l'application, administrateur système

Découper

Tâche	Description	Compétences requises
Basculez les clients de l'application vers la nouvelle infrastructure.		DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources AWS temporaires.		Administrateur de systèmes
Passez en revue et validez les documents du projet.		DBA, propriétaire de l'application, administrateur système
Collectez des indicateurs concernant le délai de migration, les économies réalisées grâce aux outils, etc.		DBA, propriétaire de l'application, administrateur système

Tâche	Description	Compétences requises
Clôturez le projet et faites part de vos commentaires.		DBA, propriétaire de l'application, administrateur système

Ressources connexes

Références Amazon RDS

- Amazon RDS for MariaDB
- Amazon Virtual Private Cloud VPCs et Amazon RDS
- Déploiements multi-AZ d'Amazon RDS
- Tarification d'Amazon RDS

Références MySQL et MariaDB

- mariadb-dump/mysqldump
- Client en ligne de commande mysql

Tutoriels et vidéos

- Getting Started with Amazon RDS (Démarrer avec Amazon RDS)

Migrer une base de données MySQL sur site vers Aurora MySQL

Créée par Igor Obradovic (AWS)

Récapitulatif

Ce modèle explique comment migrer une base de données source MySQL sur site vers Amazon Aurora MySQL Compatible Edition. Il décrit deux options de migration : using AWS Database Migration Service (AWS DMS) ou utiliser des outils MySQL natifs tels que mysqldbcopy et mysqldump.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une base de données MySQL source dans un centre de données sur site

Limites

- Limite de taille de base de données : 128 To

Versions du produit

- MySQL version 8.0 (Aurora MySQL version 3) est disponible dans le cadre du support standard.
- MySQL version 5.7 (Aurora MySQL version 2) est disponible dans le cadre d'un support étendu, moyennant des frais supplémentaires.

Pour obtenir la dernière liste des versions prises en charge, consultez les versions d'Amazon Aurora dans la AWS documentation. Si vous utilisez AWS DMS, consultez également Utiliser une base de données compatible MySQL comme cible pour les versions de AWS DMS MySQL prises en charge par. AWS DMS

Architecture

Pile technologique source

- Une base de données MySQL sur site

Pile technologique cible

- Amazon Aurora MySQL-Compatible Edition

Architecture cible

Les données Aurora sont stockées dans un volume de cluster, qui est un volume virtuel unique utilisant des disques SSD (SSDs). Un volume de cluster se compose de copies des données couvrant trois zones de disponibilité d'une même région AWS. Les données étant automatiquement répliquées entre les zones de disponibilité, elles sont extrêmement durables et réduisent les risques de perte de données.

Aurora divise automatiquement le volume de votre base de données en segments de 10 Go répartis sur de nombreux disques. Chaque segment de 10 Go de votre volume de base de données est répliqué de six manières, dans trois zones de disponibilité. Le schéma suivant illustre la relation entre le volume du cluster, l'instance de base de données du rédacteur et les instances de base de données du lecteur dans un cluster de base de données Aurora, et la séparation entre la capacité de calcul et le stockage. Pour plus d'informations sur cette architecture, consultez la documentation et la FAQ d'Aurora.

Architecture de migration des données

En utilisant AWS DMS :

Le schéma suivant illustre la migration d'une base de données MySQL locale vers un cluster compatible Aurora MySQL dans le, en utilisant. AWS Cloud AWS DMS

À l'aide des outils MySQL natifs :

Le schéma suivant illustre la migration d'une base de données MySQL locale vers un cluster compatible Aurora MySQL dans le, à l' AWS Cloud aide d'outils MySQL natifs tels que mysqldbcopy et mysqldump.

Outils

- AWS Database Migration Service (AWS DMS) prend en charge plusieurs moteurs de base de données source et cible. Pour plus d'informations sur les bases de données source et cible MySQL

prises en charge par AWS DMS, consultez la section Migration de bases de données compatibles MySQL vers. AWS Nous vous recommandons d'utiliser la dernière version de AWS DMS pour bénéficier de la prise en charge la plus complète possible des versions et des fonctionnalités.

- mysqldbcopy est un utilitaire MySQL qui copie une base de données MySQL sur un seul serveur ou entre plusieurs serveurs.
- mysqldump est un utilitaire MySQL qui crée un fichier dump à partir d'une base de données MySQL à des fins de sauvegarde ou de migration.

Épopées

Planifier la migration

Tâche	Description	Compétences requises
Validez la version et le moteur.	Validez la version et le moteur de base de données pour les bases de données source et cible.	DBA
Identifiez les exigences matérielles.	Identifiez la configuration matérielle requise pour l'instance de serveur cible.	DBA, administrateur système
Identifiez les besoins en matière de stockage.	Identifiez les exigences de stockage (type et capacité de stockage).	DBA, administrateur système
Choisissez le type d'instance.	Choisissez le type d'instance approprié en fonction de vos besoins en matière de calcul, de stockage et de réseau.	DBA, administrateur système
Déterminez les exigences de sécurité d'accès au réseau.	Identifiez les exigences de sécurité d'accès au réseau pour les bases de données source et cible.	DBA, administrateur système

Tâche	Description	Compétences requises
Déterminez la stratégie.	Identifiez la stratégie de migration des applications.	DBA, propriétaire de l'application, administrateur système

Configuration de l'infrastructure

Tâche	Description	Compétences requises
Créer un cloud privé virtuel (VPC)	Pour obtenir des instructions, consultez la section Créer un VPC dans la documentation Amazon Virtual Private Cloud (Amazon VPC).	Administrateur de systèmes
Créez des groupes de sécurité.	Pour obtenir des instructions, consultez la section Créer un groupe de sécurité pour votre VPC dans la documentation Amazon VPC.	Administrateur de systèmes
Configurez et démarrez un cluster de base de données compatible Aurora MySQL dans votre. Compte AWS	Pour obtenir des instructions, consultez la section Création d'un cluster de base de données Amazon Aurora dans la documentation Aurora.	Administrateur de systèmes

Migrer les données - option 1

Tâche	Description	Compétences requises
Utilisez des outils MySQL natifs ou des outils tiers pour migrer des objets et des données de base de données.	Pour obtenir des instructions, consultez la documentation des outils MySQL tels que mysqldbcopy et mysqldump.	DBA

Migrer les données - option 2

Tâche	Description	Compétences requises
Migrez les données avec AWS DMS.	Pour obtenir des instructions, consultez les sections Utilisation d'une base de données compatible MySQL comme source et Utilisation d'une base de données compatible MySQL comme cible dans la documentation. AWS DMS	DBA

Migrer l'application

Tâche	Description	Compétences requises
Suivez la stratégie.	Suivez la stratégie de migration des applications.	DBA, propriétaire de l'application, administrateur système

Découper

Tâche	Description	Compétences requises
Changez de client d'application.	Changez les clients de l'application pour qu'ils se connectent au nouveau point de terminaison du cluster Aurora.	DBA, propriétaire de l'application, administrateur système

Fermez le projet

Tâche	Description	Compétences requises
Arrêtez les ressources.	Arrêtez les AWS ressources temporaires.	DBA, administrateur système
Consultez la documentation.	Passez en revue et validez les documents du projet.	DBA, propriétaire de l'application, administrateur système
Collectez des métriques.	Collectez des indicateurs concernant le délai de migration, le pourcentage d'étapes manuelles par rapport à l'utilisation des outils, les économies de coûts, etc.	DBA, propriétaire de l'application, administrateur système
Projet de migration complet.	Clôturez le projet et faites part de vos commentaires.	Propriétaire de l'application, DBA, administrateur système

Ressources connexes

Références

- Migration des données vers le cluster de base de données Amazon Aurora MySQL
- AWS DMS website
- AWS DMS documentation
- Tarification d'Amazon Aurora
- Création et connexion à un cluster de base de données Aurora MySQL
- Amazon VPC et Amazon RDS
- Documentation Amazon Aurora

Tutoriels et vidéos

- Commencer avec AWS DMS
- Commencer à utiliser Amazon Aurora

Migrez des bases de données MySQL sur site vers Aurora MySQL à l'aide de Percona, XtraBackup Amazon EFS et Amazon S3

Créée par Rohan Jamadagni (AWS), Sajith Menon (AWS) et Udayasimha Theepireddy (AWS)

Récapitulatif

Ce modèle décrit comment migrer efficacement de grandes bases de données MySQL locales vers Amazon Aurora MySQL à l'aide de XtraBackup Percona. Percona XtraBackup est un utilitaire de sauvegarde open source non bloquant pour les serveurs basés sur MySQL. Le modèle montre comment utiliser Amazon Elastic File System (Amazon EFS) pour réduire le délai de chargement de la sauvegarde sur Amazon Simple Storage Service (Amazon S3) et pour restaurer la sauvegarde sur Amazon Aurora MySQL. Le modèle fournit également des détails sur la façon de réaliser des sauvegardes incrémentielles de Percona afin de minimiser le nombre de journaux binaires à appliquer à la base de données Aurora MySQL cible.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorisations pour créer des rôles et des politiques AWS Identity and Access Management (IAM)
- Connectivité réseau entre la base de données MySQL sur site et le cloud privé virtuel (VPC) sur AWS

Limites

- Les serveurs sources doivent être des systèmes basés sur Linux capables d'installer un client NFS (Network File System) (nfs-utils/nfs-common).
- Le compartiment S3 utilisé pour le téléchargement des fichiers de sauvegarde prend uniquement en charge le chiffrement côté serveur (SSE-S3/SSE-KMS).
- Amazon S3 limite la taille des fichiers de sauvegarde à 5 To. Si votre fichier de sauvegarde dépasse 5 To, vous pouvez le diviser en plusieurs fichiers plus petits.
- Le nombre de fichiers source chargés dans le compartiment S3 ne peut pas dépasser un million de fichiers.
- Le modèle prend uniquement en charge la sauvegarde XtraBackup complète Percona et la sauvegarde incrémentielle. Il ne prend pas en charge les sauvegardes partielles qui utilisent --

`tables` `--tables-exclude--tables-file`,`--databases`,,`--databases-exclude`, ou`--databases-file`.

- Aurora ne restaure pas les utilisateurs, les fonctions, les procédures stockées ou les informations de fuseau horaire à partir de la base de données MySQL source.

Versions du produit

- La base de données source doit être MySQL version 5.5, 5.6 ou 5.7.
- Pour MySQL 5.7, vous devez utiliser Percona XtraBackup 2.4.
- Pour MySQL 5.6 et 5.6, vous devez utiliser Percona XtraBackup 2.3 ou 2.4.

Architecture

Pile technologique source

- Système d'exploitation basé sur Linux
- serveur MySQL
- Percona XtraBackup

Pile technologique cible

- Amazon Aurora
- Amazon S3
- Amazon EFS

Architecture cible

Outils

Services AWS

- Amazon Aurora est un moteur de base de données relationnelle entièrement géré qui permet de configurer, d'exploiter et de dimensionner les déploiements MySQL de manière simple et rentable. Aurora MySQL est une alternative directe à MySQL.

- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Percona XtraBackup est un utilitaire open source qui effectue des sauvegardes en streaming, compressées et incrémentielles de bases de données MySQL sans perturber ni bloquer vos bases de données.

Épopées

Créer un système de fichiers Amazon EFS

Tâche	Description	Compétences requises
Créez un groupe de sécurité à associer aux cibles de montage Amazon EFS.	Créez un groupe de sécurité dans le VPC configuré avec une connexion VPN à la base de données sur site via AWS Transit Gateway. Pour plus d'informations sur les commandes et les étapes décrites dans cet article et dans d'autres, consultez les liens de la section « Ressources connexes » à la fin de ce modèle.	AWS DevOps /administrateur de base de données
Modifiez les règles du groupe de sécurité.	Ajoutez une règle entrante en utilisant le type NFS, le port 2049 et la plage d'adresse s IP du serveur de base de données local comme source. Par défaut, la règle de sortie	AWS DevOps /administrateur de base de données

Tâche	Description	Compétences requises
	autorise le départ de tout le trafic. Si ce n'est pas le cas, ajoutez une règle de sortie pour ouvrir une connexion pour le port NFS. Ajoutez deux autres règles entrantes : port 2049 (source : ID de groupe de sécurité de ce même groupe de sécurité) et port 22 (source : plage d'adresses IP à partir de laquelle vous allez vous connecter à une EC2 instance).	
Créez un système de fichiers.	Dans les cibles de montage, utilisez le VPC et le groupe de sécurité que vous avez créés dans l'article précédent. Choisissez le mode de débit et les performances en fonction des exigences d'E/S de la base de données locale. Activez éventuellement le chiffrement au repos.	AWS DevOps /administrateur de base de données

Monter le système de fichiers

Tâche	Description	Compétences requises
Créez un rôle de profil d'instance IAM à associer à une EC2 instance.	Créez un rôle IAM autorisé à télécharger des objets et à y accéder dans Amazon S3. Choisissez le compartiment S3 dans lequel la sauvegard	AWS DevOps

Tâche	Description	Compétences requises
	e sera stockée en tant que ressource de politique.	
Créez une EC2 instance.	Lancez une EC2 instance basée sur Linux et associez le rôle de profil d'instance IAM que vous avez créé à l'étape précédente et le groupe de sécurité que vous avez créé précédemment.	AWS DevOps
Installez le client NFS.	Installez le client NFS sur le serveur de base de données local et sur l' EC2 instance. Pour les instructions d'install ation, reportez-vous à la section « Informations supplémentaires ».	DevOps
Montage d’un système de fichiers Amazon EFS	Montez le système de fichiers Amazon EFS sur site et sur l' EC2 instance. Sur chaque serveur, créez un répertoir e pour stocker la sauvegard e et montez le système de fichiers en utilisant le point de terminaison cible du montage. Pour un exemple, consultez la section « Informations supplémentaires ».	DevOps

Effectuez une sauvegarde de la base de données source MySQL

Tâche	Description	Compétences requises
Installez Percona XtraBackup.	Installez Percona XtraBackup 2.3 ou 2.4 (selon la version de votre base de données MySQL) sur le serveur de base de données local. Pour les liens d'installation, consultez la section « Ressources associées ».	Administrateur de base de données
Comptez les schémas et les tables de la base de données source.	Rassemblez et notez le nombre de schémas et d'objets dans la base de données MySQL source. Vous utiliserez ces nombres pour valider la base de données Aurora MySQL après la migration.	Administrateur de base de données
(Facultatif) Notez la dernière séquence de journal binaire de la base de données source.	Effectuez cette étape si vous souhaitez établir une réplication binaire des journaux entre la base de données source et Aurora MySQL afin de minimiser les temps d'arrêt. log-bin doit être activé et server_id doit être unique. Notez la séquence de journal binaire actuelle de la base de données source, juste avant de lancer une sauvegarde. Effectuez cette étape juste avant la sauvegarde complète si vous prévoyez de n'utiliser	Administrateur de base de données

Tâche	Description	Compétences requises
	que la sauvegarde complète. Si vous prévoyez d'effectuer des sauvegardes incrément ielles après une sauvegard e complète, effectuez cette étape juste avant la sauvegard e incrémentielle finale que vous allez restaurer sur l'instance de base de données Aurora MySQL.	
Lancez une sauvegarde complète de la base de données MySQL source.	Effectuez une sauvegard e complète de la base de données source MySQL à l'aide de Percona XtraBacku p. Pour des exemples de commandes pour des sauvegardes complètes et incrémentielles, consultez la section « Informations supplémentaires ».	Administrateur de base de données

Tâche	Description	Compétences requises
(Facultatif) Effectuez des sauvegardes incrémentielles à l'aide de Percona XtraBackup.	Les sauvegardes incrément ielles peuvent être utilisées pour réduire le nombre de journaux binaires que vous devez appliquer pour synchroniser la base de données source avec Aurora MySQL. Les bases de données volumineuses et gourmandes en transactions peuvent générer un grand nombre de journaux binaires lors des sauvegardes. En effectuant des sauvegard es incrémentielles et en les stockant sur un système de fichiers Amazon EFS partagé, vous pouvez réduire considérablement le temps de sauvegarde et de télécharg ement de votre base de données. Pour plus de détails, consultez la section « Informations supplémen taires ». Continuez à effectuer des sauvegardes incrément ielles jusqu'à ce que vous soyez prêt à commencer le processus de migration vers Aurora.	Administrateur de base de données

Tâche	Description	Compétences requises
Préparez des sauvegardes.	Au cours de cette étape, des journaux de transactions sont appliqués à la sauvegard e pour les transactions qui étaient en cours pendant la sauvegarde. Continuez à appliquer des journaux transactionnels (--apply-log-only) à chaque sauvegarde incrémentielle pour fusionner les sauvegardes, à l'excepti on de la dernière sauvegarde. Pour des exemples, consultez la section « Informations supplémentaires ». <efs_moun t_name>Après cette étape, la sauvegarde complète et fusionnée se trouvera dans ~/ /fullbackup.	Administrateur de base de données
Compressez et divisez la sauvegarde fusionnée finale.	Après avoir préparé la sauvegarde fusionnée finale, utilisez les commandes tar, zip et split pour créer des fichiers compressés plus petits à partir de la sauvegarde. Pour des exemples, consultez la section « Informations supplémen taires ».	Administrateur de base de données

Restaurez la sauvegarde sur un cluster de base de données Aurora MySQL

Tâche	Description	Compétences requises
Téléchargez la sauvegarde sur Amazon S3.	Le système de fichiers Amazon EFS dans lequel les fichiers de sauvegarde sont stockés est monté à la fois sur la base de données locale et sur une EC2 instance, de sorte que les fichiers de sauvegarde sont facilement accessibles à l' EC2 instance. <bucket_name>Connectez-vous à l' EC2 instance à l'aide de Secure Shell (SSH) et téléchargez les fichiers de sauvegarde compressés dans un compartiment S3 nouveau ou existant ; par exemple : aws s3 sync ~/ <efs_moun t_name>/fullbackup s3 :/// fullbackup. Pour plus de détails, consultez les liens dans la section « Ressources connexes ».	AWS DevOps
Créez un rôle de service pour qu'Aurora accède à Amazon S3.	Créez un rôle IAM de confiance sur « rds.amazo naws.com » et une politique qui permettra à Aurora d'accéder au compartiment S3 dans lequel les fichiers de sauvegarde sont stockés. Les autorisations requises sont ListBucket GetObject, et GetObjectVersion.	AWS DevOps

Tâche	Description	Compétences requises
Créez la configuration réseau pour Aurora.	Créez un groupe de sous-réseaux de base de données de cluster avec au moins deux zones de disponibilité et une configuration de table de routage de sous-réseau qui autorise la connectivité sortante à la base de données source. Créez un groupe de sécurité qui autorise les connexions sortantes à la base de données locale et permet aux administr ateurs de se connecter au cluster de base de données Aurora. Pour plus d'informa tions, consultez les liens de la section « Ressources connexes ».	AWS DevOps /administrateur de base de données

Tâche	Description	Compétences requises
Restaurez la sauvegarde sur un cluster de base de données Aurora MySQL.	Restaurez vos données à partir de la sauvegarde que vous avez téléchargée sur Amazon S3. Spécifiez la version MySQL de votre base de données source, indiquez le nom du compartiment S3 et le préfixe du chemin du dossier dans lequel vous avez chargé le fichier de sauvegarde (par exemple, « fullbackup » pour les exemples de la section « Informations supplémentaires ») et indiquez le rôle IAM que vous avez créé pour autoriser Aurora à accéder à Amazon S3.	AWS DevOps /administrateur de base de données
Validez la base de données Aurora MySQL.	Validez le nombre de schémas et d'objets dans le cluster de base de données Aurora restauré par rapport au nombre obtenu à partir de la base de données source.	Administrateur de base de données

Tâche	Description	Compétences requises
Configurez la réplication du journal binaire.	Utilisez la séquence de journal binaire que vous avez indiquée précédemment, avant d'effectuer la dernière sauvegarde restaurée sur le cluster de base de données Aurora. Créez un utilisateur de réplication sur la base de données source et suivez les instructions de la section « Informations supplémen taires » pour fournir les privilèges appropriés, activer la réplication sur Aurora et vérifier que la réplication est synchronisée.	AWS DevOps /administrateur de base de données

Ressources connexes

Création d'un système de fichiers Amazon EFS

- Création d'un groupe de sécurité (documentation Amazon VPC)
- Pièces jointes VPN pour passerelle de transit (documentation Amazon VPC)
- Diminution du débit VPN à l'aide d'AWS Transit Gateway (blog sur la mise en réseau et la diffusion de contenu)
- Création d'un système de fichiers Amazon EFS (documentation Amazon EFS)
- Création de cibles de montage (documentation Amazon EFS)
- Chiffrement des données au repos (documentation Amazon EFS)

Montage du système de fichiers

- Rôles IAM pour Amazon EC2 (EC2 documentation Amazon)
- Lancement d'une instance Amazon EC2 Linux (EC2 documentation Amazon)

- Installation du client NFS (documentation Amazon EFS)
- Montage du système de fichiers Amazon EFS sur votre client sur site (documentation Amazon EFS)
- Montage de systèmes de fichiers EFS (documentation Amazon EFS)

Création d'une sauvegarde de la base de données source MySQL

- Installation de Percona XtraBackup 2.3 (documentation Percona XtraBackup)
- Installation de Percona XtraBackup 2.4 (documentation Percona XtraBackup)
- Configuration de la configuration principale de réplication (documentation MySQL)
- Migration de données d'une base de données MySQL externe vers un cluster de base de données Aurora MySQL (documentation Aurora)
- Sauvegarde incrémentielle (documentation Percona XtraBackup)

Restauration de la sauvegarde sur Amazon Aurora MySQL

- Création d'un compartiment (documentation Amazon S3)
- Connexion à votre instance Linux via SSH (documentation Amazon Ec2)
- Configuration de l'interface de ligne de commande AWS (documentation de l'interface de ligne de commande AWS)
- commande de synchronisation (référence de commande de l'AWS CLI)
- Création d'une politique IAM pour accéder aux ressources Amazon S3 (documentation Aurora)
- Conditions requises pour le cluster de bases de données (documentation Aurora)
- Utilisation de groupes de sous-réseaux de base de données (documentation Aurora)
- Création d'un groupe de sécurité VPC pour une instance de base de données privée (documentation Aurora)
- Restauration d'un cluster de base de données Aurora MySQL à partir d'un compartiment S3 (documentation Aurora)
- Configuration de la réplication avec MySQL ou un autre cluster de base de données Aurora (documentation Aurora)
- procédure mysql.rds_set_external_master (référence SQL MySQL sur Amazon RDS)
- procédure mysql.rds_start_replication (référence SQL MySQL sur Amazon RDS)

Références supplémentaires

- Migration de données d'une base de données MySQL externe vers un cluster de base de données Aurora MySQL (documentation Aurora)
- Téléchargements du serveur MySQL (site Web Oracle)

Tutoriels et vidéos

- Migration de données MySQL vers un cluster de bases de données Aurora MySQL à l'aide d'Amazon S3 (AWS Knowledge Center)
- Configuration et montage d'Amazon EFS (vidéo)

Informations supplémentaires

Installation d'un client NFS

- Si vous utilisez Red Hat ou un système d'exploitation Linux similaire, utilisez la commande suivante :

```
$ sudo yum -y install nfs-utils
```

- Si vous utilisez Ubuntu ou un système d'exploitation Linux similaire, utilisez la commande suivante :

```
$ sudo apt-get -y install nfs-common
```

Pour plus d'informations, consultez la procédure pas à pas dans la documentation Amazon EFS.

Montage du système de fichiers Amazon EFS

Utilisez les commandes suivantes :

```
mkdir ~/<efs_mount_name>
$ sudo mount -t nfs -o
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport mount-
target-IP:/ ~/<efs_mount_name>
```

Pour plus d'informations, consultez la procédure pas à pas et le montage des systèmes de fichiers EFS dans la documentation Amazon EFS.

Effectuer des sauvegardes de la base de données source MySQL

Sauvegardes complètes

Utilisez une commande comme la suivante, qui prend la sauvegarde, la compresse et la divise en petits morceaux de 1 Go chacun :

```
xtrabackup --backup --user=dbuser --password=<password> --binlog-info=AUTO --stream=tar
 --target-dir=~/<efs_mount_name>/fullbackup | gzip - | split -d --bytes=1024MB - ~/
<efs_mount_name>/fullbackup/backup.tar.gz &
```

Si vous prévoyez d'effectuer des sauvegardes incrémentielles ultérieures après la sauvegarde complète, ne compressez pas et ne divisez pas la sauvegarde. Utilisez plutôt une commande similaire à la suivante :

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/fullbackup/
```

Sauvegardes incrémentielles

Utilisez le chemin de sauvegarde complet pour le `--incremental-basedir` paramètre, par exemple :

```
xtrabackup --backup --user=dbuser --password=<password> --target-dir=~/
<efs_mount_name>/incremental/backupdate --incremental-basedir=~/<efs_mount_name>/
fullbackup
```

où basedir est le chemin d'accès à la sauvegarde complète et au fichier xtrabackup_checkpoints.

Pour plus d'informations sur la réalisation de sauvegardes, consultez la section Migration de données d'une base de données MySQL externe vers un cluster de bases de données Amazon Aurora MySQL dans la documentation Aurora.

Préparation des sauvegardes

Pour préparer une sauvegarde complète :

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup
```

Pour préparer une sauvegarde incrémentielle :

```
xtrabackup --prepare --apply-log-only --target-dir=~/<efs_mount_name>/fullbackup --
incremental-dir=~/<efs_mount_name>/incremental/06062020
```

Pour préparer la sauvegarde finale, procédez comme suit :

```
xtrabackup --prepare --target-dir=~/<efs_mount_name>/fullbackup --incremental-dir=~/
<efs_mount_name>/incremental/06072020
```

Pour plus d'informations, consultez la section Sauvegardes incrémentielles dans la documentation de Percona XtraBackup .

Compression et division de la sauvegarde fusionnée

Pour compresser la sauvegarde fusionnée dans ~/ <efs_mount_name>/fullbackup :

```
tar -zcvf <backupfilename.tar.gz> ~/<efs_mount_name>/fullbackup
```

Pour fractionner la sauvegarde, procédez comme suit :

```
split -d -b1024M --verbose  <backupfilename.tar.gz> <backupfilename.tar.gz>
```

Configuration de la réplication binlog

Pour créer un utilisateur de réplication sur la base de données source et fournir les privilèges appropriés :

```
CREATE USER 'repl_user'@'' IDENTIFIED BY ''; GRANT REPLICATION CLIENT, REPLICATION
 SLAVE ON *.* TO 'repl_user'@'';
```

Pour activer la réplication sur Aurora en vous connectant au cluster de base de données Aurora, activez les journaux binaires dans le groupe de paramètres du cluster de base de données. `binlog_format = mixed`Régler (le mode mixte est préférable). Cette modification nécessite que vous redémarriez l'instance pour appliquer la mise à jour.

```
CALL mysql.rds_set_external_master ('sourcedbinstanceIP', sourcedbport, 'repl_user',
 '', 'binlog_file_name', binlog_file_position, 0); CALL mysql.rds_start_replication;
```

Pour vérifier que la réplication est synchronisée, procédez comme suit :

```
SHOW Slave Status \G;
```

Le champ Seconds behind master indique à quel point Aurora est en retard par rapport à la base de données locale.

Migrez des applications Java sur site vers AWS à l'aide d'AWS App2Container

Créée par Dhananjay Karanjkar (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

AWS App2Container (A2C) est un outil de ligne de commande qui permet de transformer des applications existantes exécutées sur des machines virtuelles en conteneurs, sans qu'aucune modification de code ne soit nécessaire. A2C découvre les applications exécutées sur un serveur, identifie les dépendances et génère des artefacts pertinents pour un déploiement fluide sur Amazon Elastic Container Service (Amazon ECS) et Amazon Elastic Kubernetes Service (Amazon EKS).

Ce modèle décrit les étapes à suivre pour migrer à distance des applications Java sur site déployées sur un serveur d'applications vers AWS Fargate ou Amazon EKS à l'aide d'App2Container via la machine subordonnée.

La machine de travail peut être utilisée dans les cas d'utilisation suivants :

- L'installation de Docker n'est pas autorisée ou n'est pas disponible sur les serveurs d'applications sur lesquels les applications Java sont exécutées.
- Vous devez gérer la migration de plusieurs applications déployées sur différents serveurs physiques ou virtuels.

Ce modèle utilise AWS CodeCommit AWS CodePipeline, et AWS CodeBuild.

Conditions préalables et limitations

Prérequis

- Un serveur d'applications avec une application Java exécutée sur un serveur Linux
- Une machine de travail dotée d'un système d'exploitation Linux
- Un ordinateur subordonné disposant d'au moins 20 Go d'espace disque disponible

Limites

- Toutes les applications ne sont pas prises en charge. Pour plus d'informations, consultez la section Applications prises en charge pour Linux.

Architecture

Pile technologique source

- Applications Java exécutées sur un serveur Linux

Pile technologique cible

- AWS CodeBuild
- AWS CodeCommit
- AWS CodeDeploy
- AWS CodePipeline
- Amazon Elastic Container Registry
- AWS Fargate

Architecture cible

Outils

Outils

- AWS App2Container — AWS App2Container (A2C) est un outil en ligne de commande qui vous permet de transférer et de déplacer des applications exécutées dans vos centres de données sur site ou sur des machines virtuelles, afin qu'elles s'exécutent dans des conteneurs gérés par Amazon ECS ou Amazon EKS.
- AWS CodeBuild — AWS CodeBuild est un service de création entièrement géré dans le cloud. CodeBuild compile votre code source, exécute des tests unitaires et produit des artefacts prêts à être déployés.
- AWS CodeCommit — AWS CodeCommit est un service de contrôle de version hébergé par Amazon Web Services que vous pouvez utiliser pour stocker et gérer des actifs privés (tels que des documents, du code source et des fichiers binaires) dans le cloud.
- AWS CodePipeline — AWS CodePipeline est un service de livraison continue que vous pouvez utiliser pour modéliser, visualiser et automatiser les étapes nécessaires à la publication de votre logiciel.

- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif qui permet d'exécuter, d'arrêter et de gérer des conteneurs sur un cluster.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un service de registre d'images de conteneurs géré par AWS qui est sécurisé, évolutif et fiable.
- Amazon EKS — Amazon Elastic Kubernetes Service (Amazon EKS) est un service géré que vous pouvez utiliser pour exécuter Kubernetes sur AWS sans avoir à installer, exploiter et gérer votre propre plan de contrôle ou vos propres nœuds Kubernetes.
- AWS Fargate — AWS Fargate est une technologie que vous pouvez utiliser avec Amazon ECS pour exécuter des conteneurs sans avoir à gérer des serveurs ou des clusters d'instances Amazon Elastic Compute Cloud (Amazon). EC2 Avec Fargate, vous n'avez plus besoin d'allouer, de configurer ou de mettre à l'échelle des clusters de machines virtuelles pour exécuter des conteneurs.

Épopées

Configurer les informations d'identification

Tâche	Description	Compétences requises
Créez un secret pour accéder au serveur d'applications.	Pour accéder au serveur d'applications à distance depuis l'ordinateur subordonné, créez un secret dans AWS Secrets Manager. Pour votre secret, vous pouvez utiliser soit la clé privée SSH, soit le certificat et la clé privée SSH. Pour plus d'informations, consultez Gérer les secrets pour AWS App2Container.	DevOps, Développeur

Configurer la machine de travail

Tâche	Description	Compétences requises
Installez le fichier tar.	Exécutez `sudo yum install -y tar`.	DevOps, Développeur
Installez l'AWS CLI.	Pour installer l'interface de ligne de commande Amazon (AWS CLI), `curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"` exécutez. Décompressez `awscliv2.zip` . Exécutez `sudo ./aws/install` .	DevOps, Développeur
Installez App2Container.	Exécutez les commandes suivantes : `curl -o AWSApp2Container-installer-linux.tar.gz https://app2container-release-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/AWSApp2Container-installer-linux.tar.gz`	DevOps, Développeur

Tâche	Description	Compétences requises

	`sudo tar xvf AWSApp2Container-installer-linux.tar.gz`
	
	`sudo ./install.sh`	

Configurez les profils.	Pour configurer le profil par défaut AWS, exécutez`sudo aws configure .` Pour configurer le profil par défaut AWS nommé, exécutez`sudo aws configure --profile <profile name>`.	DevOps, Développeur

Installez Docker.	Exécutez les commandes suivantes.
	
	`sudo yum install -y docker`
	
	`sudo systemctl enable docker & sudo systemctl restart docker`	

Tâche	Description	Compétences requises
Initialisez App2Container.	Pour initialiser App2Container, vous avez besoin des informations suivantes : • `workspace` : pour stocker les artefacts de conteneurisation des applications. Nous vous recommandons de fournir un chemin de répertoire comportant au moins 20 Go d'espace disque disponible. • `awsProfile` : profil AWS configuré sur le serveur. Cela est nécessaire pour télécharger des artefacts sur Amazon S3, exécuter la `containerize` commande et générer des artefacts AWS à déployer sur Amazon ECS ou Amazon EKS. • `s3Bucket`: pour extraire et stocker des artefacts AWS. • `metricsReportPermission` : pour collecter et stocker les statistiques signalées. • `dockerContentTrust` : pour signer l'image Docker. Exécutez `sudo app2container init` .	DevOps, Développeur

Configuration de la machine subordonnée

Tâche	Description	Compétences requises
Configurez l'ordinateur subordonné pour qu'il se connecte à distance et exécute les commandes App2Container sur le serveur d'applications.	Pour configurer la machine subordonnée, les informations suivantes sont requises : • `Server FQDN`: nom de domaine complet du serveur d'applications. • `Server IP address`: adresse IP du serveur d'applications. Le nom de domaine complet ou l'adresse IP sont suffisants. • `SecretARN` : Amazon Resource Name (ARN) du secret utilisé pour se connecter au serveur d'applications et stocké dans Secrets Manager. • `AuthMethod` : méthode `cert` d'authentification `key` or. Exécutez `sudo app2container remote configure` .	DevOps, Développeur

Découvrez, analysez et extrayez des applications sur la machine de travail

Tâche	Description	Compétences requises
Découvrez les applications Java locales.	Pour découvrir à distance toutes les applications exécutées sur le serveur d'applications, exécutez la commande suivante. `sudo app2container remote inventory --target <FQDN/IP of App server>` Cette commande génère une liste des applications déployées dans`inventory .json` .	Développeur, DevOps
Analysez les applications découvertes.	Pour analyser à distance chaque application à l'aide de l'identifiant d'application obtenu lors de la phase d'inventaire, exécutez la commande suivante. `sudo app2container remote analyze --application-id <java-app-id> --target <FQDN/IP of App Server>` Cela génère un `analysis.json` fichier dans l'emplace ment de l'espace de travail. Une fois ce fichier généré,	Développeur, DevOps

Tâche	Description	Compétences requises
	vous pouvez modifier les paramètres de conteneur isation en fonction de vos besoins.	
Extrayez les applications analysées.	Pour générer une archive d'application pour l'application analysée, exécutez à distance la commande suivante, qui générera le bundle tar dans l'emplacement de l'espace de travail. `sudo app2container remote extract --application-id <application id> --target <FQDN/IP of App Server>` Les artefacts extraits peuvent être générés sur la machine de travail locale.	Développeur, DevOps

Conteneurisez les artefacts extraits sur la machine de travail

Tâche	Description	Compétences requises
Conteneurisez les artefacts extraits.	Conteneurisez les artefacts extraits à l'étape précédente en exécutant la commande suivante. `sudo app2container containerize --input-`	Développeur, DevOps

Tâche	Description	Compétences requises
	`archive <tar bundle location on worker machine>`	
Finalisez la cible.	Pour finaliser la cible, ouvrez`deployment.json` , qui est créée lors de l'exécution de la `containerize` commande. Pour spécifier AWS Fargate comme cible, définissez sur. `createEcsArtifacts true` Pour définir Amazon EKS comme cible, définissez ce paramètre `createEksArtifacts` sur true.	Développeur, DevOps

Génération et approvisionnement d'artefacts AWS

Tâche	Description	Compétences requises
Générez des artefacts de déploiement AWS sur la machine subordonnée.	Pour générer des artefacts de déploiement, exécutez la commande suivante. `sudo app2container generate app-deployment --application-id <application id>` Cela génère le CloudFormation modèle `ecs-master.yml` AWS dans l'espace de travail.	DevOps

Tâche	Description	Compétences requises
Fournissez les artefacts.	Pour continuer à approvisi onner les artefacts générés, déployez le CloudFormation modèle AWS en exécutant la commande suivante. `aws cloudformation deploy --template-file <path to ecs-master.yml> --capabilities CAPABILITY_NAMED_IAM --stack-name <application id>-ECS`	DevOps
Générez le pipeline.	`pipeline.json` Modifie, qui a été créé dans l'article précédent, en fonction de vos besoins. Exécutez ensuite la `generate pipeline` commande pour générer les artefacts de déploiement du pipeline.	DevOps

Ressources connexes

- Qu'est-ce qu'App2Container ?
- Article de blog AWS App2Container
- Principes de base de configuration de l'AWS CLI
- Principes de base de Docker pour Amazon ECS
- Commandes Docker

Migrer des systèmes de fichiers partagés dans le cadre d'une migration AWS de grande envergure

Créée par Amit Rudraraju (AWS), Sam Apa (AWS), Bheemeswararao Balla (AWS), Wally Lu (AWS) et Sanjeev Prakasam (AWS)

Récapitulatif

La migration de 300 serveurs ou plus est considérée comme une migration de grande envergure. L'objectif d'une migration de grande envergure est de migrer les charges de travail de leurs centres de données sur site existants vers le cloud AWS, et ces projets se concentrent généralement sur les charges de travail des applications et des bases de données. Cependant, les systèmes de fichiers partagés nécessitent une attention particulière et un plan de migration distinct. Ce modèle décrit le processus de migration des systèmes de fichiers partagés et fournit les meilleures pratiques pour réussir leur migration dans le cadre d'un projet de migration de grande envergure.

Un système de fichiers partagé (SFS), également appelé réseau ou système de fichiers en cluster, est un partage de fichiers monté sur plusieurs serveurs. Les systèmes de fichiers partagés sont accessibles via des protocoles tels que NFS (Network File System), CIFS (Common Internet File System) ou SMB (Server Message Block).

Ces systèmes ne sont pas migrés à l'aide d'outils de migration standard tels qu'AWS Application Migration Service, car ils ne sont ni dédiés à l'hôte à migrer ni représentés sous forme de périphérique en mode bloc. Bien que la plupart des dépendances de l'hôte soient migrées de manière transparente, la coordination et la gestion des systèmes de fichiers dépendants doivent être gérées séparément.

Vous migrez des systèmes de fichiers partagés selon les phases suivantes : découverte, planification, préparation, découpe et validation. À l'aide de ce modèle et des classeurs joints, vous migrez votre système de fichiers partagé vers un service de stockage AWS, tel qu'Amazon Elastic File System (Amazon EFS), Amazon FSx for NetApp ONTAP ou Amazon FSx for Windows File Server. Pour transférer le système de fichiers, vous pouvez utiliser AWS DataSync ou un outil tiers, tel que NetApp SnapMirror.

> **Note**
>
> Ce modèle fait partie d'une série de directives AWS Prescriptive Guidance sur les grandes migrations vers le cloud AWS. Ce modèle inclut les meilleures pratiques et les instructi

ons à SFSs intégrer dans vos plans de vague pour les serveurs. Si vous migrez un ou plusieurs systèmes de fichiers partagés en dehors d'un projet de migration de grande envergure, consultez les instructions de transfert de données figurant dans la documenta tion AWS pour Amazon EFS, Amazon FSx pour Windows File Server et Amazon FSx pour NetApp ONTAP.

Conditions préalables et limitations

Prérequis

Les prérequis peuvent varier en fonction de vos systèmes de fichiers partagés source et cible et de votre cas d'utilisation. Les plus courants sont les suivants :

- Un compte AWS actif.
- Vous avez terminé la découverte du portefeuille d'applications pour votre projet de migration de grande envergure et vous avez commencé à élaborer des plans de vague. Pour plus d'informations, consultez le manuel Portfolio pour les migrations AWS à grande échelle.
- Clouds privés virtuels (VPCs) et groupes de sécurité qui autorisent le trafic entrant et sortant entre le centre de données sur site et votre environnement AWS. Pour plus d'informations, consultez les options de connectivité Network-to-Amazon VPC et les exigences DataSync du réseau AWS.
- Autorisations pour créer des CloudFormation piles AWS ou autorisations pour créer des FSx ressources Amazon EFS ou Amazon. Pour plus d'informations, consultez la CloudFormation documentation, la documentation Amazon EFS ou FSx la documentation Amazon.
- Si vous utilisez AWS DataSync pour effectuer la migration, vous devez disposer des autorisations suivantes :
  - Autorisations permettant DataSync à AWS d'envoyer des journaux à un groupe de CloudWatch journaux AWS Logs. Pour plus d'informations, consultez Autoriser DataSync le téléchargement de journaux vers des groupes de CloudWatch journaux.
  - Autorisations d'accès au groupe de CloudWatch journaux Logs. Pour plus d'informations, voir Présentation de la gestion des autorisations d'accès à vos ressources CloudWatch Logs.
  - Autorisations permettant de créer des agents et des tâches dans DataSync. Pour plus d'informations, consultez la section Autorisations IAM requises pour utiliser AWS DataSync.

Limites

- Ce modèle est conçu pour effectuer une migration dans SFSs le cadre d'un projet de migration de grande envergure. Il inclut les meilleures pratiques et les instructions à SFSs intégrer dans vos plans de migration d'applications. Si vous migrez un ou plusieurs systèmes de fichiers partagés en dehors d'un projet de migration de grande envergure, consultez les instructions de transfert de données figurant dans la documentation AWS pour Amazon EFS, Amazon FSx pour Windows File Server et Amazon FSx pour NetApp ONTAP.
- Ce modèle est basé sur les architectures, les services et les modèles de migration couramment utilisés. Cependant, les grands projets et stratégies de migration peuvent varier d'une organisation à l'autre. Vous devrez peut-être personnaliser cette solution ou les classeurs fournis en fonction de vos besoins.

Architecture

Pile technologique source

Un ou plusieurs des éléments suivants :

- serveur de fichiers Linux (NFS)
- Serveur de fichiers Windows (SMB)
- NetApp baie de stockage
- Unité multidisque de stockage Dell EMC Isilon

Pile technologique cible

Un ou plusieurs des éléments suivants :

- Amazon Elastic File System
- Amazon FSx pour NetApp ONTAP
- Serveur FSx de fichiers Amazon pour Windows

Architecture cible

Le schéma montre le processus suivant :

1. Vous établissez une connexion entre le centre de données sur site et le cloud AWS à l'aide d'un service AWS tel qu'AWS Direct Connect ou AWS Site-to-Site VPN.

2. Vous installez l' DataSync agent dans le centre de données sur site.
3. Selon votre plan de vague, vous pouvez DataSync répliquer les données du système de fichiers partagé source vers le partage de fichiers AWS cible.

Phases de migration

L'image suivante montre les phases et les étapes de haut niveau de la migration d'un SFS dans le cadre d'un projet de migration de grande envergure.

La section Epics de ce modèle contient des instructions détaillées sur la façon de terminer la migration et d'utiliser les classeurs joints. Voici un aperçu général des étapes de cette approche progressive.

Phase	Étapes
Découvrez	1. À l'aide d'un outil de découverte, vous collectez des données sur le système de fichiers partagé, notamment les serveurs, les points de montage et les adresses IP. 2. À l'aide d'une base de données de gestion de configuration (CMDB) ou de votre outil de migration, vous collectez des informations sur le serveur, notamment des informations sur la vague de migration, l'environnement, le propriétaire de l'application, le nom du service de gestion des services informatiques (ITSM), l'unité organisationnelle et l'ID de l'application.
Plan	3. À l'aide des informations collectées sur les serveurs SFSs et les serveurs, créez le plan de vague SFS. 4. À l'aide des informations contenues dans la feuille de travail de création, pour chaque SFS, choisissez un service AWS cible et un outil de migration.

Préparation	5. Configurez l'infrastructure cible dans Amazon EFS, Amazon FSx for NetApp ONTAP ou Amazon FSx pour Windows File Server. 6. Configurez le service de transfert de données, par exemple DataSync, puis lancez la synchronisation initiale des données. Lorsque la synchronisation initiale est terminée, vous pouvez configurer des synchronisations récurrentes pour qu'elles s'exécutent selon un calendrier, 7. Mettez à jour le plan de vague SFS avec des informations sur le partage de fichiers cible, telles que l'adresse IP ou le chemin.
Découper	8. Arrêtez les applications qui accèdent activement au SFS source. 9. Dans le service de transfert de données, effectuez une synchronisation finale des données. 10. Lorsque la synchronisation est terminée, vérifiez qu'elle s'est parfaitement déroulée en consultant les données du journal dans CloudWatch Logs.
Valider	11. Sur les serveurs, remplacez le point de montage par le nouveau chemin SFS. 12. Redémarrez et validez les applications.

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.

- AWS DataSync est un service de transfert et de découverte de données en ligne qui vous aide à déplacer des fichiers ou des données d'objets vers, depuis et entre les services de stockage AWS.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS.
- Amazon FSx fournit des systèmes de fichiers qui prennent en charge les protocoles de connectivité standard du secteur et offrent une disponibilité et une réplication élevées dans les régions AWS.

Autres outils

- SnapMirrorest un outil de réplication de NetApp données qui réplique les données provenant de volumes sources ou de qtrees spécifiés vers des volumes cibles ou des qtrees, respectivement. Vous pouvez utiliser cet outil pour migrer un système de fichiers NetApp source vers Amazon FSx pour ONTAP.
- Robocopy, abréviation de Robust File Copy, est un répertoire de ligne de commande et une commande pour Windows. Vous pouvez utiliser cet outil pour migrer un système de fichiers source Windows vers Amazon FSx pour Windows File Server.

Bonnes pratiques

Approches de planification des vagues

Lorsque vous planifiez des vagues pour votre projet de migration de grande envergure, tenez compte de la latence et des performances des applications. Lorsque le SFS et les applications dépendantes fonctionnent dans différents emplacements, tels que l'un dans le cloud et l'autre dans le centre de données sur site, cela peut augmenter la latence et affecter les performances des applications. Les options disponibles lors de la création de plans de vagues sont les suivantes :

1. Migrez le SFS et tous les serveurs dépendants au sein de la même vague : cette approche permet d'éviter les problèmes de performances et de minimiser les retouches, telles que la reconfiguration des points de montage à plusieurs reprises. Il est recommandé lorsqu'une très faible latence est requise entre l'application et le SFS. Cependant, la planification des vagues est complexe et l'objectif est généralement de supprimer des variables des groupes de dépendances, et non d'en ajouter. De plus, cette approche n'est pas recommandée si de nombreux serveurs accèdent au même SFS, car cela rend la vague trop importante.
2. Migrer le SFS après la migration du dernier serveur dépendant : par exemple, si plusieurs serveurs accèdent à un SFS et que la migration de ces serveurs est planifiée au cours des vagues 4, 6 et 7, planifiez le SFS pour qu'il migre au cours de la vague 7.

Cette approche est souvent la plus logique pour les grandes migrations et elle est recommandée pour les applications sensibles à la latence. Il réduit les coûts associés au transfert de données. Cela minimise également la période de latence entre le SFS et les applications de niveau supérieur (telles que la production), car les applications de niveau supérieur sont généralement programmées pour migrer en dernier, après les applications de développement et d'assurance qualité.

Cependant, cette approche nécessite toujours de la découverte, de la planification et de l'agilité. Il se peut que vous deviez migrer le SFS lors d'une vague précédente. Vérifiez que les applications peuvent supporter la latence supplémentaire pendant la période comprise entre la première vague dépendante et la vague contenant le SFS. Organisez une session de découverte avec les propriétaires de l'application et faites migrer l'application la plus sensible à la latence en même temps. Si des problèmes de performances sont découverts après la migration d'une application dépendante, préparez-vous à effectuer une transition rapide pour migrer le SFS le plus rapidement possible.

3. Migrer le SFS à la fin d'un projet de migration de grande envergure : cette approche est recommandée si le temps de latence n'est pas un facteur, par exemple lorsque les données du SFS sont rarement consultées ou qu'elles ne sont pas essentielles aux performances de l'application. Cette approche rationalise la migration et simplifie les tâches de transfert.

Vous pouvez combiner ces approches en fonction de la sensibilité à la latence de l'application. Par exemple, vous pouvez effectuer une migration sensible à la latence SFSs en utilisant les approches 1 ou 2, puis migrer le reste SFSs en utilisant l'approche 3.

Choix d'un service de système de fichiers AWS

AWS propose plusieurs services cloud pour le stockage de fichiers. Chacune offre des avantages et des limites différents en termes de performances, d'évolutivité, d'accessibilité, d'intégration, de conformité et d'optimisation des coûts. Il existe des options par défaut logiques. Par exemple, si votre système de fichiers sur site actuel fonctionne sous Windows Server, Amazon FSx pour Windows File Server est le choix par défaut. Ou si le système de fichiers sur site utilise NetApp ONTAP, Amazon FSx pour NetApp ONTAP est le choix par défaut. Toutefois, vous pouvez choisir un service cible en fonction des exigences de votre application ou pour bénéficier d'autres avantages liés à l'exploitation du cloud. Pour plus d'informations, consultez Choisir le service de stockage de fichiers AWS adapté à votre déploiement (présentation du sommet AWS).

Choix d'un outil de migration

Amazon EFS et Amazon FSx prennent en charge l'utilisation d'AWS DataSync pour migrer des systèmes de fichiers partagés vers le cloud AWS. Pour plus d'informations sur les systèmes et services de stockage pris en charge, les avantages et les cas d'utilisation, consultez Qu'est-ce qu'AWS DataSync ? Pour un aperçu du processus d'utilisation DataSync pour transférer vos fichiers, consultez Comment fonctionnent DataSync les transferts AWS.

Plusieurs outils tiers sont également disponibles, notamment les suivants :

- Si vous choisissez Amazon FSx pour NetApp ONTAP, vous pouvez l'utiliser NetApp SnapMirror pour migrer les fichiers du centre de données sur site vers le cloud. SnapMirror utilise la réplication au niveau des blocs, qui peut être plus rapide que le processus de transfert de données DataSync et en réduire la durée. Pour plus d'informations, consultez la section Migration vers ONTAP à l'aide FSx d'ONTAP. NetApp SnapMirror
- Si vous choisissez Amazon FSx pour Windows File Server, vous pouvez utiliser Robocopy pour migrer des fichiers vers le cloud. Pour plus d'informations, voir Migration de fichiers existants vers un serveur de fichiers Windows FSx à l'aide de Robocopy.

Épopées

Découvrez

Tâche	Description	Compétences requises
Préparez le classeur de découverte SFS.	1. Téléchargez les classeurs dans la section Pièces jointes de ce modèle. Il contient deux fichiers, SFS-Discovery-Workbook.xlsx et SFS-Wave-Plan-Workbook.xlsx. 2. Ouvrez le fichier SFS-Discovery-Workbook dans Microsoft Excel. 3. Dans la feuille de travail du tableau de bord, procédez comme suit :	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	• Dans la colonne A, mettez à jour le nom de l'environnement. • Dans la colonne B, mettez à jour l'ordre des environnements pour les classer de la priorité la plus faible (1) à la priorité la plus élevée. • Dans les colonnes D—E, mettez à jour le calendrier des vagues. • Dans les colonnes C et K, mettez à jour les noms des comptes AWS. • Dans la colonne L, mettez à jour le VPC IDs. • Dans les colonnes M—O, mettez à jour le sous-réseau. IDs 4. Passez en revue le reste du modèle de classeur et mettez à jour toutes les autres valeurs nécessaires à votre organisation ou à votre cas d'utilisation. 5. Enregistrez le classeur.	

Tâche	Description	Compétences requises
Collectez des informations sur le SFS source.	1. À l'aide de votre outil de découverte préféré, identifiez tous les montages SFS sur tous les périphériques de stockage, serveurs Linux et serveurs Windows applicables. En règle générale, vous devez collecter les informations suivantes : • Appareils clients • Adresse IP du client • Détails du SFS • Point de montage **Note** Vous pouvez ajouter les détails du point de montage à votre runbook de migration pour le remontage du SFS après la migration. 2. Ouvrez le fichier SFS-Discovery-Workbook. 3. Dans la feuille de travail Wave-Sheet, procédez comme suit : • Dans la colonne Emplacement du serveur	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	(D), dans la formule, vérifiez que le format de la plage CIDR pour la source locale fonctionne pour votre plage. Par exemple, si votre plage CIDR est égale à`10.0.0.0/8` , entrez`10.*.*.*`. • Dans la colonne Emplacement SFS (E), dans la formule, vérifiez que le format de la plage CIDR pour le VPC cible convient à votre plage. Par exemple, si votre plage CIDR est égale à`176.16.0.0/16` , entrez`176.16.*.*` . 4. Dans la feuille de travail SFS Data, procédez comme suit : • Dans la colonne Nom du serveur (A), entrez le nom du serveur sur lequel le SFS est monté. • Dans la colonne SFS path (B), entrez le nom du SFS. • Dans la colonne Adresse IP (C), entrez l'adresse IP du serveur. • Ajoutez toutes les autres informations pertinentes	

Tâche	Description	Compétences requises
	que vous avez collectées lors de la découverte, telles que le point de montage et la taille du SFS. Vous pourrez utiliser ces données ultérieurement pour modifier les calculs de planification des vagues. 5. Enregistrez le classeur.	

Tâche	Description	Compétences requises
Collectez des informations sur les serveurs.	1. À l'aide de votre CMDB ou des données enregistrées dans votre outil de migration, identifiez toutes les informations suivantes concernant les serveurs dotés de montages SFS : • Server name • Adresse IP • Vague • Unité d'organisation (UO) • Environnement de serveur, tel que `DEVQA`, ou `PROD` • Nom de l'application • Propriétaire de l'application et coordonnées 2. Ouvrez le fichier SFS-Discovery-Workbook. 3. Dans la feuille de travail Server-Data, dans les colonnes A à H, entrez les informations que vous avez collectées sur les serveurs sources. Remarques : • Dans la colonne Wave # (C), entrez le nom de la vague (tel que`Wave1`), out-of-scope (`OOS`) ou`Retire`. • Si la colonne de contact du propriétaire de	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	l'application (H) est indiquée, vérifiez que l'adresse e-mail est correcte. Cette adresse e-mail est automatiq uement générée en fonction du nom que vous avez indiqué dans la colonne Propriétaire de l'application (G). Si nécessaire, mettez à jour manuellement la valeur pour qu'elle reflète la bonne adresse e-mail. • Ne modifiez pas les colonnes I—J, qui contiennent des formules. 4. Enregistrez le classeur.	

Plan

Tâche	Description	Compétences requises
Élaborez le plan de vague SFS.	1. Ouvrez le fichier SFS-Disco very-Workbook. 2. Vérifiez que toutes les informations collectées lors de la phase de découverte sont exactes et à jour. 3. Dans la feuille de travail Wave-Sheet, filtrez la colonne SFS wave (K) en fonction de la valeur.	Responsable du développe ment, Responsable du transfert, Ingénieur de migration, Responsable de la migration

Tâche	Description	Compétences requises
	1 Voici une liste de tous les membres SFSs de la première vague. **Note** Une valeur de `0` dans cette colonne indique que le SFS n'est pas concerné par la migration. Cela peut être dû au fait que le SFS est déjà hébergé sur AWS ou parce que les serveurs qui accèdent au partage ne sont pas concernés par la migration. 4. Vérifiez que vous souhaitez les migrer SFSs dans cette vague. Pour plus d'informations sur l'attribution SFSs aux vagues, consultez la section Approches de planification des vagues dans la section Bonnes pratiques. 5. Sélectionnez et copiez les cellules contenant les valeurs filtrées. Ne copiez pas la ligne d'en-	

Tâche	Description	Compétences requises
	tête contenant les titres des colonnes. 6. Ouvrez le fichier SFS-Wave-Plan-Workbook que vous avez précédemment téléchargé. 7. Dans la feuille de travail Export-from-Discovery, sélectionnez la cellule A2. 8. Collez les données copiées. 9. Enregistrez les fichiers SFS-Discovery-Workbook et SFS-Wave-Plan-Work book.	

Tâche	Description	Compétences requises
Choisissez le service AWS et l'outil de migration cibles.	1. Dans le SFS-Wave-Plan-Workbook fichier, sur la Exported-from-Discovery feuille de travail, sélectionnez et copiez les valeurs de la colonne Ancien chemin (C). 2. Dans la feuille de travail Build-Wave, sélectionnez la cellule A2. 3. Collez les données copiées. Les colonnes B à M de cette feuille de travail sont automatiquement mises à jour pour refléter les autres données associées à ce chemin. 4. Supprimez toutes les valeurs dupliquées dans la colonne A. Pour obtenir des instructions, voir Supprimer les valeurs dupliquées (site Web du Microsoft Support). 5. Dans la colonne Modèle ou service cible (F), passez en revue le service AWS cible recommandé et mettez-le à jour si nécessaire. Pour plus d'informations, consultez Choisir un service de système de fichiers AWS dans la section Bonnes pratiques de ce modèle.	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	6. Dans la colonne Méthode de migration (G), passez en revue l'outil de migration recommandé et mettez-le à jour si nécessaire. Pour plus d'informations, consultez la section Choix d'un outil de migration dans la section Meilleures pratiques de ce modèle. 7. Enregistrez le fichier SFS-Discovery-Workbook. Vous avez fini de créer un plan de vague pour cette vague. 8. Répétez ces instructions pour préparer un plan de vagues pour chaque vague. Les plans de vagues étant susceptibles de changer au cours de la migration, nous vous recommandons de ne pas planifier plus de 5 vagues à l'avance.	

Préparation

Tâche	Description	Compétences requises
Configurez le système de fichiers cible.	Selon les informations enregistrées dans votre plan de vague, configurez les systèmes de fichiers cibles dans le compte AWS, le VPC et les sous-réseaux cibles.	Ingénieur en migration, responsable de la migration, administrateur AWS

Tâche	Description	Compétences requises
	Pour obtenir des instructions, consultez la documentation AWS suivante : • Amazon EFS • Amazon FSx pour NetApp ONTAP • Serveur FSx de fichiers Amazon pour Windows	

Tâche	Description	Compétences requises
Configurez l'outil de migration et transférez les données.	1. Si vous utilisez AWS DataSync, configurez la journalisation des DataSync tâches. Pour obtenir des instructions, consultez la section Journalisation des activités de vos DataSync tâches AWS. 2. Configurez l'outil de migration et effectuez un transfert de données initial conformément aux instructions de l'outil sélectionné : • Pour Amazon EFS, consultez les rubriques suivantes : • Transférer des fichiers vers Amazon EFS à l'aide d'AWS DataSync • Pour Amazon FSx pour ONTAP, consultez ce qui suit : • Migration vers FSx for ONTAP à l'aide de NetApp SnapMirror • Migration vers FSx for ONTAP à l'aide d'AWS DataSync • Pour le serveur de fichiers Amazon FSx pour Windows, consultez ce qui suit :	Administrateur AWS, administrateur cloud, ingénieur de migration, responsable de la migration

Tâche	Description	Compétences requises
	• Migration de fichiers existants vers un serveur FSx de fichiers Windows à l'aide d'AWS DataSync • Migration de fichiers existants vers un serveur de fichiers Windows FSx à l'aide de Robocopy 3. Des modifications peuvent être apportées au SFS source pendant ou après le transfert initial. Configurez des transferts de données récurrents entre les systèmes de fichiers source et cible pour assurer la synchronisation des données : • Si vous en utilisez DataSync, consultez la section Planification de votre DataSync tâche AWS. DataSync transfère uniquement les fichiers modifiés ou nouveaux dans le SFS source. • Si vous utilisez un outil tiers, consultez la documentation de l'outil que vous avez sélection né.	

Tâche	Description	Compétences requises
Mettez à jour le plan des vagues.	1. Ouvrez le fichier SFS-Wave-Plan-Workbook pour la vague en cours. 2. Dans la feuille de travail Build—Wave, dans la colonne New path IP address (N), entrez l'adresse IP du système de fichiers cible. Procédez de l'une des manières suivantes pour localiser l'adresse IP : • FSx Pour Windows File Server, sur la FSx console Amazon, choisissez Systèmes de fichiers, choisissez votre système de fichiers, puis consultez la section Réseau et sécurité. • FSx Pour ONTAP, voir Montage des volumes. • Pour Amazon EFS, consultez la section Montage avec une adresse IP. 3. Dans la colonne Nouveau chemin (O), entrez le nouveau chemin de montage. Le chemin de montage est le nom DNS du système de fichiers. Procédez de l'une des	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	manières suivantes pour localiser le chemin de montage : • FSx Pour Windows File Server, sur la FSx console Amazon, choisissez Systèmes de fichiers, choisissez votre système de fichiers, puis choisissez Joindre. • FSx Pour ONTAP, consultez la page de détails du système de fichiers. Pour obtenir des instructions, reportez-vous à la section Montage des volumes. • Pour Amazon EFS, consultez la section Collecter des informations. 4. Dans la feuille de travail Remount-Summary, vérifiez que les colonnes Nouveau chemin (C) et Adresse IP du nouveau chemin (D) reflètent les valeurs mises à jour. 5. Vérifiez que votre organisation a préparé des runbooks pour le remontage des systèmes de fichiers Linux et Windows après le transfert. Pour obtenir	

Tâche	Description	Compétences requises
	des instructions générales , consultez les rubriques suivantes : • Montage de systèmes de fichiers EFS • Accès FSx aux partages de fichiers du serveur de fichiers Windows • Montage FSx pour volumes ONTAP 6. Si aucun serveur dépendant n'est inclus dans cette vague, enregistrez-le sur la feuille de travail App-Team-Communication. Informez les propriéta ires de l'application ou du serveur concernés, car ils risquent de ne pas être inclus dans les communica tions par ondes standard. 7. S' SFSs ils sont retirés de la vague après avoir terminé le plan de vague, suivez-les sur la feuille de travail Descoped.	

Découper

Tâche	Description	Compétences requises
Arrêtez les applications.	Si des applications ou des clients effectuent activemen	Propriétaire de l'application, développeur de l'application

Tâche	Description	Compétences requises
	t des opérations de lecture et d'écriture dans le SFS source, arrêtez-les avant de procéder à la synchronisation finale des données. Pour obtenir des instructions, consultez la documentation de l'applica tion ou vos processus internes pour arrêter les activités de lecture et d'écriture. Par exemple, consultez Démarrer ou arrêter le serveur Web (IIS 8) (documentation Microsoft) ou Gestion des services système avec systemctl (documentation Red Hat).	

Tâche	Description	Compétences requises
Effectuez le transfert de données final.	1. Dans l'outil de migration , exécutez manuellement une tâche ou une tâche de transfert de données finale pour synchroniser le système de fichiers cible avec le SFS source. Pour obtenir des instructions, consultez la section Démarrer votre DataSync tâche ou consultez la documentation de l'outil de migration tiers que vous avez sélectionné. 2. Attendez que la tâche de transfert de données soit terminée. Pour plus d'informations, consultez AWS Monitoring AWS DataSync activity with Amazon CloudWatch et Monitoring your DataSync task depuis la ligne de commande.	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
Validez le transfert de données.	Si vous utilisez AWS DataSync, procédez comme suit pour valider le transfert de données final effectué avec succès : 1. Dans la DataSync console AWS, notez la tâche et l'ID d'exécution, tels que `task-0000-exec-1111` . 2. Accédez à la section Enregistrement des tâches de la DataSync tâche. 3. Choisissez le lien vers le groupe de CloudWatch journaux. 4. Dans les journaux, recherchez la tâche et l'ID d'exécution. 5. Prenez note de toute erreur de transfert. Pour plus d'informations, consultez la section Erreurs courantes dans la DataSync documentation. 6. Validez les éléments suivants : • Comparez les listes de fichiers de la source et de la cible SFSs pour confirmer que toutes les données ont été transféré es	Ingénieur en migration, responsable de la migration

Tâche	Description	Compétences requises
	• Comparez les autorisations d'accès aux fichiers entre la source et la cible SFSs. Si vous utilisez un outil tiers, consultez les instructions de validation du transfert de données dans la documentation de l'outil de migration sélectionné.	

Valider

Tâche	Description	Compétences requises
Remontez le système de fichiers et validez le fonctionnement et les performances de l'application.	1. Si des serveurs dépendants ont été migrés au cours de cette vague, dans le fichier SFS-Wave-Plan-Workbook, sur la feuille de travail Remount-Summary, entrez la nouvelle adresse IP du serveur dans la colonne Nouvelle adresse IP du serveur (F). 2. Sur tous les serveurs, mettez à jour le point de montage du système de fichiers de l'ancien chemin vers le nouveau. Utilisez le runbook de votre organisation pour le remontage dont il a été question	Administrateur système AWS, propriétaire de l'application

Tâche	Description	Compétences requises
	précédemment dans la phase de préparation. 3. Vérifiez que le système de fichiers est correctement monté et qu'il est accessible en vérifiant les montages et en vérifiant la présence de fichiers. L'équipe chargée de l'infrastructure effectue généralement ces activités. 4. Redémarrez les applications et demandez aux propriétaires de l'application ou à l'équipe d'assurance qualité d'effectuer des tests fonctionnels et de performance sur l'application, selon les besoins de l'application.	

Résolution des problèmes

Problème	Solution
Les valeurs des cellules dans Microsoft Excel ne sont pas mises à jour.	Copiez les formules dans les lignes d'exemple en faisant glisser la poignée de remplissage. Pour plus d'informations, consultez les instructions pour Windows ou pour Mac (site Web du Support Microsoft).

Ressources connexes

Documentation AWS

- DataSync Documentation AWS
- Documentation Amazon EFS
- FSx Documentation Amazon
- Migrations de grande envergure vers le cloud AWS
  - Guide pour les migrations AWS à grande échelle
  - Guide de portefeuille pour les migrations AWS à grande échelle

Dépannage

- Résolution des problèmes DataSync liés à AWS
- Résolution des problèmes liés à Amazon EFS
- Résolution des problèmes liés au serveur de fichiers Amazon FSx pour Windows
- Résolution des problèmes liés à Amazon FSx pour NetApp ONTAP

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Migrer une base de données Oracle vers Amazon RDS for Oracle à l'aide d'adaptateurs de GoldenGate fichiers plats Oracle

Créée par Dhairya Jindani (AWS) et Baji Shaik (AWS)

Récapitulatif

Oracle GoldenGate est un service de capture et de réplication de données en temps réel pour les bases de données et les environnements informatiques hétérogènes. Toutefois, ce service ne prend actuellement pas en charge Amazon Relational Database Service (Amazon RDS) pour Oracle. Pour obtenir la liste des bases de données prises en charge, consultez Oracle GoldenGate pour les bases de données hétérogènes (documentation Oracle). Ce modèle décrit comment utiliser les adaptateurs de fichiers GoldenGate plats Oracle GoldenGate et Oracle pour générer des fichiers plats à partir de la base de données Oracle source, qui peut se trouver sur site ou sur une instance Amazon Elastic Compute Cloud (Amazon EC2). Vous pouvez ensuite importer ces fichiers plats dans une instance de base de données Amazon RDS for Oracle.

Dans ce modèle, vous utilisez Oracle GoldenGate pour extraire les fichiers de suivi de votre base de données Oracle source. La pompe de données copie les fichiers de suivi sur un serveur d'intégration, qui est une EC2 instance Amazon. Sur le serveur d'intégration, Oracle GoldenGate utilise l'adaptateur de fichiers plats pour générer une série de fichiers plats séquentiels basés sur la capture des données transactionnelles des fichiers de suivi. Oracle met en GoldenGate forme les données sous forme de valeurs séparées par des délimiteurs ou de valeurs délimitées par des longueurs. Vous utilisez ensuite Oracle SQL*Loader pour importer les fichiers plats dans l'instance de base de données Amazon RDS for Oracle cible.

Public visé

Ce modèle est destiné à ceux qui ont de l'expérience et des connaissances sur les éléments GoldenGate de base d'un Oracle. Pour plus d'informations, voir Présentation de l' GoldenGate architecture Oracle (documentation Oracle).

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Une GoldenGate licence Oracle.
- Une licence distincte pour un GoldenGate adaptateur Oracle.
- Une base de données Oracle source, exécutée sur site ou sur une EC2 instance Amazon.

- Une instance Amazon EC2 Linux utilisée comme serveur d'intégration. Pour plus d'informations, consultez Commencer avec les instances Amazon EC2 Linux (EC2 documentation Amazon).
- Une instance de base de données Amazon RDS for Oracle cible. Pour plus d'informations, consultez Création d'une instance de base de données Oracle (documentation Amazon RDS).

Versions du produit

- Oracle Database Enterprise Edition version 10g, 11g, 12c ou ultérieure
- Oracle GoldenGate version 12.2.0.1.1 ou ultérieure

Architecture

Pile technologique source

Une base de données Oracle (sur site ou sur une EC2 instance Amazon)

Pile technologique cible

Amazon RDS for Oracle

Architecture source et cible

1. Oracle GoldenGate extrait les traces des journaux de la base de données source.
2. La pompe de données extrait les traces et les fait migrer vers un serveur d'intégration.
3. L'adaptateur de fichier GoldenGate plat Oracle lit les traces, les définitions de source et les paramètres d'extraction.
4. Vous quittez l'extraction, qui génère un fichier de contrôle et des fichiers de données plats.
5. Vous migrez les fichiers de données plats vers une instance de base de données Amazon RDS for Oracle dans le AWS Cloud.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.

- Amazon Relational Database Service (Amazon RDS) pour Oracle vous aide à configurer, exploiter et dimensionner une base de données relationnelle Oracle dans le. AWS Cloud

Autres services

- Oracle GoldenGate est un service qui vous aide à répliquer, filtrer et transformer les données d'une base de données vers une autre base de données hétérogène ou vers une autre topologie cible, telle que des fichiers plats.
- Les adaptateurs GoldenGate d'application Oracle permettent GoldenGate à Oracle de produire une série de fichiers plats séquentiels et de fichiers de contrôle à partir des données transactionnelles capturées dans les fichiers de suivi d'une base de données source. Ces adaptateurs sont largement utilisés pour les opérations d'extraction, de transformation et de chargement (ETL) dans les applications d'entrepôt de données et les applications propriétaires ou existantes. Oracle GoldenGate effectue cette capture et l'applique en temps quasi réel sur des bases de données, des plateformes et des systèmes d'exploitation hétérogènes. Les adaptateurs prennent en charge différents formats pour les fichiers de sortie, tels que CSV ou Apache Parquet. Vous pouvez charger ces fichiers générés afin de charger les données dans différentes bases de données hétérogènes.

Épopées

Configuration d'Oracle GoldenGate sur le serveur de base de données source

Tâche	Description	Compétences requises
Téléchargez Oracle GoldenGate.	Sur le serveur de base de données source, téléchargez Oracle GoldenGate version 12.2.0.1.1 ou ultérieure. Pour obtenir des instructions, voir Téléchargement d'Oracle GoldenGate (documentation Oracle).	DBA
Installez Oracle GoldenGate.	Pour obtenir des instructi ons, voir Installation d'Oracle	DBA

Tâche	Description	Compétences requises
	GoldenGate (documentation Oracle).	
Configurez Oracle GoldenGate.	Pour obtenir des instructions, voir Préparation de la base de données pour Oracle GoldenGate (documentation Oracle).	DBA

Configuration d'Oracle GoldenGate sur le serveur d'intégration

Tâche	Description	Compétences requises
Téléchargez Oracle GoldenGate.	Sur le serveur d'intégration, téléchargez la GoldenGate version 12.2.0.1.1 ou ultérieure d'Oracle. Pour obtenir des instructions, voir Téléchargement d'Oracle GoldenGate (documentation Oracle).	DBA
Installez Oracle GoldenGate.	Créez des répertoires, configurez le processus de gestion et créez le `defgen` fichier pour un environnement hétérogène. Pour obtenir des instructions, voir Installation d'Oracle GoldenGate (documentation Oracle).	DBA

Modifier la configuration de capture GoldenGate de données Oracle

Tâche	Description	Compétences requises
Préparez les GoldenGate adaptateurs Oracle.	Sur le serveur d'intégration, configurez le logiciel de l' GoldenGate adaptateur Oracle. Procédez comme suit : 1. À partir d'Oracle Software Delivery Cloud, téléchargez ggs_Adapters_Linux_x64.zip. 2. Décompressez ggs_Adapters_Linux_x64.zip. 3. Exécutez la commande suivante pour installer les adaptateurs : `tar -xvf ggs_Adapters_Linux_x64.tar`	DBA
Configurez la pompe de données.	Sur le serveur source, configurez la pompe de données pour transférer le fichier de suivi du serveur source vers le serveur d'intégration. Créez le fichier de paramètres de la pompe de données et le répertoire des fichiers de suivi. Pour obtenir des instructions, voir Configuration de l'adaptateur de fichiers plats (documentation Oracle).	DBA

Génération et migration des fichiers plats

Tâche	Description	Compétences requises
Générez les fichiers plats.	Créez le fichier d'extrait et le fichier de contrôle, puis lancez le processus d'extraction sur le serveur d'intégration. Cela extrait les modifications de base de données et écrit la base de données source dans les fichiers plats. Pour obtenir des instructions, voir Utilisation de l'adaptateur de fichiers plats (documentation Oracle).	DBA
Chargez les fichiers plats dans la base de données cible.	Chargez les fichiers plats dans l'instance de base de données Amazon RDS for Oracle cible. Pour plus d'informations, consultez Importation à l'aide d'Oracle SQL*Loader (documentation Amazon RDS).	DBA

Résolution des problèmes

Problème	Solution
L'adaptateur de fichiers GoldenGate plats Oracle génère une erreur.	Pour une description des erreurs de l'adaptateur, voir Localisation des messages d'erreur (documentation Oracle). Pour obtenir des instructions de dépannage, voir Résolution des problèmes liés à l'adaptateur de fichiers plats (documentation Oracle).

Ressources connexes

- Installation d'Oracle GoldenGate (documentation Oracle)
- Configuration d'Oracle GoldenGate (documentation Oracle)
- Comprendre les GoldenGate adaptateurs Oracle (documentation Oracle)
- Configuration de l'adaptateur de fichiers plats (documentation Oracle)

Modifier les applications Python et Perl pour prendre en charge la migration de bases de données de Microsoft SQL Server vers Amazon Aurora PostgreSQL Compatible Edition

Créée par Dwarika Patra (AWS) et Deepesh Jayaprakash (AWS)

Récapitulatif

Ce modèle décrit les modifications apportées aux référentiels d'applications qui peuvent être nécessaires lorsque vous migrez des bases de données de Microsoft SQL Server vers Amazon Aurora PostgreSQL Compatible Edition. Le modèle suppose que ces applications sont basées sur Python ou Perl, et fournit des instructions distinctes pour ces langages de script.

La migration de bases de données SQL Server vers une version compatible avec Aurora PostgreSQL implique la conversion de schémas, la conversion d'objets de base de données, la migration de données et le chargement de données. En raison des différences entre PostgreSQL et SQL Server (relatives aux types de données, aux objets de connexion, à la syntaxe et à la logique), la tâche de migration la plus difficile consiste à apporter les modifications nécessaires à la base de code afin qu'elle fonctionne correctement avec PostgreSQL.

Pour une application basée sur Python, les objets et les classes de connexion sont dispersés dans tout le système. En outre, la base de code Python peut utiliser plusieurs bibliothèques pour se connecter à la base de données. Si l'interface de connexion à la base de données change, les objets qui exécutent les requêtes en ligne de l'application doivent également être modifiés.

Pour une application basée sur Perl, les modifications concernent les objets de connexion, les pilotes de connexion à la base de données, les instructions SQL en ligne statiques et dynamiques, ainsi que la façon dont l'application gère les requêtes DML dynamiques complexes et les ensembles de résultats.

Lorsque vous migrez votre application, vous pouvez également envisager d'apporter des améliorations à AWS, telles que le remplacement du serveur FTP par un accès Amazon Simple Storage Service (Amazon S3).

Le processus de migration des applications comporte les défis suivants :

- Objets de connexion. Si les objets de connexion sont dispersés dans le code avec plusieurs bibliothèques et appels de fonctions, vous devrez peut-être trouver un moyen généralisé de les modifier pour qu'ils soient compatibles avec PostgreSQL.

- Gestion des erreurs ou des exceptions lors de la récupération ou des mises à jour des enregistrements. Si vous effectuez des opérations conditionnelles de création, de lecture, de mise à jour et de suppression (CRUD) sur la base de données qui renvoient des variables, des ensembles de résultats ou des blocs de données, toute erreur ou exception peut entraîner des erreurs d'application avec des effets en cascade. Celles-ci doivent être traitées avec soin, avec des validations appropriées et des points de sauvegarde. L'un de ces points de sauvegarde consiste à appeler de grandes requêtes SQL en ligne ou des objets de base de données à l'intérieur de `BEGIN...EXCEPTION...END` blocs.
- Contrôle des transactions et de leur validation. Cela inclut les validations et annulations manuels et automatiques. Le pilote PostgreSQL pour Perl vous oblige à toujours définir explicitement l'attribut de validation automatique.
- Gestion des requêtes SQL dynamiques. Cela nécessite une solide compréhension de la logique des requêtes et des tests itératifs pour garantir que les requêtes fonctionnent comme prévu.
- Rendement. Vous devez vous assurer que les modifications du code n'entraînent pas de dégradation des performances des applications.

Ce modèle explique le processus de conversion en détail.

Conditions préalables et limitations

Prérequis

- Connaissance pratique de la syntaxe Python et Perl.
- Compétences de base en SQL Server et PostgreSQL.
- Compréhension de l'architecture de votre application existante.
- Accès au code de votre application, à la base de données SQL Server et à la base de données PostgreSQL.
- Accès à l'environnement de développement Windows ou Linux (ou autre Unix) avec des informations d'identification pour développer, tester et valider les modifications apportées aux applications.
- Pour une application basée sur Python, les bibliothèques Python standard dont votre application peut avoir besoin, telles que Pandas pour gérer les trames de données et psycopg2 ou pour les connexions aux bases de données. SQLAlchemy
- Pour une application basée sur Perl, des packages Perl avec des bibliothèques ou des modules dépendants sont nécessaires. Le module Comprehensive Perl Archive Network (CPAN) peut répondre à la plupart des exigences des applications.

- Toutes les bibliothèques ou modules personnalisés dépendants requis.
- Informations d'identification de base de données pour l'accès en lecture à SQL Server et l'accès en lecture/écriture à Aurora.
- PostgreSQL pour valider et déboguer les modifications apportées aux applications avec les services et les utilisateurs.
- Accès aux outils de développement lors de la migration d'applications, tels que Visual Studio Code, Sublime Text ou pgAdmin.

Limites

- Certaines versions, modules, bibliothèques et packages de Python ou Perl ne sont pas compatibles avec l'environnement cloud.
- Certaines bibliothèques et frameworks tiers utilisés pour SQL Server ne peuvent pas être remplacés pour prendre en charge la migration vers PostgreSQL.
- Les variations de performances peuvent nécessiter des modifications de votre application, des requêtes Transact-SQL (T-SQL) en ligne, des fonctions de base de données et des procédures stockées.
- PostgreSQL prend en charge les noms en minuscules pour les noms de tables, les noms de colonnes et les autres objets de base de données.
- Certains types de données, tels que les colonnes UUID, sont stockés en minuscules uniquement. Les applications Python et Perl doivent gérer de telles différences de cas.
- Les différences de codage de caractères doivent être gérées avec le type de données approprié pour les colonnes de texte correspondantes dans la base de données PostgreSQL.

Versions du produit

- Python 3.6 ou version ultérieure (utilisez la version compatible avec votre système d'exploitation)
- Perl 5.8.3 ou version ultérieure (utilisez la version compatible avec votre système d'exploitation)
- Aurora PostgreSQL Compatible Edition 4.2 ou version ultérieure (voir les détails)

Architecture

Pile technologique source

- Langage de script (programmation d'applications) : Python 2.7 ou version ultérieure, ou Perl 5.8
- Base de données : Microsoft SQL Server version 13
- Système d'exploitation : Red Hat Enterprise Linux (RHEL) 7

Pile technologique cible

- Langage de script (programmation d'applications) : Python 3.6 ou version ultérieure, ou Perl 5.8 ou version ultérieure
- Base de données : Aurora PostgreSQL 4.2 compatible
- Système d'exploitation : RHEL 7

Architecture de migration

Outils

Services et outils AWS

- Aurora PostgreSQL—Compatible Edition est un moteur de base de données relationnelle entièrement géré, compatible avec PostgreSQL et ACID qui associe la vitesse et la fiabilité des bases de données commerciales haut de gamme à la rentabilité des bases de données open source. Aurora PostgreSQL remplace directement PostgreSQL et permet de configurer, d'exploiter et de dimensionner vos déploiements PostgreSQL nouveaux et existants de manière plus simple et plus rentable.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS en utilisant des commandes dans votre shell de ligne de commande.

Autres outils

- bibliothèques de connexion aux bases de données Python et PostgressQL telles que psycopg2 et SQLAlchemy
- Perl et ses modules DBI
- Terminal interactif PostgreSQL (psql)

Épopées

Migrez votre référentiel d'applications vers PostgreSQL : étapes de haut niveau

Tâche	Description	Compétences requises
Suivez ces étapes de conversion de code pour migrer votre application vers PostgreSQL.	1. Définissez des pilotes et des bibliothèques ODBC spécifiques à la base de données pour PostgreSQL. Par exemple, vous pouvez utiliser l'un des modules CPAN pour Perl et pyodbc, psycopg2 ou Python. SQLAlchemy 2. Convertissez des objets de base de données à l'aide de ces bibliothèques pour vous connecter à Aurora PostgreSQL compatible. 3. Appliquez des modifications de code dans les modules d'application existants pour obtenir des instructions T-SQL compatibles. 4. Réécrivez les appels de fonction et les procédures stockées spécifiques à la base de données dans le code de l'application. 5. Gérez les modifications apportées aux variables de votre application et à leurs types de données utilisés pour les requêtes SQL en ligne.	Développeur d’applications

Tâche	Description	Compétences requises
	6. Gérez les fonctions incompatibles spécifiques à la base de données. 7. end-to-endTest complet du code d'application converti pour la migration de base de données. 8. Comparez les résultats de Microsoft SQL Server à ceux de l'application que vous avez migrée vers PostgreSQL. 9. Réalisez une analyse comparative des performances des applications entre Microsoft SQL Server et PostgreSQL. 10. Révisez les procédures stockées ou les instructions T-SQL en ligne appelées par l'application pour améliorer les performances. Les epics suivants fournissent des instructions détaillées pour certaines de ces tâches de conversion pour les applications Python et Perl.	

Tâche	Description	Compétences requises
Utilisez une liste de contrôle pour chaque étape de la migration.	Ajoutez les éléments suivants à votre liste de contrôle pour chaque étape de la migration des applications, y compris la dernière étape : • Consultez la documentation de PostgreSQL pour vous assurer que toutes vos modifications sont compatibles avec le standard PostgreSQL. • Vérifiez les valeurs entières et flottantes pour les colonnes. • Identifiez le nombre de lignes insérées, mises à jour et extraites, ainsi que les noms des colonnes et les horodatages. Vous pouvez utiliser un utilitaire de comparaison ou écrire un script pour automatiser ces vérifications. • Effectuez des contrôles de performance pour les instructions SQL intégrées de grande taille et vérifiez les performances globales de l'application. • Vérifiez que les erreurs sont correctement gérées pour les opérations de base de données et que vous quittez	Développeur d’applications

Tâche	Description	Compétences requises
	le programme correctement en utilisant plusieurs blocs try/catch. • Vérifiez que les processus de journalisation appropriés sont en place.	

Analyser et mettre à jour votre application — Base de code Python

Tâche	Description	Compétences requises
Analysez votre base de code Python existante.	Votre analyse doit inclure les éléments suivants pour faciliter le processus de migration des applications : • Identifiez tous les objets de connexion dans le code. • Identifiez toutes les requêtes SQL en ligne incompatibles (telles que les instructions T-SQL et les procédures stockées) et analysez les modifications requises. • Consultez la documenta tion de votre code et suivez le flux de contrôle pour comprendre les fonctionn alités du code. Cela vous sera utile ultérieurement lorsque vous testerez l'application pour des	Développeur d’applications

Tâche	Description	Compétences requises
	comparaisons de performances ou de charge. • Comprenez l'objectif de l'application afin de pouvoir la tester efficacement après la conversion de la base de données. La plupart des applications Python susceptibles d'être converties par des migrations de bases de données sont soit des flux qui chargent des données provenant d'autres sources dans des tables de base de données, soit des extracteurs qui extraient les données des tables et les transforment en différents formats de sortie (tels que CSV, JSON ou fichiers plats) adaptés à la création de rapports ou aux appels d'API pour effectuer des validations.	

Tâche	Description	Compétences requises
Convertissez vos connexions de base de données pour qu'elles soient compatibles avec PostgreSQL.	La plupart des applications Python utilisent la bibliothèque pyodbc pour se connecter aux bases de données SQL Server comme suit. `import pyodbc .... try: conn_string = "Driver=ODBC Driver 17 for SQL Server;UID={};PWD={};Server={};Database={}".format (conn_user, conn_password, conn_server, conn_database) conn = pyodbc.connect(conn_string) cur = conn.cursor() result = cur.execute(query_string) for row in result: print (row) except Exception as e: print(str(e))` Convertissez la connexion à la base de données pour qu'elle prenne en charge PostgreSQL comme suit. `import pyodbc import psycopg2 .... try:`	Développeur d’applications

Tâche	Description	Compétences requises

	``
	  conn_string =
	  'postgresql+psycop
	g2://'+
	  conn_user+':'+conn
	_password+'@'+conn
	_server+'/'+conn_d
	atabase
	  conn = pyodbc.co
	nnect(conn_string,
	  connect_args={'opt
	ions':'-csearch_pa
	th=dbo'})
	  cur = conn.cursor()
	  result = cur.execu
	te(query_string)
	  for row in result:
	  print (row)
	except Exception as e:
	  print(str(e))
	``	

Tâche	Description	Compétences requises

Remplacez les requêtes SQL en ligne par PostgreSQL.	Convertissez vos requêtes SQL en ligne dans un format compatible avec PostgreSQL. Par exemple, la requête SQL Server suivante extrait une chaîne d'une table.
	
	`dtype = “type1”`
	`stm = ‘“SELECT TOP 1 searchcode FROM TypesTable (NOLOCK) WHERE code=”’ + “’” + str(dtype) + “’”`
	`# For Microsoft SQL Server Database Connection`
	`engine = create_engine(‘mssql+pyodbc:///?odbc_connect=%s’ % urllib.parse.quote_plus(conn_string), connect_args={‘connect_timeout’:login_timeout})`
	`conn = engine_connect()`
	`rs = conn.execute(stm)`
	`for row in rs:`
	`  print(row)`
	
	Après la conversion, la requête SQL en ligne compatible avec PostgreSQL se présente comme suit.
	
	`dtype = “type1”`
	`stm = ‘“SELECT searchcode FROM TypesTable`
		Développeur d’applications

Tâche	Description	Compétences requises

	WHERE code=”’ + “’” + str(dtype) + “’ LIMIT 1”
	# For PostgreSQL Database Connection
	engine = create_engine(‘postgres+psycopg2://%s’ %conn_string, connect_args={‘connect_timeout’:login_timeout})
	conn = engine.connect()
	rs = conn.execute(stm)
	for row in rs:
	print(row)	

Tâche	Description	Compétences requises

Gérez les requêtes SQL dynamiques.	Le SQL dynamique peut être présent dans un ou plusieurs scripts Python. Les exemples précédents montraient comment utiliser la fonction de remplacement de chaîne de Python pour insérer des variables afin de créer des requêtes SQL dynamiques. Une autre approche consiste à ajouter des variables à la chaîne de requête, le cas échéant.
	
	Dans l'exemple suivant, la chaîne de requête est construite à la volée en fonction des valeurs renvoyées par une fonction.
	
	`query = '"SELECT id from equity e join issues i on e.permId=i.permId where e.id'"`
	`query += get_id_filter(ids) + " e.id is NOT NULL`
	
	Ces types de requêtes dynamiques sont très courants lors de la migration d'applications. Pour gérer les requêtes dynamiques, procédez comme suit :
		Développeur d'applications

Tâche	Description	Compétences requises
	• Vérifiez la syntaxe globale (par exemple, la syntaxe de l'`SELECT`instruction contenant une `JOIN` clause). • Vérifiez toutes les variables ou les noms de colonnes utilisés dans la requête, tels que `i` et`id`. • Vérifiez les fonctions, les arguments et les valeurs de retour utilisés dans la requête (par exemple, `get_id_filter` et son argument`ids`).	

Tâche	Description	Compétences requises

Gérez les ensembles de résultats, les variables et les blocs de données.	Pour Microsoft SQL Server, vous utilisez des méthodes Python telles que `fetchone()` ou `fetchall()` pour récupérer le jeu de résultats de la base de données. Vous pouvez également utiliser `fetchmany(size)` et spécifier le nombre d'enregis trements à renvoyer à partir de l'ensemble de résultats. Pour ce faire, vous pouvez utiliser l'objet de connexion pyodbc comme indiqué dans l'exemple suivant.
	
	pyodbc (Microsoft SQL Server)
	
	`import pyodbc`
	`server = 'tcp:myse`
	`rver.database.wind`
	`ows.net'`
	`database = 'exampledb'`
	`username = 'exampleu`
	`sername'`
	`password = 'examplep`
	`assword'`
	`conn = pyodbc.co`
	`nnect('DRIVER={ODB`
	`C Driver 17 for SQL`
	` Server};SERVER='+s`
	`erver+';DATABASE='`
	`+database+';UID='+`
	`username+';PWD='+`
	` password)`
	`cursor = conn.cursor()`
		Développeur d’applications

Tâche	Description	Compétences requises

	``
	cursor.execute("SELECT
	 * FROM ITEMS")
	row = cursor.fe
	tchone()
	while row:
	    print(row[0])
	    row = cursor.fe
	tchone()
	``	

	Dans Aurora, pour effectuer des tâches similaires telles que la connexion à PostgreSQL et l'extraction de jeux de résultats, vous pouvez utiliser psycopg2 ou. SQLAlchemy Ces bibliothèques Python fournissent le module de connexion et l'objet curseur permettant de parcourir les enregistrements de la base de données PostgreSQL, comme illustré dans l'exemple suivant.	
	psycopg2 (compatible avec Aurora PostgreSQL)	

	``
	import psycopg2
	query = "SELECT * FROM
	 ITEMS;"
	//Initialize
	 variables
	host=dbname=user=
	password=port=sslm
	ode=connect_timeou
	t=""
	connstring = "host='{h
	ost}' dbname='{
	``	

Tâche	Description	Compétences requises
	dbname}' user='{user}' \ password='{password}'port='{port}' ".format(host=host,dbname=dbname,\ user=user,password=password,port=port) conn = psycopg2.connect(connstring) cursor = conn.cursor() cursor.execute(query) column_names = [column[0] for column in cursor.description] print("Column Names: ", column_names) print("Column values: " for row in cursor: print("itemid :", row[0]) print("itemdescription :", row[1]) print("itemprice :", row[3]))	
	SQLAlchemy (Compatible avec Aurora PostgreSQL) from sqlalchemy import create_engine from pandas import DataFrame conn_string = 'postgresql://core:database@localhost:5432/exampledatabase' engine = create_engine(conn_string)	

Tâche	Description	Compétences requises
	conn = engine.co nnect() dataid = 1001 result = conn.exec ute("SELECT * FROM ITEMS") df = DataFrame (result.fetchall()) df.columns = result.ke ys() df = pd.DataFrame() engine.connect() df = pd.read_sql_query(sql_query, engine, coerce_float=False) print(“df=”, df)	

Tâche	Description	Compétences requises
Testez votre application pendant et après la migration.	Le test de l'application Python migrée est un processus continu. Étant donné que la migration inclut des modifications d'objets de connexion (psycopg2 ou SQLAlchemy), la gestion des erreurs, de nouvelles fonctionnalités (blocs de données), des modifications du code SQL intégré, des fonctionnalités de copie en bloc (`bcp`au lieu de`COPY`) et des modifications similaires, elle doit être testée avec soin pendant et après la migration de l'application. Vérifiez : • Conditions d'erreur et gestion • Toute anomalie d'enregistrement après la migration • Enregistrer les mises à jour ou les suppressions • Temps nécessaire pour exécuter l'application	Développeur d’applications

Analyser et mettre à jour votre application — Base de code Perl

Tâche	Description	Compétences requises
Analysez votre base de code Perl existante.	Votre analyse doit inclure les éléments suivants pour faciliter le processus de	Développeur d’applications

Tâche	Description	Compétences requises
	migration des applications. Vous devez identifier : • Tout code INI ou basé sur la configuration • Pilotes Perl standard ODBC (Open Database Connectivity) spécifiques à la base de données ou tout autre pilote personnalisé • Modifications de code requises pour les requêtes en ligne et T-SQL • Interactions entre différents modules Perl (par exemple, un seul objet de connexion ODBC Perl appelé ou utilisé par plusieurs composants fonctionnels) • Gestion des ensembles de données et des ensembles de résultats • Bibliothèques Perl externes et dépendantes • Tous APIs ceux utilisés dans l'application • Compatibilité des versions de Perl et compatibilité des pilotes avec Aurora PostgreSQL compatible	

Tâche	Description	Compétences requises

Convertissez les connexions de l'application Perl et du module DBI pour qu'elles soient compatibles avec PostgreSQL.	Les applications basées sur Perl utilisent généralement le module Perl DBI, qui est un module d'accès aux bases de données standard pour le langage de programmation Perl. Vous pouvez utiliser le même module DBI avec différents pilotes pour SQL Server et PostgreSQL.
	
	Pour plus d'informations sur les modules Perl requis, les installations et les autres instructions, consultez la documentation DBD : :Pg. L'exemple suivant se connecte à Aurora PostgreSQL compatible à l'adresse. `exampletest-aurora pg-database.cluste r-sampleclusture.u s-east-.rds.amazon aws.com`
	
	`#!/usr/bin/perl`
	`use DBI;`
	`use strict;`
	`my $driver = "Pg";`
	`my $hostname = “examplet`
	`est-aurorapg-datab`
	`ase-sampleclusture`
	`.us-east.rds.amazo`
	`naws.com”`
	`my $dsn = "DBI:$driver:`
	` dbname = $hostname`
		Développeur d’applications

Tâche	Description	Compétences requises
	;host = 127.0.0.1;port = 5432"; my $username = "postgres "; my $password = "pass123" ; $dbh = DBI->conn ect("dbi:Pg:dbname =$hostname;host=$h ost;port=$port;opt ions=$options", $username, $password, {AutoCommit => 0, RaiseError => 1, PrintError => 0});	

Tâche	Description	Compétences requises

Remplacez les requêtes SQL en ligne par PostgreSQL.	Votre application peut comporter des requêtes SQL en ligne avec`SELECT`, `DELETEUPDATE`, et des instructions similaires qui incluent des clauses de requête non prises en charge par PostgreSQL. Par exemple, les mots clés de requête tels que `TOP` et `NOLOCK` ne sont pas pris en charge dans PostgreSQL. Les exemples suivants montrent comment vous pouvez gérer les variables `TOP` booléenne s et `NOLOCK` les variables booléennes.
	
	Dans SQL Server :
	
	`$sqlStr = $sqlStr . "WHERE a.student_id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_record b WITH (NOLOCK) \ INNER JOIN student_contributor c WITH (NOLOCK) on c.contributor_id = b.c_st)`
	
	Pour PostgreSQL, convertissez en :
	
	`$sqlStr = $sqlStr`
		Développeur d’applications

Tâche	Description	Compétences requises
	. "WHERE a.student _id in (SELECT TOP $numofRecords c_student_id \ FROM active_student_rec ord b INNER JOIN student_contributor c \ on c.contributor_id = b.c_student_contr_id WHERE b_current_1 is true \ LIMIT $numofRecords)"	

Tâche	Description	Compétences requises
Gérez les requêtes SQL dynamiques et les variables Perl.	Les requêtes SQL dynamiques sont des instructions SQL créées lors de l'exécution de l'application. Ces requêtes sont construites dynamiquement lorsque l'application est en cours d'exécution, en fonction de certaines conditions, de sorte que le texte complet de la requête n'est pas connu avant l'exécution. Par exemple, une application d'analyse financière qui analyse les 10 meilleures actions sur une base quotidienne, et ces actions changent tous les jours. Les tables SQL sont créées en fonction des meilleures performances, et les valeurs ne sont connues qu'au moment de l'exécution. Supposons que les requêtes SQL en ligne de cet exemple soient transmises à une fonction wrapper pour obtenir les résultats définis dans une variable, puis qu'une variable utilise une condition pour déterminer si la table existe : • Si la table existe, ne la créez pas ; effectuez un traitement.	Développeur d’applications

Tâche	Description	Compétences requises

	• Si la table n'existe pas, créez-la et effectuez également un traitement.
	
	Voici un exemple de gestion des variables, suivi des requêtes SQL Server et PostgreSQL pour ce cas d'utilisation.
	
	`my $tableexists = db_read( arg 1, $sql_qry, undef, 'writer'); my $table_already_exists = $tableexists->[0]{table_exists}; if ($table_already_exists){ # do some thing } else { # do something else }`
	
	Serveur SQL :
	
	`my $sql_qry = “SELECT OBJECT_ID('$backendTable', 'U') table_exists", undef, 'writer') ";`
	
	PostgreSQL :
	
	`my $sql_qry = “SELECT TO_REGCLASS('$backendTable', 'U')`	

Tâche	Description	Compétences requises
	table_exists", undef, 'writer')"; L'exemple suivant utilise une variable Perl dans le SQL en ligne, qui exécute une SELECT instruction avec un JOIN pour récupérer la clé primaire de la table et la position de la colonne clé. Serveur SQL : my $sql_qry = "SELECT column_name', character_maxi mum_length \ FROM INFORMATION_SCHEMA .COLUMNS \ WHERE TABLE_SCH EMA='$example_sche maInfo' \ AND TABLE_NAME='$examp le_table' \ AND DATA_TYPE IN ('varchar','nvarch ar');"; PostgreSQL : my $sql_qry = "SELECT c1.column_name, c1.ordinal_position \ FROM information_schema .key_column_usage AS c LEFT \ JOIN information_schema .table_constraints AS t1 \	

Tâche	Description	Compétences requises
	`ON t1.constraint_name = c1.constraint_name \ WHERE t1.table_name = $example_schemaInfo'.'$example_table' \ AND t1.constraint_type = 'PRIMARY KEY' ;";`	

Apportez des modifications supplémentaires à votre application basée sur Perl ou Python pour prendre en charge PostgreSQL

Tâche	Description	Compétences requises
Convertissez des constructions SQL Server supplémentaires en PostgreSQL.	Les modifications suivantes s'appliquent à toutes les applications, quel que soit le langage de programmation. • Qualifiez les objets de base de données utilisés par votre application avec des noms de schéma nouveaux et appropriés. • Gérez les opérateurs LIKE pour une correspondance distinguant majuscules/minuscules avec la fonctionnalité de classement de PostgreSQL. • Gérez les fonctions spécifiques à la base de données non prises en charge `DATEDIFF`, telles que `DATEADD`, `GETDATE`, `CONVE` et `CAST` les opérateur	Développeur d'applications

Tâche	Description	Compétences requises
	s. Pour des fonctions compatibles avec PostgreSQL équivalentes, consultez la section Fonctions SQL natives ou intégrées dans la section Informations supplémentaires. • Gérez les valeurs booléennes dans les instructions de comparaison. • Gérez les valeurs renvoyées par les fonctions. Il peut s'agir d'ensembles d'enregistrements, de cadres de données, de variables et de valeurs booléennes. Gérez-les conformément aux exigences de votre application et pour prendre en charge PostgreSQL. • Gérez les blocs anonymes (tels que`BEGIN TRAN`) avec de nouvelles fonctions PostgreSQL définies par l'utilisateur. • Convertissez les encarts groupés en lignes. L'équivalent pour PostgreSQL de l'utilitaire SQL Server Bulk copy `bcp` (), qui est appelé depuis l'intérieur de l'application, est. `COPY`	

Tâche	Description	Compétences requises
	• Convertissez les opérateurs de concaténation de colonnes. SQL Server utilise + la concaténation de chaînes, mais PostgreSQL l'utilise. | |	

Améliorez les performances

Tâche	Description	Compétences requises
Tirez parti des services AWS pour améliorer les performances.	Lorsque vous migrez vers le cloud AWS, vous pouvez affiner la conception de votre application et de votre base de données afin de tirer parti des services AWS. Par exemple, si les requêtes de votre application Python, connectée à un serveur de base de données compatible Aurora PostgreSQL, prennent plus de temps que vos requêtes Microsoft SQL Server d'origine, vous pouvez envisager de créer un flux de données historiques directement vers un bucket Amazon Simple Storage Service (Amazon S3) depuis le serveur Aurora, et d'utiliser des requêtes SQL basées sur Amazon Athena pour générer des rapports et des requêtes de données analytiques pour	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	votre tableaux de bord utilisateur.	

Ressources connexes

- Perl
- Module DBI Perl
- Python
- psycopg2
- SQLAlchemy
- Copie en bloc - PostgreSQL
- Copie en bloc - Microsoft SQL Server
- PostgreSQL
- Utilisation d'Amazon Aurora PostgreSQL

Informations supplémentaires

La compatibilité avec Microsoft SQL Server et Aurora PostgreSQL est conforme à la norme ANSI SQL. Cependant, vous devez toujours être conscient des incompatibilités liées à la syntaxe, aux types de données de colonne, aux fonctions natives spécifiques à la base de données, aux insertions groupées et à la distinction majuscules/minuscules lorsque vous migrez votre application Python ou Perl de SQL Server vers PostgreSQL.

Les sections suivantes fournissent plus d'informations sur les incohérences possibles.

Comparaison des types de données

Les changements de type de données entre SQL Server et PostgreSQL peuvent entraîner des différences significatives dans les données obtenues sur lesquelles les applications fonctionnent. Pour une comparaison des types de données, consultez le tableau sur le site Web de Sqlines.

Fonctions SQL natives ou intégrées

Le comportement de certaines fonctions diffère entre les bases de données SQL Server et PostgreSQL. Le tableau suivant fournit une comparaison.

Microsoft SQL Server	Description	PostgreSQL
`CAST`	Convertit une valeur d'un type de données en un autre.	PostgreSQL `type ::` `operator`
`GETDATE()`	Renvoie la date et l'heure actuelles du système de base de données, dans un `YYYY-MM-DD hh:mm:ss.mmm` format.	`CLOCK_TIMESTAMP`
`DATEADD`	Ajoute un intervalle heure/date à une date.	`INTERVAL`expression
`CONVERT`	Convertit une valeur dans un format de données spécifique.	`TO_CHAR`
`DATEDIFF`	Renvoie la différence entre deux dates.	`DATE_PART`
`TOP`	Limite le nombre de lignes d'un ensemble `SELECT` de résultats.	`LIMIT/FETCH`

Blocs anonymes

Une requête SQL structurée est organisée en sections telles que la déclaration, les exécutables et la gestion des exceptions. Le tableau suivant compare les versions Microsoft SQL Server et PostgreSQL d'un bloc anonyme simple. Pour les blocs anonymes complexes, nous vous recommandons d'appeler une fonction de base de données personnalisée au sein de votre application.

Microsoft SQL Server

```
my $sql_qry1=
my $sql_qry2 =
my $sqlqry = "BEGIN TRAN
$sql_qry1 $sql_qry2
```

PostgreSQL

```
my $sql_qry1=
my $sql_qry2 =
my $sql_qry = " DO \$\$
BEGIN
```

```
if @\@error !=0 ROLLBACK
TRAN
else COMIT TRAN";
```

```
$header_sql $content_sql
END
\$\$";
```

Autres différences

- Insertions groupées de lignes : l'équivalent dans PostgreSQL de l'utilitaire bcp de Microsoft SQL Server est COPY.
- Sensibilité majuscules/minuscules : les noms de colonnes distinguent les majuscules et minuscules dans PostgreSQL. Vous devez donc convertir les noms de colonne de SQL Server en minuscules ou en majuscules. Cela devient un facteur lorsque vous extrayez ou comparez des données, ou lorsque vous placez des noms de colonnes dans des ensembles de résultats ou des variables. L'exemple suivant identifie les colonnes dans lesquelles les valeurs peuvent être stockées en majuscules ou en minuscules.

```
my $sql_qry = "SELECT $record_id FROM $exampleTable WHERE LOWER($record_name) =
 \'failed transaction\'";
```

- Concaténation : SQL Server l'utilise + comme opérateur pour la concaténation de chaînes, alors que PostgreSQL l'utilise. | |
- Validation : vous devez tester et valider les requêtes et les fonctions SQL en ligne avant de les utiliser dans le code d'application pour PostgreSQL.
- Inclusion de la bibliothèque ORM : vous pouvez également rechercher l'inclusion ou le remplacement d'une bibliothèque de connexion à une base de données existante par des bibliothèques ORM Python telles que SQLAlchemyPynomODB. Cela permettra d'interroger et de manipuler facilement les données d'une base de données en utilisant un paradigme orienté objet.

Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS

Créée par Battulga Purevragchaa (AWS), Babu Srinivasan (MongoDB) et Igor Alekseev (AWS)

Récapitulatif

Ce modèle décrit les étapes de migration des données depuis IBM Db2 et d'autres bases de données telles que les bases de données mainframe et Sybase vers MongoDB Atlas sur le. AWS Cloud Il permet AWS Glued'accélérer la migration des données vers MongoDB Atlas.

Le modèle accompagne le guide Migrating to MongoDB Atlas AWS sur le site Web de Prescriptive AWS Guidance. Il fournit les étapes de mise en œuvre de l'un des scénarios de migration décrits dans ce guide. Pour d'autres scénarios de migration, consultez les modèles suivants sur le site Web des directives AWS prescriptives :

- Migrer un environnement MongoDB auto-hébergé vers MongoDB Atlas sur AWS
- Migrer des bases de données relationnelles vers MongoDB Atlas sur AWS

Le modèle est destiné aux partenaires et aux AWS utilisateurs de AWS Managed Services.

Conditions préalables et limitations

Prérequis

- Une base de données source telle que SAP, Sybase, IBM Db2, etc. à migrer vers MongoDB Atlas.
- Connaissance des bases de données telles que SAP, Sybase, IBM Db2, MongoDB Atlas et. Services AWS

Versions du produit

- MongoDB version 5.0 ou ultérieure.

Architecture

Le schéma suivant illustre le chargement de données par lots et le streaming de données à l'aide AWS Glue Studio d'Amazon Kinesis Data Streams et de MongoDB Atlas.

Cette architecture de référence permet AWS Glue Studio de créer des pipelines d'extraction, de transformation et de chargement (ETL) afin de migrer les données vers MongoDB Atlas. An AWS Glue crawler s'intègre à MongoDB Atlas pour faciliter la gouvernance des données. Les données peuvent être portées par lots ou diffusées vers MongoDB Atlas à l'aide d'Amazon Kinesis Data Streams.

Chargement de données par lots

Pour plus d'informations sur la migration des données par lots, consultez le billet de AWS blog Composez vos tâches ETL pour MongoDB Atlas with. AWS Glue

Streaming de données

Pour les architectures de référence MongoDB Atlas qui prennent en charge différents scénarios d'utilisation, consultez la section Migration vers MongoDB Atlas AWS sur le site Web des directives prescriptives. AWS

Outils

- AWS Glueest un service ETL entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- Amazon Kinesis Data Streams vous aide à collecter et à traiter de grands flux d'enregistrements de données en temps réel.
- MongoDB Atlas est une base de données en tant que service (DBaaS) entièrement gérée pour le déploiement et la gestion des bases de données MongoDB dans le cloud.

Bonnes pratiques

Pour les directives, consultez le Guide des meilleures pratiques pour MongoDB dans le référentiel MongoDB. GitHub

Épopées

Découverte et évaluation

Tâche	Description	Compétences requises
Déterminez la taille du cluster.	Estimez la taille de l'ensemble de travail en utilisant les informations provenant de `db.stats()` pour l'espace d'index total. Supposons qu'un pourcentage de votre espace de données soit fréquemment consulté. Vous pouvez également estimer vos besoins en mémoire en fonction de vos hypothèses. Cette tâche devrait prendre environ une semaine. Pour plus d'informations et des exemples concernant cette histoire et les autres de cette épopée, consultez les liens dans la section Ressources connexes.	MongoDB DBA, architecte d'applications
Estimez les besoins en bande passante du réseau.	Pour estimer les besoins en bande passante de votre réseau, multipliez la taille moyenne des documents par le nombre de documents servis par seconde. Tenez compte du trafic maximal que chaque nœud de votre cluster pourra supporter comme base. Pour calculer les taux de transfert de données en	Base de données MongoDB

Tâche	Description	Compétences requises
	aval de votre cluster vers les applications clientes, utilisez la somme du total des documents renvoyés sur une période donnée. Si vos applications lisent à partir de nœuds secondair es, divisez le nombre total de documents par le nombre de nœuds pouvant effectuer des opérations de lecture. Pour connaître la taille moyenne des documents d'une base de données, utilisez la `db.stats().avgObjS ize` commande. Cette tâche prend généralement une journée.	
Sélectionnez le niveau Atlas.	Suivez les instructions de la documentation MongoDB pour sélectionner le niveau de cluster Atlas approprié.	Base de données MongoDB
Planifiez le transfert.	Planifiez le transfert des applications.	MongoDB DBA, architecte d'applications

Configuration d'un nouvel environnement MongoDB Atlas sur AWS

Tâche	Description	Compétences requises
Créez un nouveau cluster MongoDB Atlas sur. AWS	Dans MongoDB Atlas, choisissez Build a Cluster,	Base de données MongoDB

Tâche	Description	Compétences requises
	puis sélectionnez AWS comme fournisseur de cloud.	
Sélectionnez Régions AWS une configuration globale du cluster.	Sélectionnez dans la liste des options disponibles Régions AWS pour votre cluster Atlas. Configurez des clusters globaux si nécessaire.	Base de données MongoDB
Sélectionnez le niveau du cluster.	Sélectionnez le niveau de cluster de votre choix. Le choix du niveau détermine des facteurs tels que la mémoire, le stockage et les spécifica tions IOPS.	Base de données MongoDB
Configurez des paramètres de cluster supplémentaires.	Configurez des paramètres de cluster supplémentaires tels que la version de MongoDB, les options de sauvegard e et de chiffrement. Pour plus d'informations sur ces options, consultez la section Ressources connexes.	Base de données MongoDB

Configuration de la sécurité et de la conformité

Tâche	Description	Compétences requises
Configurez la liste d'accès.	Pour vous connecter au cluster Atlas, vous devez ajouter une entrée à la liste d'accès du projet. Atlas utilise Transport Layer Security (TLS) /Secure Sockets	Base de données MongoDB

Tâche	Description	Compétences requises
	Layer (SSL) pour chiffrer les connexions au cloud privé virtuel (VPC) de votre base de données. Pour configure r la liste d'accès au projet et pour plus d'informations sur les histoires de cette épopée, consultez les liens dans la section Ressources connexes.	
Authentifiez et autorisez les utilisateurs.	Vous devez créer et authentif ier les utilisateurs de base de données qui accèderont aux clusters MongoDB Atlas. Pour accéder aux clusters d'un projet, les utilisateurs doivent appartenir à ce projet, et ils peuvent appartenir à plusieurs projets. Vous pouvez également activer l'autoris ation avec AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Configurer l'authent ification avec IAM dans la documentation de MongoDB.	Base de données MongoDB
Créez des rôles personnal isés.	(Facultatif) Atlas prend en charge la création de rôles personnalisés si les privilège s utilisateur de la base de données Atlas intégrés ne couvrent pas l'ensemble de privilèges souhaité.	Base de données MongoDB

Tâche	Description	Compétences requises
Configurez le peering VPC.	(Facultatif) Atlas prend en charge le peering VPC avec d'autres AWS. VPCs	Base de données MongoDB
Configurez un AWS PrivateLink point de terminaison.	(Facultatif) Vous pouvez configurer des points de terminaison privés AWS en utilisant AWS PrivateLink.	Base de données MongoDB
Activez l'authentification à deux facteurs.	(Facultatif) Atlas prend en charge l'authentification à deux facteurs (2FA) pour aider les utilisateurs à contrôler l'accès à leurs comptes Atlas.	Base de données MongoDB
Configurez l'authentification et l'autorisation des utilisateurs avec LDAP.	(Facultatif) Atlas prend en charge l'authentification et l'autorisation des utilisateurs avec le protocole LDAP (Lightweight Directory Access Protocol).	Base de données MongoDB
Configurez un AWS accès unifié.	(Facultatif) Certaines fonctionnalités d'Atlas, notamment Atlas Data Lake et le chiffrement au repos à l'aide de la gestion des clés client, utilisent des rôles IAM pour l'authentification.	Base de données MongoDB

Tâche	Description	Compétences requises
Configurez le chiffrement au repos en utilisant AWS KMS.	(Facultatif) Atlas prend en charge l'utilisation de AWS Key Management Service (AWS KMS) pour chiffrer les moteurs de stockage et les sauvegardes des fournisseurs de cloud.	Base de données MongoDB
Configurez CSFLE.	(Facultatif) Atlas prend en charge le chiffrement au niveau des champs côté client (CSFLE), y compris le chiffrement automatique des champs.	Base de données MongoDB

Migrer les données

Tâche	Description	Compétences requises
Lancez votre ensemble de répliques cible dans MongoDB Atlas.	Lancez votre ensemble de répliques cible dans MongoDB Atlas. Dans Atlas Live Migration Service, choisissez Je suis prêt à migrer.	Base de données MongoDB
Établissez la connexion AWS Glue avec MongoDB Atlas.	Utilisez an AWS Glue crawler pour vous connecter AWS Glue à MongoDB Atlas (base de données cible). Cette étape permet de préparer l'environ nement cible pour la migration . Pour plus d'informations, consultez la documentation AWS Glue.	Base de données MongoDB

Tâche	Description	Compétences requises
Établissez la connexion AWS Glue avec la base de données source ou le flux source.	Cela permet de préparer l'environnement cible pour la migration.	Base de données MongoDB
Configurez la transformation des données.	Configurez la logique de transformation pour migrer les données de l'ancien schéma structuré vers le schéma flexible de MongoDB.	Base de données MongoDB
Migrez les données.	Planifiez la migration dans AWS Glue Studio.	Base de données MongoDB

Configuration de l'intégration opérationnelle

Tâche	Description	Compétences requises
Connectez-vous au cluster.	Connectez-vous au cluster MongoDB Atlas.	Développeur d’applications
Interagissez avec les données.	Interagissez avec les données du cluster.	Développeur d’applications
Surveillez les clusters.	Surveillez vos clusters MongoDB Atlas.	Base de données MongoDB
Sauvegardez et restaurez les données.	Sauvegardez et restaurez les données du cluster.	Base de données MongoDB

Résolution des problèmes

Problème	Solution
Si vous rencontrez des problèmes	Consultez la section Résolution des problèmes dans le référentiel MongoDB Atlas CloudFormation Resources.

Ressources connexes

Tous les liens suivants, sauf indication contraire, renvoient à des pages Web de la documentation de MongoDB.

Guide de migration

- Migration vers MongoDB Atlas AWS sur AWS (conseils prescriptifs)

Découverte et évaluation

- Mémoire
- Exemple de dimensionnement avec des exemples de jeux de données Atlas
- Exemple de dimensionnement pour applications mobiles
- Trafic réseau
- Mise à l'échelle automatique du cluster
- Modèle de dimensionnement Atlas

Configuration de la sécurité et de la conformité

- Configuration des entrées de liste d'accès IP
- Configuration des utilisateurs de base de données
- Configuration de l'accès à l'interface utilisateur d'Atlas
- Configuration de rôles de base de données personnalisés
- Configuration des utilisateurs de base de données
- Configuration d'une connexion d'appairage réseau
- En savoir plus sur les points de terminaison privés dans Atlas

- Gérez vos options d'authentification multifactorielle
- Configuration de l'authentification et de l'autorisation des utilisateurs avec LDAP
- Lac de données Atlas
- Chiffrement au repos à l'aide de la gestion des clés client
- Méthodes pour assumer un rôle (documentation IAM)
- Chiffrement au niveau des champs côté client
- Chiffrement automatique
- Contrôles de sécurité MongoDB Atlas
- Centre de gestion de la confidentialité MongoDB
- Configuration des fonctionnalités de sécurité pour les clusters

Configuration d'un nouvel environnement MongoDB Atlas sur AWS

- Fournisseurs de cloud et régions
- Gérer les clusters mondiaux
- Sélectionnez le niveau du cluster
- Configurer des paramètres supplémentaires
- Commencez avec Atlas
- Configuration de l'accès à l'interface utilisateur d'Atlas
- Gérer les clusters

Migration des données

- Migrer ou importer des données

Clusters de surveillance

- Surveillez vos clusters

Intégration des opérations

- Se connecter à un cluster
- Interagissez avec vos données

- Surveillez vos clusters
- Sauvegarder, restaurer et archiver des données

GitHub référentiel

- Diffusez des données vers MongoDB Atlas à l'aide de AWS Glue

Schémas de migration par charge de travail

Rubriques

- IBM
- Microsoft
- N/A
- Open source
- Oracle
- SAP

IBM

- Migrer une base de données DB2 d'Amazon EC2 vers Aurora compatible avec MySQL à l'aide d'AWS DMS
- Migrez Db2 for LUW vers Amazon EC2 en utilisant l'expédition des journaux pour réduire les temps d'arrêt
- Migrez Db2 for LUW vers Amazon EC2 avec une reprise après sinistre à haute disponibilité
- Migrez d'IBM Db2 sur Amazon vers une version compatible avec Aurora PostgreSQL EC2 à l'aide d'AWS DMS et d'AWS SCT
- Migrer d'un serveur WebSphere d'applications IBM vers Apache Tomcat sur Amazon EC2
- Diffusez des données depuis IBM Db2, SAP, Sybase et d'autres bases de données vers MongoDB Atlas sur AWS

Microsoft

- Accélérez la découverte et la migration des charges de travail Microsoft vers AWS
- Modifier les applications Python et Perl pour prendre en charge la migration de bases de données de Microsoft SQL Server vers Amazon Aurora PostgreSQL Compatible Edition
- Création de CloudFormation modèles AWS pour les tâches AWS DMS à l'aide de Microsoft Excel et Python
- Exporter une base de données Microsoft SQL Server vers Amazon S3 à l'aide d'AWS DMS
- SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL
- Ingérez et migrez des instances EC2 Windows vers un compte AWS Managed Services
- Migrer une file d'attente de messagerie de Microsoft Azure Service Bus vers Amazon SQS
- Migrer une base de données Microsoft SQL Server d'Amazon EC2 vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server vers Aurora MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une application .NET de Microsoft Azure App Service vers AWS Elastic Beanstalk
- Migrer une base de données Microsoft SQL Server sur site vers Amazon EC2
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de serveurs liés
- Migrer une base de données Microsoft SQL Server locale vers Amazon RDS for SQL Server à l'aide de méthodes de sauvegarde et de restauration natives
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide d'AWS DMS
- Migrer une base de données Microsoft SQL Server sur site vers Amazon Redshift à l'aide des agents d'extraction de données AWS SCT
- Migrer une base de données Microsoft SQL Server sur site vers Microsoft SQL Server sur Amazon EC2 exécutant Linux
- Migrez les données de Microsoft Azure Blob vers Amazon S3 à l'aide de Rclone
- Migrer une base de données Microsoft SQL Server sur site vers Amazon à EC2 l'aide du service de migration d'applications
- Migrer une base de données relationnelle vers MongoDB Atlas sur AWS

- Migrer les certificats SSL Windows vers un Application Load Balancer à l'aide d'ACM
- Réhébergez les charges de travail sur site dans le cloud AWS : liste de contrôle pour la migration
- Résoudre les erreurs de connexion après la migration de Microsoft SQL Server vers le cloud AWS
- Configurez une infrastructure multi-AZ pour un SQL Server Always On FCI à l'aide d'Amazon FSx

N/A

- Créez un processus d'approbation pour les demandes de pare-feu lors d'une migration de réhébergement vers AWS

Open source

- Création d'utilisateurs et de rôles d'application dans Aurora PostgreSQL compatible
- Migrer Amazon RDS for Oracle vers Amazon RDS for PostgreSQL avec et en utilisant et AWS SCTAWS DMSAWS CLIAWS CloudFormation
- Migrer une base de données MariaDB sur site vers Amazon RDS for MariaDB à l'aide d'outils natifs
- Migrer une base de données MySQL sur site vers Amazon EC2
- Migrer une base de données MySQL sur site vers Amazon RDS for MySQL
- Migrer une base de données MySQL sur site vers Aurora MySQL
- Migrer une base de données PostgreSQL locale vers Aurora PostgreSQL
- Migrer une base de données Couchbase Server vers Amazon EC2
- Migrez d'IBM WebSphere Application Server vers Apache Tomcat sur Amazon EC2 avec Auto Scaling
- Migrer d'Oracle GlassFish vers AWS Elastic Beanstalk
- Migrez de PostgreSQL sur EC2 Amazon vers Amazon RDS pour PostgreSQL à l'aide de pglogical
- Migrez les charges de travail de création, de formation et de déploiement de ML vers Amazon à SageMaker l'aide des outils de développement AWS
- Migrez des applications Java sur site vers AWS à l'aide d'AWS App2Container
- Migrez des bases de données MySQL sur site vers Aurora MySQL à l'aide de Percona, XtraBackup Amazon EFS et Amazon S3
- Migrer des tables externes Oracle vers des tables compatibles avec Amazon Aurora PostgreSQL
- Migrer les charges de travail Redis vers Redis Enterprise Cloud sur AWS
- Redémarrez automatiquement l'agent de réplication AWS sans le désactiver SELinux après le redémarrage d'un serveur source RHEL
- Transportez des bases de données PostgreSQL entre deux instances de base de données Amazon RDS à l'aide de pg_transport

Oracle

- Convertir VARCHAR2 (1) le type de données pour Oracle en type de données booléen pour Amazon Aurora PostgreSQL
- Émulez Oracle DR à l'aide d'une base de données globale Aurora compatible avec PostgreSQL
- Migrez progressivement d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle SQL Developer et d'AWS SCT
- Chargez des fichiers BLOB dans TEXT en utilisant le codage de fichiers compatible avec Aurora PostgreSQL
- Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS
- Migrer une base de données Amazon RDS for Oracle vers Compte AWS une autre Région AWS et AWS DMS l'utiliser pour une réplication continue
- Migrer une instance de base de données Amazon RDS pour Oracle vers un autre VPC
- Migrer une base de données Oracle sur site vers Amazon à l'aide EC2 d'Oracle Data Pump
- Migrer une base de données Oracle sur site vers Amazon OpenSearch Service à l'aide de Logstash
- Migrer une base de données Oracle sur site vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle
- Migrez une base de données Oracle sur site vers Amazon RDS for Oracle en utilisant directement Oracle Data Pump Import via un lien de base de données
- Migrer une base de données Oracle sur site vers Amazon RDS for Oracle à l'aide d'Oracle Data Pump
- Migrer une base de données Oracle sur site vers Amazon RDS for PostgreSQL à l'aide d'un assistant Oracle et d'AWS DMS
- Migrer une base de données Oracle sur site vers Oracle sur Amazon EC2
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for MariaDB à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle d'Amazon EC2 vers Amazon RDS for Oracle à l'aide d'AWS DMS
- Migrer une base de données Oracle vers Amazon DynamoDB à l'aide d'AWS DMS

- Migrer une base de données Oracle vers Amazon RDS for Oracle à l'aide d'adaptateurs de GoldenGate fichiers plats Oracle
- Migrer une base de données Oracle vers Amazon Redshift à l'aide d'AWS DMS et d'AWS SCT
- Migrer une base de données Oracle vers Aurora PostgreSQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer une EnterpriseOne base de données Oracle JD Edwards vers AWS à l'aide d'Oracle Data Pump et d'AWS DMS
- Migrer une table partitionnée Oracle vers PostgreSQL à l'aide d'AWS DMS
- Migrer une PeopleSoft base de données Oracle vers AWS à l'aide d'AWS DMS
- Migrer les données d'une base de données Oracle sur site vers Aurora PostgreSQL
- Migrer d'Amazon RDS for Oracle vers Amazon RDS for MySQL
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide de vues matérialisées et d'AWS DMS
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for PostgreSQL à l'aide d'AWS DMS SharePlex
- Migrer d'une base de données Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle GoldenGate
- Migrez d'Oracle sur Amazon EC2 vers Amazon RDS for MySQL à l'aide d'AWS DMS et d'AWS SCT
- Migrer d'Oracle vers Amazon DocumentDB à l'aide d'AWS DMS
- Migrer d'Oracle WebLogic vers Apache Tomcat (ToMee) sur Amazon ECS
- Migrer les index basés sur les fonctions d'Oracle vers PostgreSQL
- Migrer les applications existantes d'Oracle Pro*C vers ECPG
- Migrer les valeurs Oracle CLOB vers des lignes individuelles dans PostgreSQL sur AWS
- Migrer les codes d'erreur de la base de données Oracle vers une base de données compatible avec Amazon Aurora PostgreSQL
- Migrer Oracle E-Business Suite vers Amazon RDS Custom
- Migrer les fonctions natives d'Oracle vers PostgreSQL à l'aide d'extensions
- Migrer Oracle PeopleSoft vers Amazon RDS Custom
- Migrer la fonctionnalité Oracle ROWID vers PostgreSQL sur AWS
- Migrer les packages pragma Oracle SERIALLY_REUSERABLE vers PostgreSQL
- Migrer les colonnes générées virtuellement d'Oracle vers PostgreSQL
- Configuration de la fonctionnalité Oracle UTL_FILE sur Aurora compatible avec PostgreSQL

- Valider les objets de base de données après la migration d'Oracle vers Amazon Aurora PostgreSQL

SAP

- Migrer une base de données SAP ASE sur site vers Amazon EC2
- Migrez de SAP ASE vers Amazon RDS for SQL Server à l'aide d'AWS DMS
- Migrez SAP ASE sur Amazon EC2 vers Amazon Aurora PostgreSQL compatible avec AWS SCT et AWS DMS
- Réduisez le temps de migration homogène vers SAP en utilisant le service de migration d'applications

Plus de modèles

- Accès Services AWS depuis IBM z/OS en installant le AWS CLI
- Évaluez l'état de préparation des applications pour la migration vers le cloud AWS à l'aide de CAST Highlight
- Évaluez les performances des requêtes pour la migration des bases de données SQL Server vers MongoDB Atlas sur AWS
- Automatisez le basculement et le retour en arrière entre régions à l'aide de DR Orchestrator Framework
- Automatisez les tâches de base de données dans l'édition SQL Server Express exécutée sur Amazon à EC2 l'aide AWS Lambda d'un planificateur de tâches
- Créez un visualiseur de fichiers mainframe avancé dans le cloud AWS
- Configuration d'une extension de centre de données vers le VMware cloud sur AWS à l'aide du mode Hybrid Linked
- Connectez-vous aux données et aux plans de contrôle du service de migration des applications via un réseau privé
- Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age
- Convertir les requêtes Oracle JSON en SQL de base de données PostgreSQL
- Convertir la fonctionnalité temporelle Teradata NORMALIZE en Amazon Redshift SQL
- Convertir la fonctionnalité Teradata RESET WHEN en Amazon Redshift SQL
- Copiez les tables Amazon DynamoDB entre les comptes à l'aide de AWS Backup
- Déployez un cluster Cassandra sur Amazon EC2 avec une statique privée IPs pour éviter le rééquilibrage
- Déployez des applications à piles multiples à l'aide d'AWS CDK avec TypeScript
- Déployez des instances de cluster de basculement SQL Server sur Amazon EC2 et Amazon à l'aide FSx de Terraform
- Émuler des charges de travail Oracle RAC à l'aide de points de terminaison personnalisés dans Aurora PostgreSQL
- Estimez la taille du moteur Amazon RDS pour une base de données Oracle à l'aide des rapports AWR
- Générez des informations sur les données en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight
- Gérer les blocs anonymes dans les instructions Dynamic SQL dans Aurora PostgreSQL

- Gérez les fonctions Oracle surchargées dans la compatibilité avec Aurora PostgreSQL
- Identifiez automatiquement les images de conteneur dupliquées lors de la migration vers un référentiel Amazon ECR
- Intégrer VMware vRealize Network Insight au VMware cloud sur AWS
- Migrer les instances de base de données Amazon RDS for Oracle vers d'autres comptes utilisant AMS
- Migrez un cluster Apache Kafka sur site vers Amazon MSK en utilisant MirrorMaker
- Migrez les charges de travail Apache Cassandra vers Amazon Keyspaces à l'aide d'AWS Glue
- Migrez vos charges de travail de conteneurs d'Azure Red Hat OpenShift (ARO) vers Red Hat OpenShift Service on AWS (ROSA)
- Migrez d'Oracle 8i ou 9i vers Amazon RDS for Oracle à l'aide d'AWS DMS SharePlex
- Migrez les données Hadoop vers Amazon S3 à l'aide de Migrator WANdisco LiveData
- Migrer les fonctions et procédures Oracle comportant plus de 100 arguments vers PostgreSQL
- Migrer les variables de liaison Oracle OUT vers une base de données PostgreSQL
- Migrez SAP HANA vers AWS à l'aide de SAP HSR avec le même nom d'hôte
- Migrer SQL Server vers AWS à l'aide de groupes de disponibilité distribués
- Migrez VMs vers VMware le cloud sur AWS à l'aide de la migration assistée par HCX OS
- Modernisez les charges de travail d'impression en ligne du mainframe sur AWS à l'aide de Micro Focus Enterprise Server et de LRS VPSX/MFI
- Modernisez la gestion des sorties du mainframe AWS en utilisant Rocket Enterprise Server et PageCenter LRS X
- Modifiez les en-têtes HTTP lors de la migration de F5 vers un Application Load Balancer sur AWS
- Gérez le basculement multi-AZ pour les clusters EMR à l'aide d'Application Recovery Controller
- Envoyez des logs depuis le VMware Cloud AWS vers Splunk en utilisant VMware Aria Operations for Logs
- Configurer un pipeline CI/CD pour la migration de base de données à l'aide de Terraform
- Configurer la reprise après sinistre pour Oracle JD Edwards EnterpriseOne avec AWS Elastic Disaster Recovery
- Simplifiez la gestion des certificats privés en utilisant AWS Private CA et AWS RAM
- Transférez des données Db2 z/OS à grande échelle vers Amazon S3 dans des fichiers CSV

Modernisation

Rubriques

- Analyser et visualiser l'architecture logicielle dans CAST Imaging
- Évaluez l'état de préparation des applications pour la migration vers le cloud AWS à l'aide de CAST Highlight
- Archivez automatiquement les éléments sur Amazon S3 à l'aide de DynamoDB TTL
- Créez une architecture sans serveur multi-locataires dans Amazon Service OpenSearch
- Déployez des applications à piles multiples à l'aide d'AWS CDK avec TypeScript
- Automatisez le déploiement d'applications imbriquées à l'aide d'AWS SAM
- Implémentez l'isolation des locataires SaaS pour Amazon S3 à l'aide d'un distributeur automatique de jetons AWS Lambda
- Implémentez le modèle de saga sans serveur à l'aide d'AWS Step Functions
- Gérez les applications de conteneur sur site en configurant Amazon ECS Anywhere avec le kit AWS CDK
- Modernisez les applications ASP.NET Web Forms sur AWS
- Exécutez des charges de travail planifiées et pilotées par des événements à grande échelle avec AWS Fargate
- Intégration des locataires dans l'architecture SaaS pour le modèle de silo à l'aide de C# et d'AWS CDK
- Décomposez les monolithes en microservices en utilisant le CQRS et le sourcing d'événements
- Plus de modèles

Analyser et visualiser l'architecture logicielle dans CAST Imaging

Créée par Arpita Sinha (Cast Software) et James Hurrell (Cast Software)

Récapitulatif

Ce modèle montre comment utiliser CAST Imaging pour naviguer visuellement dans un système logiciel complexe et effectuer une analyse précise de la structure logicielle. En utilisant CAST Imaging de cette manière, vous pouvez prendre des décisions plus éclairées concernant l'architecture de votre application, notamment à des fins de modernisation.

Pour visualiser l'architecture de votre application dans CAST Imaging, vous devez d'abord intégrer le code source de votre application via la console CAST. La console publie ensuite les données de votre application sur CAST Imaging, où vous pouvez visualiser et parcourir l'architecture de votre application couche par couche.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- L'Amazon Machine Image (AMI) pour CAST Imaging
- Une instance Amazon Elastic Compute Cloud (Amazon EC2) qui inclut les éléments suivants (une instance EC2 Amazon r5.xlarge optimisée pour la mémoire est recommandée) :
  - 4 vCPU
  - 32 GO DE RAM
  - Volume minimum de 500 Go de disque SSD (General Usage Solid State Drive) (gp3)
- Clés de licence CAST Console et CAST Imaging (pour obtenir les clés de licence requises, contactez CAST à l'adresse aws.contact-me@castsoftware.com)
- Le code source complet de l'application que vous souhaitez analyser au format compressé (.zip)
- Microsoft Edge, Mozilla Firefox ou Google Chrome

Architecture

Le schéma suivant montre un exemple de flux de travail permettant d'intégrer le code source d'une application via la console CAST, puis de le visualiser dans CAST Imaging :

Le schéma suivant illustre le flux de travail suivant :

1. CAST génère les métadonnées du code source des applications en rétro-ingénierie du code frontal, du middleware et du code principal.
2. Les données d'application générées par CAST sont automatiquement importées dans CAST Imaging, où elles peuvent être visualisées et analysées.

Voici un aperçu du fonctionnement de ce processus :

Outils

- CAST Imaging est une application basée sur un navigateur qui vous permet de visualiser et de naviguer visuellement dans votre système logiciel, afin que vous puissiez prendre des décisions éclairées concernant son architecture.
- La console CAST est une application basée sur un navigateur qui vous permet de configurer, d'exécuter et de gérer les analyses CAST AIP.

> **Note**
>
> L'imagerie CAST et la console CAST sont incluses dans l'AMI pour CAST Imaging.

Épopées

Configuration de l'environnement d'imagerie CAST

Tâche	Description	Compétences requises
Exécutez la configuration initiale de la console CAST.	1. Ouvrez votre navigateur Web et connectez-vous à la console CAST en saisissant l'URL suivante : http://localhost:8081 2. Lorsque vous y êtes invité, entrez votre clé de licence	Architectes logiciels, développeurs, responsables techniques

Tâche	Description	Compétences requises
	CAST Console. Ensuite, choisissez Suivant. 3. Vérifiez les paramètres de configuration. Si aucune modification n'est nécessaire, choisissez Enregistrer et terminer.	
Exécutez la configuration initiale de CAST Imaging.	1. Ouvrez votre navigateur Web et connectez-vous à CAST Imaging en saisissant l'URL suivante : http://localhost:8083 2. Lorsque vous y êtes invité, connectez-vous en saisissant admin pour le nom d'utilisateur et le mot de passe. 3. Lorsque vous y êtes invité, entrez votre clé de licence CAST Imaging. Choisissez ensuite Mettre à jour pour enregistrer la clé.	Architectes logiciels, développeurs, responsables techniques

Tâche	Description	Compétences requises
Configurez le serveur local CAST Extend.	(Facultatif) Par défaut, le serveur local CAST Extend est configuré pour fonctionner en mode hors ligne. Si cela est acceptable, aucune configuration supplémentaire n'est nécessaire. Toutefois, si vous préférez configurer le serveur local CAST Extend en mode en ligne/proxy avec une connexion directe à CAST Extend, procédez comme suit. **Note** Pour les informations d'identification CAST Extend, consultez la page d'enregistrement de CAST Extend. 1. Utilisez le raccourci du centre d'administration CAST Extend sur le bureau pour charger votre navigateur Web et vous connecter au serveur local de CAST Extend. 2. Choisissez l'option En ligne. 3. Entrez vos informations d'identification CAST Extend (e-mail et mot de passe), puis choisissez	Architectes logiciels, développeurs, responsables techniques

Tâche	Description	Compétences requises
	Enregistrer pour terminer le processus.	

Intégrez votre application à CAST Imaging

Tâche	Description	Compétences requises
Préparez le code source de votre application.	Enregistrez le code source de votre application dans un seul fichier .zip compressé.	Architectes logiciels, développeurs, responsables techniques
Ajoutez votre application à la console CAST.	1. Ouvrez votre navigateur Web et connectez-vous à la console CAST en saisissant l'URL suivante : http://localhost:8081 2. Lorsque vous y êtes invité, connectez-vous en saisissant admin pour le nom d'utilisateur et le mot de passe. 3. Choisissez Add application (Ajouter une application). Entrez ensuite le nom de l'application et choisissez Ajouter.	Architectes logiciels, développeurs, responsables techniques
Ouvrez l'assistant de livraison du code source.	Recherchez l'application que vous avez créée dans la console CAST. Choisissez ensuite Ajouter une version.	Architectes logiciels, développeurs, responsables techniques
Téléchargez le code source de votre application.	Effectuez l’une des actions suivantes :	Architectes logiciels, développeurs, responsables techniques

Tâche	Description	Compétences requises
	• Faites glisser le fichier .zip qui contient le code source de votre application dans l'assistant de distribution du code source. –ou– • Choisissez l'icône du cloud de téléchargement. Ouvrez ensuite le fichier .zip qui contient le code source de votre application.	

Tâche	Description	Compétences requises
Lancez le processus d'analyse .	1. Dans l'assistant de livraison , fournissez les détails de la version et spécifiez les options de configura tion. Pour plus d'informa tions, consultez la section Intégration standard pour CAST Imaging dans la documentation CAST Imaging. 2. Assurez-vous que l'option Publier sur CAST Imaging est sélectionnée. Choisisse z ensuite Proceed. **Note** Choisissez Proceed pour démarrer le processus d'analyse du code source. La fenêtre de progressi on de la console CAST montre chaque étape du processus d'analyse et affiche une notification lorsque l'analyse est terminée.	Architectes logiciels, développeurs, responsables techniques

Vérifiez les résultats d'analyse et les données publiés sur CAST Imaging

Tâche	Description	Compétences requises
Vérifiez le statut et les journaux.	Lorsque toutes les actions d'analyse sont terminées, vérifiez qu'un message de réussite apparaît dans la fenêtre de progression. **Note** Vous pouvez consulter les journaux individuels pour chaque action d'analyse immédiatement après son exécution. Pour consulter les journaux d'une action spécifique, choisissez Afficher le journal dans la fenêtre de progression.	Architectes logiciels, développeurs, responsables techniques
Vérifiez les détails de l'application.	Dans le panneau Détails de l'application, passez en revue les détails des résultats de l'analyse. Assurez-vous d'examiner les technologies découvertes et l'organisation du code source.	Architectes logiciels, développeurs, responsables techniques
Vérifiez et accédez à CAST Imaging.	1. Dans le volet Gestion des applications de la console CAST, vérifiez que le statut de version de votre applicati	Architectes logiciels, développeurs, responsables techniques

Tâche	Description	Compétences requises
	on est Traitement par imagerie. Une icône CAST Imaging apparaît. 2. Cliquez sur l'icône CAST Imaging pour accéder directement aux données de votre application dans CAST Imaging. **Note** L'état Imagerie traitée signifie que le code source a été analysé et téléchargé sur votre instance CAST Imaging.	

Commencez à analyser votre application avec CAST Imaging

Tâche	Description	Compétences requises
Connectez-vous à CAST Imaging.	Ouvrez Cast Imaging et entrez les informations d'identification d'administrateur par défaut (admin/admin). Les données de votre application apparaissent.	Architectes logiciels, développeurs, responsables techniques
Explorez les données de votre application dans CAST Imaging.	Commencez à visualiser votre architecture logicielle à l'aide des fonctionnalités d'imagerie CAST.	Architectes logiciels, développeurs, responsables techniques

Tâche	Description	Compétences requises
	Pour un didacticiel rapide sur l'utilisation des fonctionnalités de CAST Imaging, cliquez sur l'icône d'aide pour afficher l'assistant d'imagerie CAST. Pour plus d'informations, consultez le guide de l'utilisateur de CAST Imaging.	

Ressources connexes

Documentation de la console CAST

- S'identifier
- Configuration des options via la console CAST

Documentation sur l'imagerie CAST

- Intégration des applications pour CAST Imaging - prérequis
- Ajouter une nouvelle application pour CAST Imaging
- Intégration standard pour CAST Imaging — vérifiez les résultats
- S'identifier
- Options de configuration — Interface graphique du centre d'administration

Plus de ressources sur l'imagerie CAST sur AWS

- Modernisation des applications vers AWS accélérée par CAST — Technique (PartnerCast webinaire AWS, nécessite un compte gratuit)
- Utilisation des espaces de refactorisation CAST et AWS Migration Hub pour moderniser les applications existantes (article de blog AWS)
- Modernisez les applications en fonction des architectures AWS avec CAST Imaging (atelier AWS)
- AWS Marketplace : imagerie CAST

- Toutes les ressources de CAST sur AWS

Évaluez l'état de préparation des applications pour la migration vers le cloud AWS à l'aide de CAST Highlight

Créée par Greg Rivera (Cast Software)

Récapitulatif

CAST Highlight est une solution logicielle en tant que service (SaaS) permettant d'effectuer une analyse rapide du portefeuille d'applications. Ce modèle décrit comment configurer et utiliser CAST Highlight pour évaluer l'état de préparation au cloud des applications logicielles personnalisées du portefeuille informatique d'une entreprise, et pour planifier la modernisation ou la migration vers le cloud Amazon Web Services (AWS).

CAST Highlight fournit des informations sur l'état de préparation d'une application au cloud, identifie les bloqueurs de code qui doivent être supprimés avant une migration, estime les efforts nécessaires pour supprimer ces bloqueurs et recommande les services AWS que les applications individuelles pourraient utiliser après la migration.

Ce modèle décrit la procédure de configuration et d'utilisation de CAST Highlight, qui comprend cinq étapes : configuration du nouvel utilisateur, gestion des applications, gestion des campagnes, analyse du code source et analyse des résultats. Vous devez effectuer toutes les étapes de la section Epics de ce modèle pour garantir le succès de l'analyse et de l'analyse des applications.

Conditions préalables et limitations

Prérequis

- Un compte CAST Highlight actif avec des autorisations de gestionnaire de portefeuille.
- Au moins 300 Mo d'espace disque disponible et 4 Go de mémoire sur votre ordinateur local pour installer l'agent local CAST Highlight.
- Microsoft Windows 8 ou version ultérieure.
- Le code source de votre application doit être stocké dans des fichiers texte accessibles depuis la machine sur laquelle l'agent local est installé. Aucun code source ne quitte les locaux et tout le code est scanné localement.

Architecture

Le schéma suivant illustre le flux de travail d'utilisation de CAST Highlight.

Le flux de travail se compose des étapes suivantes :

1. Connectez-vous au portail CAST Highlight, téléchargez l'agent local et installez-le sur votre ordinateur local. Amazon Simple Storage Service (Amazon S3) stocke le package d'installation de l'agent local.
2. Scannez vos fichiers de code source et produisez un fichier de résultats.
3.
> **Important**
>
> Téléchargez le fichier de résultats sur le portail CAST Highlight. : aucun code source n'est inclus dans le fichier de résultats.

4. Répondez aux questions du sondage pour chaque application que vous avez scannée.
5. Consultez les tableaux de bord et les rapports disponibles sur le portail CAST Highlight. Amazon Relational Database Service (Amazon RDS) stocke le scan du code, les résultats d'analyse et les données du logiciel CAST Highlight.

Pile technologique

CAST Highlight prend en charge les technologies suivantes pour analyser l'état de préparation des applications au cloud :

- Java
- COBOL
- C#
- C++
- Clojure
- PHP
- JavaScript
- TypeScript
- Python
- Microsoft Transact-SQL
- VB.Net

- Kotlin
- Scala
- Swift

Automatisation et mise à l'échelle

- Un analyseur CLI peut être utilisé pour automatiser le processus d'analyse CAST Highlight.

Outils

Aucun outil n'est requis pour ce modèle si tous les prérequis sont remplis. Toutefois, vous pouvez choisir d'utiliser des outils facultatifs, tels que des utilitaires de gestion du code source (SCM), des extracteurs de code ou d'autres outils pour gérer vos fichiers de code source.

Épopées

Nouvelle configuration utilisateur

Tâche	Description	Compétences requises
Activez votre compte CAST Highlight et choisissez votre mot de passe.	Tous les nouveaux utilisateurs de CAST Highlight reçoivent un e-mail d'activation de compte. Suivez le lien d'activation pour activer votre compte CAST Highlight et entrez un mot de passe pour terminer le processus d'activation.	N/A
Connectez-vous au portail CAST Highlight.	La page d'accueil de CAST Highlight apparaît une fois que vous avez saisi votre nouveau mot de passe. Connectez-vous au portail CAST Highlight à l'aide de vos informations d'identification d'utilisateur.	N/A

Gestion des applications

Tâche	Description	Compétences requises
Créez un enregistrement de candidature.	Dans le portail CAST Highlight , accédez à l'onglet Gérer l'application dans la section Gérer le portefeuille. Dans la vignette Applications en haut de l'écran, choisissez Ajouter.	N/A
Choisissez le nom de l'application.	Entrez le nom de votre application, puis choisissez Enregistrer. Ce nom est utilisé pour l'enregistrement de votre candidature dans CAST Highlight.	N/A
Répétez les étapes pour toutes les applications.	Répétez ces étapes pour chaque application que vous souhaitez analyser.	N/A

Gestion des campagnes

Tâche	Description	Compétences requises
Créer une campagne.	CAST Highlight utilise le terme « campagne » pour décrire un ensemble d'applications qui seront analysées à un moment précis. Dans le portail CAST Highlight, accédez à l'onglet Gérer les campagnes dans la section Gérer le portefeuille. Choisissez Créer une	N/A

Tâche	Description	Compétences requises
	campagne pour lancer l'écran de création de campagne.	
Entrez un nom et choisissez une date de clôture pour la campagne.	Entrez un nom pour votre campagne et choisissez une date de clôture pour celle-ci. **Important** Les contributeurs ne peuvent pas soumettre les résultats de l'analyse des candidatures après la date de clôture de la campagne.	N/A

Tâche	Description	Compétences requises
Décidez d'inclure l'analyse du code source, les réponses aux enquêtes, ainsi que le domaine et le champ d'application.	Choisissez une ou plusieurs enquêtes standard utilisées pour améliorer les données d'analyse du code source avec des informations qualitatives. Les catégories de l'enquête sont l'impact commercial, les efforts de maintenance logicielle CloudReady, les propriétés des applications et l'impact écologique. Choisissez le domaine et les applications analysés pendant la campagne. **Important** Assurez-vous d'ajouter toutes les applications que vous souhaitez scanner dans la section Gérer les applications avant de commencer la campagne.	N/A
Personnalisez le message de lancement.	Personnalisez le message de lancement qui sera envoyé par e-mail à tous les contributeurs associés aux applications de la campagne.	N/A
Lancez la campagne.	Choisissez Terminer pour lancer la campagne.	N/A

Analyse du code source

Tâche	Description	Compétences requises
Téléchargez l'agent local CAST Highlight.	Dans le portail CAST Highlight , choisissez Application Scans et téléchargez l'agent local sur votre ordinateur local.	N/A
Installez l'agent local.	Lancez le programme d'installation CASTHighl ight Setup.exe et suivez les instructions de configuration qui s'affichent. Une fois l'agent local installé, vous êtes prêt à analyser vos applications.	N/A
Définissez l'étendue du scan du code de l'agent local.	L'analyse du code est effectuée au niveau du fichier et ne prend pas en compte les liens logiques ou les dépendances entre les fichiers. Tous les fichiers sont considérés comme égaux et font partie de l'application. Pour obtenir des résultats précis et cohérents, préparez la portée de votre analyse de code à l'aide des fonctionn alités d'exclusion de fichiers ou de dossiers disponibles dans l'agent local.	N/A
Incluez des packages open source ou COTS.	(Facultatif) Si vous souhaitez inclure des packages open source ou commerciaux off-the-shelf (COTS), assurez-	N/A

Tâche	Description	Compétences requises
	vous qu'ils figurent dans les dossiers que vous prévoyez de scanner. Généralement, les bibliothèques externes sont regroupées dans un sous-dossier appelé « third-party » ou quelque chose de similaire , et le code principal se trouve souvent dans le dossier de fichiers « src/main ».	
Exclure les classes de test.	Les classes de test sont généralement exclues de l'analyse du code source car elles ne font généralement pas partie de l'application compilée. Cependant, vous pouvez choisir de les inclure dans le scan si nécessaire.	N/A
Excluez les dossiers SCM, build et deployment.	Pour des résultats plus cohérents, évitez d'inclure des dossiers SCM, build ou deployment (par exemple, des fichiers .git ou .svn) dans votre analyse.	N/A

Tâche	Description	Compétences requises
Incluez les fichiers de dépendance.	Si vous souhaitez obtenir des informations sur les frameworks et les dépendances dont les fichiers physiques ne font pas partie du dossier que vous analysez, assurez-vous d'inclure les fichiers de dépendance (tels que les fichiers pom.xml, build.gradle, package.json ou .vcsproj).	N/A
Appelez l'agent local.	Exécutez l'agent local sur votre ordinateur Windows local.	N/A

Tâche	Description	Compétences requises
Choisissez le dossier qui contient votre code source.	Choisissez le dossier qui contient votre code source. Vous pouvez ajouter plusieurs dossiers à découvrir par l'agent local. Bien que l'agent local prenne en charge la découverte de sources par le biais de chemins réseau, vous devez vous assurer que les dossiers sources se trouvent sur votre machine locale. **Important** Nous vous recommandons d'exécuter plusieurs analyses s'il y a plus de 10 000 fichiers dans vos dossiers sources.	N/A

Tâche	Description	Compétences requises
Lancez la découverte de fichiers.	Sur le tableau de bord de l'agent local, choisissez Discover Files. L'agent local découvre les fichiers dans vos dossiers et sous-dossiers, et détecte leurs technologies. Vous pouvez cliquer sur le bouton Annuler pour annuler la découverte à tout moment. Une fois la découverte des fichiers terminée, l'agent local répertorie les dossiers et les fichiers trouvés. La colonne Technologies indique les technologies associées et le nombre de fichiers. La colonne Path indique l'emplacement des dossiers et des fichiers.	N/A

Tâche	Description	Compétences requises
Affinez la configuration de numérisation du code source.	(Facultatif) Pour affiner le scan de l'agent local, vous pouvez désactiver une ou plusieurs technologies pour un dossier ou un fichier spécifique. Si toutes les technologies sont désactivées, votre dossier ou fichier sera exclu de la portée de l'analyse. Pour désactiver les technologies, choisissez l'étiquette jaune de la technologie que vous souhaitez désactiver. Vous pouvez également choisir l'icône du filtre lorsque vous survolez un fichier ou un dossier pour associer une technologie à un fichier ou un dossier spécifique. Ces paramètres sont enregistrés et accélèrent le processus de découverte du dossier ou du fichier.	N/A
Lancez l'analyse du code source.	Après avoir configuré votre analyse, choisissez « Numériser les fichiers » pour commencer le processus de numérisation.	N/A

Tâche	Description	Compétences requises
Vérifiez les étiquettes vertes ou grises.	Une fois l'analyse du code source terminée, une étiquette d'état s'affiche au niveau des dossiers et des fichiers. Une étiquette verte signifie que les fichiers ont été correctement scannés avec la technologie associée. Une étiquette grise signifie que les fichiers n'ont pas été scannés et sont exclus. La raison de leur exclusion s'affiche lorsque vous passez le curseur sur l'étiquette de chaque fichier. Les raisons possibles de l'exclusion de fichiers incluent les fichiers binaires, les fichiers illisibles, les fichiers manquants, les bibliothèques externes, les fichiers codés, les fichiers générés, les erreurs de syntaxe, le contenu qui n'est pas dans la langue attendue, le code non conforme aux critères d'analyse suffisants, les fichiers dont la taille dépasse la limite (10 Mo), les problèmes de délai d'attente ou l'indisponibilité de l'analyseur.	N/A

Tâche	Description	Compétences requises
Modifiez la configuration de numérisation et scannez à nouveau le code.	(Facultatif) Vous pouvez modifier vos paramètres de configuration de numérisation et choisir Analyser les fichiers pour scanner à nouveau les fichiers.	N/A
Confirmez les résultats du scan.	Choisissez Confirmer les résultats si les résultats du scan répondent à vos exigences.	N/A
Affichez les frameworks et les bibliothèques de logiciels trouvés par l'agent local.	Affichez les frameworks et les bibliothèques logicielles utilisés ou référencés par vos applications et découvert s par l'agent local lors de l'analyse du code. Vous pouvez conserver ou ignorer les éléments de ces listes en choisissant leur bouton de commutation individuel. Choisissez Confirmer les dépendances pour continuer. ⚠ Important Si un framework est désactivé, il n'est pas répertorié dans le portail CAST Highlight ni joint à votre applicati on.	N/A

Tâche	Description	Compétences requises
Enregistrez les résultats du scan du code.	L'agent local affiche un résumé des résultats de votre analyse de code regroupés par technologie. Choisisse z Enregistrer et spécifiez le dossier dans lequel vous souhaitez enregistrer les résultats. L'agent local génère un fichier .zip par scan, qui contient tous les résultats de l'analyse. En fonction du nombre de technologies distinctes et de dossiers sources racines, l'agent local génère automatiq uement un ou plusieurs fichiers .csv avec la structure de dénomination FolderNam e.TECHNOLOGY.Date.csv.	N/A
Téléchargez les résultats du scan de code sur le portail CAST Highlight.	Dans le portail CAST Highlight , choisissez les applications que vous avez analysées dans la section Applications Scans. Choisissez Upload Results et choisissez les fichiers .csv. Vous pouvez également télécharger les fichiers .csv individuellement. Une fois que chaque fichier est chargé, un enregistrement du téléchargement apparaît sur votre écran.	N/A

Tâche	Description	Compétences requises
Supprimez les fichiers de résultats d'analyse, si nécessaire.	(Facultatif) Un fichier de résultats d'analyse peut être supprimé à tout moment pendant le processus de téléchargement en cliquant sur l'icône de la corbeille. **Important** Seuls les utilisateurs disposant de privilèges de gestionnaire de portefeuille ou le contributeur qui a téléchargé les résultats peuvent supprimer les résultats.	N/A

Tâche	Description	Compétences requises
Répondez à l'enquête de candidature.	Un bouton Sondage apparaît sur les applications qui nécessitent un sondage. Choisissez Sondage, répondez aux questions pour chaque section du sondage, puis choisissez Soumettre une fois que vous avez terminé. La progression de votre enquête est affichée en haut de votre écran. Vous pouvez soumettre vos résultats une fois que toutes les informations obligatoires ont été soumises. Cependant , vous pouvez enrichir les données de l'instance CAST Highlight de votre organisat ion en répondant à toutes les questions.	N/A
Soumettez les résultats du scan du code.	Après avoir chargé tous les fichiers de résultats .csv de l'application et répondu aux questions du sondage, choisissez Soumettre dans la section Scans de l'application. Cette étape est nécessaire pour terminer le processus et garantir que les résultats sont disponibles sur le portail CAST Highlight.	N/A

Analyse des résultats

Tâche	Description	Compétences requises
Voir la page d'accueil du portail CAST Highlight.	La page d'accueil du portail CAST Highlight inclut des vignettes contenant des informations de haut niveau sur votre portefeuille d'applications, telles que l'état de santé des logiciels CloudReady, et les scores de sécurité open source pour l'ensemble de votre portefeuille. La page d'accueil indique également le nombre d'applications intégrées. Pour plus d'informations sur les définitions des métriques CAST Highlight et la méthodologie de mesure, voir CAST Highlight — Métriques et méthodologie (PowerPoint présentation Microsoft).	N/A
Consultez le CloudReady tableau de bord.	Choisissez la CloudReady vignette pour ouvrir le CloudReady tableau de bord. Il s'agit du principal tableau de bord au niveau du portefeuille permettant d'évaluer l'état de préparation de vos applications au cloud. Il vous aide à planifier et à développer une feuille de route de portefeuille pour votre migration vers le cloud	N/A

Tâche	Description	Compétences requises
Consultez le tableau de bord de Portfolio Advisor for Cloud.	Le tableau de bord Portfolio Advisor for Cloud segmente automatiquement les applications selon les catégories de migration recommandées. La segmentation est basée sur les caractéristiques techniques de chaque application. Les facteurs incluent l'analyse du code source (préparation au cloud, résilience logicielle, etc.) et l'impact commercial, qui ressort de l'enquête. Dans le coin supérieur droit, choisissez Compute pour générer les recommandations de segmentation initiales. Les bulles dans les graphiques en haut du tableau de bord représentent chaque application du portefeuille, organisée selon la segmentation recommandée. Chaque application est également répertoriée dans un tableau de données situé sous les graphiques, y compris les mesures pertinentes pour chaque application. Les segments possibles recommandés sont les suivants :	N/A

Tâche	Description	Compétences requises
	• Réhébergement : recommandation visant à modifier la configuration de l'infrastructure de l'application afin de la transférer et de la transférer vers le cloud en utilisant une solution d'infrastructure en tant que service (IaaS). • Refactorisation : recommandation visant à apporter de légères modifications au code de l'application sans en modifier l'architecture ou les fonctionnalités afin de pouvoir le migrer à l'aide d'une solution de conteneur en tant que service (CaaS) ou de plate-forme en tant que service (PaaS). • Réarchitecture : recommandation visant à modifier radicalement le code de l'application afin d'améliorer l'état de l'application et de la préparer à la migration en utilisant une solution PaaS ou de la déployer en tant qu'application sans serveur à l'aide d'une solution de fonction en tant que service (FaaS).	

Tâche	Description	Compétences requises
	• Reconstruire : recommandation de supprimer le code de l'application et de le développer à nouveau dans le cloud à l'aide d'une solution PaaS ou de le développer à nouveau en tant qu'application sans serveur à l'aide d'une solution FaaS. • Retraite : recommandation de supprimer complètement l'application ou de la remplacer éventuellement par une alternative commerciale au logiciel en tant que service (SaaS).	

Tâche	Description	Compétences requises
Modifiez les recommandations de segmentation.	Dans certains cas, vous pouvez choisir de modifier le segment recommandé par CAST Highlight. Vous pouvez le faire en accédant à l'application dans le tableau de données et en sélectionnant un segment différent dans la liste déroulante à côté du nom de l'application. Choisissez ensuite Enregistrer dans le coin supérieur droit pour enregistrer vos modifications. Vous pouvez également exporter ces données à tout moment en choisissant Exporter en haut à droite.	N/A

Tâche	Description	Compétences requises
Choisissez une application à analyser.	Sur le tableau de bord de Portfolio Advisor for Cloud, choisissez une bulle d'application pour analyser cette application. Choisissez le nom de l'application dans le tableau après le graphique à bulles pour commencer une analyse plus approfondie. Différents tableaux de bord sont disponibles pour analyser les applications individuelles, tels que Code Insights (modèles de santé des logiciels), Trends et Software Composition (risques liés à l'open source).	N/A

Tâche	Description	Compétences requises
Analysez les CloudReady résultats d'une application individuelle.	Choisissez l'CloudRead yonglet qui affiche le CloudReady score global de l'application. Ce score est une moyenne pondérée basée sur une combinaison des réponses au CloudRead y sondage et du scan CloudReady du code. Les réponses aux questions de l'enquête apparaissent dans le tableau situé sous les vignettes. Choisissez CloudReady Code Scan pour afficher les résultats du scan de code. Il existe une liste de CloudRead y modèles pour lesquels le code de l'application a été scanné. Cette liste comprend les colonnes suivantes : • Cloud Requirement est le modèle de code spécifique. • La technologie est le langage de programma tion du modèle. « Impact » est l'impact du modèle sur l'application (C = code, F = framework, A = architect ure). • La criticité est le niveau d'importance qu'il y a à	N/A

Tâche	Description	Compétences requises
	corriger ce schéma avant de procéder à la migration. • La contribution est la façon dont ce modèle contribue au CloudReady score global. Si le motif est vert, cela augmente le CloudReady score. Si le motif est rouge, il s'agit d'un bloqueur qui diminue le CloudReady score. Si le motif n'a pas de couleur, c'est un bloqueur qui n'a pas été détecté et qui augmente le CloudRead y score. • Les barrages routiers sont le nombre d'occurrences individuelles d'un schéma de blocage. Choisissez le numéro du barrage routier pour afficher la liste des fichiers de code source dans lesquels le modèle a été détecté. • Est. L'effort est une estimation du nombre de jours qu'il faudra pour éliminer les obstacles dans chaque rangée.	

Tâche	Description	Compétences requises
Exportez les données vers Microsoft Excel.	(Facultatif) Choisissez Exporter vers Excel pour exporter les données en vue d'une analyse plus approfondie. Les données des résultats de l'analyse des applications peuvent être utilisées pour analyser plus en détail l'état de préparation d'une application au cloud et déterminer le code à mettre à jour avant une migration.	N/A
Afficher les recommandations.	Choisissez Recommandations à côté de CloudReady Code Scan pour afficher l'écran des recommandations de service cloud. Cela permet d'identifier les services AWS que l'application pourrait adopter en fonction de ses caractéristiques. Répétez cette étape pour afficher les recommandations pour toutes les applications que vous avez analysées.	N/A

Ressources connexes

Gestion des campagnes

- Section 3 de la formation à la certification CAST Highlight Foundation : Configuration du portefeuille (vidéo)

Analyse du code source

- Section 4 de la formation à la certification CAST Highlight Foundation : Analyse des applications (vidéo)

Autres ressources

- Le point fort de CAST sur AWS Marketplace
- AWS et CAST : accélérer la modernisation des applications
- CAST Highlight — Documentation, didacticiels sur les produits et outils tiers
- CAST Highlight — Démonstration du produit Cloud Readiness (vidéo)
- Modernisation du portefeuille d'applications avec CAST Highlight (atelier AWS)

Archivez automatiquement les éléments sur Amazon S3 à l'aide de DynamoDB TTL

Créée par Tabby Ward (AWS)

Récapitulatif

Ce modèle fournit des étapes pour supprimer les anciennes données d'une table Amazon DynamoDB et les archiver dans un bucket Amazon Simple Storage Service (Amazon S3) sur Amazon Web Services (AWS) sans avoir à gérer un parc de serveurs.

Ce modèle utilise Amazon DynamoDB Time to Live (TTL) pour supprimer automatiquement les anciens éléments et Amazon DynamoDB Streams pour capturer les articles dont le TTL a expiré. Il connecte ensuite DynamoDB Streams à AWS Lambda, qui exécute le code sans provisionner ni gérer de serveurs.

Lorsque de nouveaux éléments sont ajoutés au flux DynamoDB, la fonction Lambda est lancée et écrit les données dans un flux de diffusion Amazon Data Firehose. Firehose fournit une solution simple et entièrement gérée pour charger les données sous forme d'archive dans Amazon S3.

DynamoDB est souvent utilisé pour stocker des données de séries chronologiques, telles que les données de clics sur les pages Web ou les données de l'Internet des objets (IoT) provenant de capteurs et d'appareils connectés. Plutôt que de supprimer les éléments les moins fréquemment consultés, de nombreux clients souhaitent les archiver à des fins d'audit. Le TTL simplifie cet archivage en supprimant automatiquement les éléments en fonction de l'attribut timestamp.

Les éléments supprimés par TTL peuvent être identifiés dans DynamoDB Streams, qui capture une séquence chronologique de modifications au niveau des éléments et stocke la séquence dans un journal pendant 24 heures au maximum. Ces données peuvent être consommées par une fonction Lambda et archivées dans un compartiment Amazon S3 afin de réduire les coûts de stockage. Pour réduire davantage les coûts, des règles de cycle de vie Amazon S3 peuvent être créées pour transférer automatiquement les données (dès leur création) vers les classes de stockage les moins coûteuses, telles que S3 Glacier Instant Retrieval ou S3 Glacier Flexible Retrieval, ou Amazon S3 Glacier Deep Archive pour le stockage à long terme.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.

- AWS Command Line Interface (AWS CLI) 1.7 ou version ultérieure, installée et configurée sous macOS, Linux ou Windows.
- Python 3.7 ou version ultérieure.
- Boto3, installé et configuré. Si Boto3 n'est pas déjà installé, exécutez la `python -m pip install boto3` commande pour l'installer.

Architecture

Pile technologique

- Amazon DynamoDB
- Amazon DynamoDB Streams
- Amazon Data Firehose
- AWS Lambda
- Amazon S3

1. Les éléments sont supprimés par TTL.
2. Le déclencheur de flux DynamoDB invoque la fonction de processeur de flux Lambda.
3. La fonction Lambda place les enregistrements dans le flux de diffusion Firehose au format batch.
4. Les enregistrements de données sont archivés dans le compartiment S3.

Outils

- AWS CLI — L'interface de ligne de commande AWS (AWS CLI) est un outil unifié permettant de gérer vos services AWS.
- Amazon DynamoDB — Amazon DynamoDB est une base de données de documents et de valeurs clés qui fournit des performances à un chiffre en millisecondes à n'importe quelle échelle.
- Amazon DynamoDB Time to Live (TTL) : Amazon DynamoDB TTL vous aide à définir un horodatage par article afin de déterminer à quel moment un article n'est plus nécessaire.
- Amazon DynamoDB Streams — Amazon DynamoDB Streams capture une séquence chronologique de modifications au niveau des éléments dans n'importe quelle table DynamoDB et stocke ces informations dans un journal pendant 24 heures maximum.

- Amazon Data Firehose — Amazon Data Firehose est le moyen le plus simple de charger de manière fiable des données de streaming dans des lacs de données, des magasins de données et des services d'analyse.
- AWS Lambda — AWS Lambda exécute du code sans qu'il soit nécessaire de configurer ou de gérer des serveurs. Vous payez uniquement pour le temps de calcul consommé.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une évolutivité, une disponibilité des données, une sécurité et des performances de pointe.

Code

Le code de ce modèle est disponible dans les éléments d' GitHub archivage vers S3 à l'aide du référentiel TTL DynamoDB.

Épopées

Configuration d'une table DynamoDB, d'un TTL et d'un flux DynamoDB

Tâche	Description	Compétences requises

Créez une table DynamoDB.	Utilisez l'AWS CLI pour créer une table dans DynamoDB appelée. `Reservation` Choisissez une unité de capacité de lecture aléatoire (RCU) et une unité de capacité d'écriture (WCU), et attribuez deux attributs à votre table : `ReservationID` et. `ReservationDate`
	
	`aws dynamodb create-table \`
	`--table-name Reservation \`
	`--attribute-definitions Attribute Name=ReservationID`
		Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	`,AttributeType=S AttributeName=ReservationDate,AttributeType=N \ --key-schema AttributeName=ReservationID,KeyType=HASH AttributeName=ReservationDate,KeyType=RANGE \ --provisioned-throughput ReadCapacityUnits=100,WriteCapacityUnits=100` `ReservationDate` est un horodatage d'époque qui sera utilisé pour activer le TTL.	
Activez DynamoDB TTL.	Utilisez l'AWS CLI pour activer DynamoDB TTL pour l'attribut. `ReservationDate` `aws dynamodb update-time-to-live \ --table-name Reservation\ --time-to-live-specification Enabled=true,AttributeName=ReservationDate`	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
Activez un flux DynamoDB.	Utilisez l'AWS CLI pour activer un flux DynamoDB pour `Reservation` la table en utilisant `NEW_AND_OLD_IMAGES` le type de flux. `aws dynamodb update-table \ --table-name Reservation \ --stream-specification StreamEnabled=true,StreamViewType=NEW_AND_OLD_IMAGES` Ce flux contiendra des enregistrements pour les nouveaux éléments, les éléments mis à jour, les éléments supprimés et les éléments supprimés par TTL. Les enregistrements des éléments supprimés par TTL contiennent un attribut de métadonnées supplémentaire pour les distinguer des éléments supprimés manuellement. Le `userIdentity` champ pour les suppressions TTL indique que le service DynamoDB a effectué l'action de suppression.	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	Dans ce modèle, seuls les éléments supprimés par TTL sont archivés, mais vous ne pouvez archiver que les enregistrements dont le nom `eventName` est `REMOVE` et le contenu `userIdentity` sont `principalId` égaux à`dynamodb.amazonaws.com` .	

Création et configuration d'un compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	Utilisez la CLI AWS pour créer un compartiment S3 de destination dans votre région AWS, en le `us-east-1` remplaçant par votre région et amzn-s3- demo-destination-bucket par le nom de votre compartiment. `aws s3api create-bucket \ --bucket amzn-s3-demo-destination-bucket \ --region us-east-1` Assurez-vous que le nom de votre compartiment S3 est unique au monde, car l'espace de noms est partagé par tous les comptes AWS.	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
Créez une politique de cycle de vie de 30 jours pour le compartiment S3.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon S3. 2. Choisissez le compartiment S3 qui contient les données de Firehose. 3. Dans le compartiment S3, choisissez l'onglet Gestion, puis choisissez Ajouter une règle de cycle de vie. 4. Entrez un nom pour votre règle dans la boîte de dialogue Règle du cycle de vie et configurez une règle de cycle de vie de 30 jours pour votre compartiment.	Architecte cloud, développeur d'applications

Création d'un flux de diffusion Firehose

Tâche	Description	Compétences requises
Créez et configurez un flux de diffusion Firehose.	Téléchargez et modifiez l'exemple de `CreateFireHoseToS3.py` code depuis le GitHub référentiel. Ce code est écrit en Python et explique comment créer un flux de diffusion Firehose et un rôle AWS Identity and Access Management (IAM). Le rôle IAM aura une politique qui pourra être utilisée par	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	Firehose pour écrire dans le compartiment S3 de destination. Pour exécuter le script, utilisez les arguments de commande et de ligne de commande suivants. Argument 1=<Your_S3_bucket_ARN> , qui est le nom de ressource Amazon (ARN) du bucket que vous avez créé précédemment Argument 2= Le nom de votre Firehose (ce pilote utilise.) firehose_to_s3_stream Argument 3= Le nom de votre rôle IAM (ce pilote utilisefirehose_to_s3 .) `python CreateFirehoseToS3.py <Your_S3_Bucket_ARN> firehose_to_s3_stream firehose_to_s3` Si le rôle IAM spécifié n'existe pas, le script créera un rôle d'assume avec une politique de relation de confiance, ainsi qu'une politique accordant une autorisation Amazon S3 suffisante. Pour des	

Tâche	Description	Compétences requises
	exemples de ces politiques, consultez la section Informati ons supplémentaires.	
Vérifiez le flux de diffusion de Firehose.	Décrivez le flux de diffusion Firehose à l'aide de la CLI AWS pour vérifier que le flux de diffusion a été créé avec succès. `aws firehose describe-delivery-stream --delivery-stream-name firehose_to_s3_stream`	Architecte cloud, développeur d'applications

Créez une fonction Lambda pour traiter le flux de diffusion Firehose

Tâche	Description	Compétences requises
Créez une politique de confiance pour la fonction Lambda.	Créez un fichier de politique de confiance contenant les informations suivantes. `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" },`	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises

	<pre>"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>
	Cela donne à votre fonction l'autorisation d'accéder aux ressources AWS.	

Créez un rôle d'exécution pour la fonction Lambda.	Pour créer le rôle d'exécution, exécutez le code suivant.
	<pre>aws iam create-role
	--role-name lambda-
	ex --assume-role-poli
	cy-document file://Tr
	ustPolicy.json</pre>
		Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises

Ajoutez une autorisation au rôle.	Pour ajouter une autorisation au rôle, utilisez la `attach-policy-to-role` commande.
	
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaDynamoDBExecutionRole`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/AmazonKinesisFirehoseFullAccess`
	`aws iam attach-role-policy --role-name lambda-ex --policy-arn arn:aws:iam::aws:policy/IAMFullAccess`
		Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises

Créez une fonction Lambda.	Compressez le `LambdaStreamProcessor.py` fichier depuis le référentiel de code en exécutant la commande suivante.
	`zip function.zip LambdaStreamProcessor.py`
	Lorsque vous créez la fonction Lambda, vous aurez besoin de l'ARN du rôle d'exécution Lambda. Pour obtenir l'ARN, exécutez le code suivant.
	`aws iam get-role \ --role-name lambda-ex`
	Pour créer la fonction Lambda, exécutez le code suivant.
	`# Review the environment variables and replace them with your values.`
	`aws lambda create-function --function-name LambdaStreamProcessor \ --zip-file fileb://function.zip --handler LambdaStreamProcessor.handler --runtime python3.8 \ --role {Your Lamda Execution Role ARN}\`
		Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	`--environment Variables="{firehose_name=firehose_to_s3_stream,bucket_arn = <Your_S3_bucket_ARN>,iam_role_name = firehose_to_s3, batch_size=400}"`	
Configurez le déclencheur de la fonction Lambda.	Utilisez l'AWS CLI pour configurer le déclencheur (DynamoDB Streams), qui appelle la fonction Lambda. La taille du lot de 400 permet d'éviter de rencontrer des problèmes de simultanéité Lambda. `aws lambda create-event-source-mapping --function-name LambdaStreamProcessor \ --batch-size 400 --starting-position LATEST \ --event-source-arn <Your Latest Stream ARN From DynamoDB Console>`	Architecte cloud, développeur d'applications

Testez les fonctionnalités

Tâche	Description	Compétences requises
Ajoutez les articles dont l'horodatage a expiré au tableau des réservations.	Pour tester la fonctionnalité, ajoutez au tableau des éléments dont l'horodat	Architecte du cloud

Tâche	Description	Compétences requises
	age d'époque a expiré. `Reservation TTL` supprimera automatiquement les éléments en fonction de l'horodatage. La fonction Lambda est lancée lors des activités de DynamoDB Stream, et elle filtre l'événement pour identifier l'activité ou les éléments supprimés. `REMOVE` Il place ensuite les enregistrements dans le flux de diffusion Firehose au format batch. Le flux de livraison Firehose transfère les articles vers un compartiment S3 de destination avec le `firehose3example/year=current year/month=current month/day=current day/hour=current hour/` préfixe. **Important** Pour optimiser la récupération des données, configurez Amazon S3 avec le `Prefix` et `ErrorOutputPrefix` qui est détaillé dans la	

Tâche	Description	Compétences requises
	section Informations supplémentaires.	

Nettoyez les ressources

Tâche	Description	Compétences requises
Supprimez toutes les ressources.	Supprimez toutes les ressources pour vous assurer que les services que vous n'utilisez pas ne vous seront pas facturés.	Architecte cloud, développeur d'applications

Ressources connexes

- Gestion du cycle de vie de votre stockage
- Classes de stockage Amazon S3
- Documentation du kit SDK AWS pour Python (Boto3)

Informations supplémentaires

Création et configuration d'un flux de diffusion Firehose — Exemples de politiques

Exemple de document de politique sur les relations de confiance Firehose

```
firehose_assume_role = {
        'Version': '2012-10-17',
        'Statement': [
            {
                'Sid': '',
                'Effect': 'Allow',
                'Principal': {
                    'Service': 'firehose.amazonaws.com'
                },
                'Action': 'sts:AssumeRole'
```

```
            }
        ]
    }
```

Exemple de politique d'autorisations S3

```
s3_access = {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Action": [
                    "s3:AbortMultipartUpload",
                    "s3:GetBucketLocation",
                    "s3:GetObject",
                    "s3:ListBucket",
                    "s3:ListBucketMultipartUploads",
                    "s3:PutObject"
                ],
                "Resource": [
                    "{your s3_bucket ARN}/*",
                    "{Your s3 bucket ARN}"
                ]
            }
        ]
    }
```

Tester la fonctionnalité — Configuration Amazon S3

La configuration Amazon S3 avec les éléments suivants `Prefix` `ErrorOutputPrefix` est choisie pour optimiser la récupération des données.

prefix

```
firehosetos3example/year=! {timestamp: yyyy}/month=! {timestamp:MM}/day=!
 {timestamp:dd}/hour=!{timestamp:HH}/
```

Firehose crée d'abord un dossier de base appelé `firehosetos3example` directement sous le compartiment S3. Il évalue ensuite les expressions`!{timestamp:yyyy}`,`!{timestamp:MM}`, `!{timestamp:dd}` et `!{timestamp:HH}` en fonction de l'année, du mois, du jour et de l'heure en utilisant le DateTimeFormatterformat Java.

Par exemple, un horodatage d'arrivée approximatif de 1604683577 dans Unix Epoch Time équivaut à,, et. `year=2020` `month=11` `day=06` `hour=05` Par conséquent, l'emplacement dans Amazon S3, où les enregistrements de données sont livrés, est évalué à`firehosetos3example/year=2020/month=11/day=06/hour=05/`.

ErrorOutputPrefix

```
firehosetos3erroroutputbase/!{firehose:random-string}/!{firehose:error-output-type}/!{timestamp:yyyy/MM/dd}/
```

Le `ErrorOutputPrefix` résultat est un dossier de base appelé `firehosetos3erroroutputbase` directement sous le compartiment S3. L'expression est `!{firehose:random-string}` évaluée en une chaîne aléatoire de 11 caractères telle que. `ztWxkdg3Thg` L'emplacement d'un objet Amazon S3 où les enregistrements défaillants sont livrés peut être évalué à`firehosetos3erroroutputbase/ztWxkdg3Thg/processing-failed/2020/11/06/`.

Créez une architecture sans serveur multi-locataires dans Amazon Service OpenSearch

Créée par Tabby Ward (AWS) et Nisha Gambhir (AWS)

Récapitulatif

Amazon OpenSearch Service est un service géré qui facilite le déploiement, l'exploitation et le dimensionnement d'Elasticsearch, un moteur de recherche et d'analyse open source populaire. OpenSearch Le service fournit une recherche en texte libre ainsi qu'une ingestion et un tableau de bord en temps quasi réel pour les données de streaming telles que les journaux et les métriques.

Les fournisseurs de logiciels en tant que service (SaaS) utilisent fréquemment le OpenSearch service pour répondre à un large éventail de cas d'utilisation, tels que l'obtention d'informations sur les clients de manière évolutive et sécurisée tout en réduisant la complexité et les temps d'arrêt.

L'utilisation OpenSearch du service dans un environnement mutualisé introduit une série de considérations qui affectent le partitionnement, l'isolation, le déploiement et la gestion de votre solution SaaS. Les fournisseurs de SaaS doivent réfléchir à la manière de faire évoluer efficacement leurs clusters Elasticsearch face à des charges de travail en constante évolution. Ils doivent également tenir compte de l'impact de la hiérarchisation et des conditions de voisinage bruyantes sur leur modèle de partitionnement.

Ce modèle passe en revue les modèles utilisés pour représenter et isoler les données des locataires à l'aide des constructions Elasticsearch. En outre, le modèle se concentre sur une architecture de référence sans serveur simple à titre d'exemple pour illustrer l'indexation et la recherche à l'aide de OpenSearch Service dans un environnement mutualisé. Il met en œuvre le modèle de partitionnement des données du pool, qui partage le même indice entre tous les locataires tout en préservant l'isolation des données d'un locataire. Ce modèle utilise les AWS services suivants : Amazon API Gateway AWS Lambda, Amazon Simple Storage Service (Amazon S3) et Service. OpenSearch

Pour plus d'informations sur le modèle de pool et les autres modèles de partitionnement des données, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS

- AWS Command Line Interface (AWS CLI) version 2.x, installée et configurée sur macOS, Linux ou Windows
- Version 3.9 de Python
- pip3 — Le code source Python est fourni sous forme de fichier .zip à déployer dans une fonction Lambda. Si vous souhaitez utiliser le code localement ou le personnaliser, procédez comme suit pour développer et recompiler le code source :
  1. Générez le `requirements.txt` fichier en exécutant la commande suivante dans le même répertoire que les scripts Python : `pip3 freeze > requirements.txt`
  2. Installez les dépendances : `pip3 install -r requirements.txt`

Limites

- Ce code fonctionne en Python et ne prend actuellement pas en charge les autres langages de programmation.
- L'exemple d'application n'inclut pas de support AWS interrégional ou de reprise après sinistre (DR).
- Ce modèle est destiné à des fins de démonstration uniquement. Il n'est pas destiné à être utilisé dans un environnement de production.

Architecture

Le schéma suivant illustre l'architecture de haut niveau de ce modèle. L'architecture inclut les éléments suivants :

- Lambda pour indexer et interroger le contenu
- OpenSearch Service pour effectuer une recherche
- API Gateway pour fournir une interaction API avec l'utilisateur
- Amazon S3 pour stocker des données brutes (non indexées)
- Amazon CloudWatch va surveiller les journaux
- AWS Identity and Access Management (IAM) pour créer des rôles et des politiques de locataire

Automatisation et mise à l'échelle

Pour des raisons de simplicité, le modèle AWS CLI est utilisé pour provisionner l'infrastructure et déployer l'exemple de code. Vous pouvez créer un AWS CloudFormation modèle ou AWS Cloud Development Kit (AWS CDK) des scripts pour automatiser le modèle.

Outils

Services AWS

- AWS CLIest un outil unifié de gestion Services AWS et de gestion des ressources à l'aide de commandes dans votre interface de ligne de commande.
- Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- API Gateway permet de créer, Service AWS de publier, de maintenir, de surveiller et de sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- Amazon S3 est un service de stockage d'objets qui vous permet de stocker et de récupérer n'importe quel volume d'informations à tout moment, où que vous soyez sur le Web.
- OpenSearch Le service est un service entièrement géré qui vous permet de déployer, de sécuriser et d'exécuter Elasticsearch facilement et de manière rentable à grande échelle.

Code

La pièce jointe fournit des fichiers d'exemple pour ce modèle. Il s'agit des licences suivantes :

- `index_lambda_package.zip`— La fonction Lambda pour indexer les données dans OpenSearch Service à l'aide du modèle de pool.
- `search_lambda_package.zip`— La fonction Lambda pour rechercher des données dans OpenSearch Service.
- `Tenant-1-data`— Échantillon de données brutes (non indexées) pour Tenant-1.
- `Tenant-2-data`— Échantillon de données brutes (non indexées) pour Tenant-2.

Important

Les articles de ce modèle incluent des exemples de AWS CLI commandes formatés pour Unix, Linux et macOS. Pour Windows, remplacez le caractère de continuation Unix, à savoir la barre oblique inversée (\), à la fin de chaque ligne par un accent circonflexe (^).

Note

Dans AWS CLI les commandes, remplacez toutes les valeurs entre crochets (**<>**) par les valeurs correctes.

Épopées

Création et configuration d'un compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment S3 dans votre Région AWS. Ce compartiment contiendra les données du locataire non indexées pour l'exemple d'application. Assurez-vous que le nom du compartiment S3 est unique au monde, car l'espace de noms est partagé par tous Comptes AWS. Pour créer un compartiment S3, vous pouvez utiliser la commande AWS CLI create-bucket comme suit : `aws s3api create-bucket \`	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

	`--bucket <tenantrawdata> \`
	`--region <your-AWS-Region>`
	
	où `tenantrawdata` est le nom du compartiment S3. (Vous pouvez utiliser n'importe quel nom unique conforme aux directives de dénomination des compartiments.)	

Création et configuration d'un cluster Elasticsearch

Tâche	Description	Compétences requises

Créez un domaine OpenSearch de service.	Exécutez la AWS CLI create-elasticsearch-domain commande pour créer un domaine OpenSearch de service :
	
	`aws es create-elasticsearch-domain \`
	`--domain-name vpc-cli-example \`
	`--elasticsearch-version 7.10 \`
	`--elasticsearch-cluster-config InstanceType=t3.medium.elasticsearch,InstanceCount=1 \`
	`--ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=10 \`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	`--domain-endpoint-options "{\"EnforceHTTPS\": true}" \ --encryption-at-rest-options "{\"Enabled\": true}" \ --node-to-node-encryption-options "{\"Enabled\": true}" \ --advanced-security-options "{\"Enabled\": true, \"InternalUserDatabaseEnabled\": true, \ \"MasterUserOptions\": {\"MasterUserName\": \"KibanaUser\", \ \"MasterUserPassword\": \"NewKibanaPassword@123\"}}" \ --vpc-options "{\"SubnetIds\": [\"<subnet-id>\"], \"SecurityGroupIds\": [\"<sg-id>\"]}" \ --access-policies "{\"Version\": \"2012-10-17\", \"Statement\": [{ \"Effect\": \"Allow\", \ \"Principal\": {\"AWS\": \"*\" }, \"Action\":\"es:*\", \ \"Resource\": \"arn:aws:es:<region>:<account-id>:domain\/vpc-cli-example\/*\" }] }"`	

Tâche	Description	Compétences requises
	Le nombre d'instances est défini sur 1 car le domaine est destiné à des fins de test. Vous devez activer le contrôle d'accès détaillé à l'aide du `advanced-security-options` paramètre, car les détails ne peuvent pas être modifiés une fois le domaine créé. Cette commande crée un nom d'utilisateur principal (`KibanaUser`) et un mot de passe que vous pouvez utiliser pour vous connecter à la console Kibana. Le domaine faisant partie d'un cloud privé virtuel (VPC), vous devez vous assurer que vous pouvez accéder à l'instance Elasticsearch en spécifiant la politique d'accès à utiliser. Pour plus d'informations, consultez la section Lancement de vos domaines Amazon OpenSearch Service au sein d'un VPC dans la AWS documentation.	

Tâche	Description	Compétences requises

Configurez un hôte bastion.	Configurez une instance Windows Amazon Elastic Compute Cloud (Amazon EC2) en tant qu'hôte bastion pour accéder à la console Kibana. Le groupe de sécurité Elasticsearch doit autoriser le trafic provenant du groupe de EC2 sécurité Amazon. Pour obtenir des instructions, consultez le billet de blog Contrôler l'accès réseau aux EC2 instances à l'aide d'un serveur Bastion.
	
	Lorsque l'hôte bastion a été configuré et que le groupe de sécurité associé à l'instanc e est disponible, utilisez la AWS CLI authorize-security -group-ingresscommande pour ajouter l'autorisation au groupe de sécurité Elasticse arch afin d'autoriser le port 443 du groupe de sécurité Amazon EC2 (hôte bastion).
	
	`aws ec2 authorize-security-group-ingress \`
	`  --group-id <SecurityGroupIdfElasticSearch> \`
	`  --protocol tcp \`
	`  --port 443 \`
		Architecte cloud, administr ateur cloud

Tâche	Description	Compétences requises
	`--source-group <SecurityGroupIdfBashionHostEC2>`	

Création et configuration de la fonction d'index Lambda

Tâche	Description	Compétences requises

Créez le rôle d'exécution Lambda.	Exécutez la commande AWS CLI create-role pour accorder à la fonction d'index Lambda l'accès aux ressources et aux ressources : Services AWS
	`aws iam create-role \ --role-name index-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	où se `lambda_assume_role.json` trouve un document JSON qui accorde des `AssumeRole` autorisations à la fonction Lambda, comme suit :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": {`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	"Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }] }	

Tâche	Description	Compétences requises

Associez des politiques gérées au rôle Lambda.	Exécutez la AWS CLI attach-role-policycommande pour associer des politiques gérées au rôle créé à l'étape précédente. Ces deux politiques autorisent le rôle à créer une interface réseau élastique et à écrire des journaux dans CloudWatch Logs.
	`aws iam attach-role-policy \ --role-name index-lambda-role \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	`aws iam attach-role-policy \ --role-name index-lambda-role \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

Créez une politique pour autoriser la fonction d'index Lambda à lire les objets S3.	Exécutez la commande AWS CLI create-policy pour `s3:GetObject` autoriser la fonction d'index Lambda à lire les objets du compartiment S3 :
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3-policy.json`
	Le fichier `s3-policy.json` est un document JSON illustré ci-dessous qui accorde des `s3:GetObject` autorisations pour autoriser l'accès en lecture aux objets S3. Si vous avez utilisé un nom différent lors de la création du compartiment S3, indiquez le nom de compartiment correct dans la `Resource` section :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::<tenantrawdata>/*"`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	<pre> }] }</pre>	

Associez la politique d'autorisation Amazon S3 au rôle d'exécution Lambda.	Exécutez la AWS CLI attach-role-policycommande pour associer la politique d'autorisation Amazon S3 que vous avez créée à l'étape précédente au rôle d'exécution Lambda :
	<pre>aws iam attach-role-policy \
	  --role-name index-lambda-role \
	  --policy-arn <PolicyARN></pre>
	où `PolicyARN` est le nom de ressource Amazon (ARN) de la politique d'autorisation Amazon S3. Vous pouvez obtenir cette valeur à partir de la sortie de la commande précédente.
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
Créez la fonction d'index Lambda.	Exécutez la commande AWS CLI create-function pour créer la fonction d'index Lambda, qui accèdera à Service : OpenSearch `aws lambda create-function \ --function-name index-lambda-function \ --zip-file fileb://index_lambda_package.zip \ --handler lambda_index.lambda_handler \ --runtime python3.9 \ --role "arn:aws:iam::account-id:role/index-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
Autorisez Amazon S3 à appeler la fonction d'index Lambda.	Exécutez la AWS CLI commande add permission pour autoriser Amazon S3 à appeler la fonction d'index Lambda : `aws lambda add-permission \ --function-name index-lambda-function \ --statement-id s3-permissions \ --action lambda:InvokeFunction \ --principal s3.amazonaws.com \ --source-arn "arn:aws:s3:::<tenantrawdata>" \ --source-account "<account-id>"`	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

Ajoutez un déclencheur Lambda pour l'événement Amazon S3.	Exécutez la AWS CLI [put-bucket-notification-configuration](#)commande pour envoyer des notifications à la fonction d'index Lambda lorsque l'`ObjectCreated` événement Amazon S3 est détecté. La fonction d'index s'exécute chaque fois qu'un objet est chargé dans le compartiment S3.
	
	`aws s3api put-bucket-notification-configuration \`
	`  --bucket <tenantrawdata> \`
	`  --notification-configuration file://s3-trigger.json`
	
	Le fichier `s3-trigger.json` est un document JSON dans le dossier actuel qui ajoute la politique de ressources à la fonction Lambda lorsque l'`ObjectCreated` événement Amazon S3 se produit.
		Architecte cloud, administrateur cloud

Création et configuration de la fonction de recherche Lambda

Tâche	Description	Compétences requises

Créez le rôle d'exécution Lambda.	Exécutez la commande AWS CLI create-role pour autoriser la fonction de recherche Lambda à accéder aux ressources et aux ressources : Services AWS
	`aws iam create-role \ --role-name search-lambda-role \ --assume-role-policy-document file://lambda_assume_role.json`
	où se `lambda_assume_role.json` trouve un document JSON dans le dossier actuel qui accorde des `AssumeRole` autorisations à la fonction Lambda, comme suit :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, ...`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

	<pre>"Action":
	"sts:AssumeRole"
	}
	]
	}</pre>	

Associez des politiques gérées au rôle Lambda.	Exécutez la AWS CLI attach-role-policycommande pour associer des politiques gérées au rôle créé à l'étape précédente. Ces deux politiques autorisent le rôle à créer une interface réseau élastique et à écrire des journaux dans CloudWatch Logs.
	<pre>aws iam attach-role-policy \
	--role-name search-lambda-role \
	--policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
	
	aws iam attach-role-policy \
	--role-name search-lambda-role \
	--policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaVPCAccessExecutionRole</pre>
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
Créez la fonction de recherche Lambda.	Exécutez la commande AWS CLI create-function pour créer la fonction de recherche Lambda, qui accèdera à Service : OpenSearch `aws lambda create-function \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip \ --handler lambda_search.lambda_handler \ --runtime python3.9 \ --role "arn:aws:iam::account-id:role/search-lambda-role" \ --timeout 30 \ --vpc-config "{\"SubnetIds\": [\"<subnet-id1\>", \"<subnet-id2>\"], \ \"SecurityGroupIds\": [\"<sg-1>\"]}"`	Architecte cloud, administrateur cloud

Création et configuration des rôles de locataire

Tâche	Description	Compétences requises
Créez des rôles IAM pour les locataires.	Exécutez la commande AWS CLI create-role pour créer deux rôles de locataire qui seront utilisés pour tester la fonctionnalité de recherche :	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	`aws iam create-role \ --role-name Tenant-1-role \ --assume-role-policy-document file://assume-role-policy.json`	
	`aws iam create-role \ --role-name Tenant-2-role \ --assume-role-policy-document file://assume-role-policy.json`	
	Le fichier `assume-role-policy.json` est un document JSON dans le dossier actuel qui accorde des `AssumeRole` autorisations au rôle d'exécution Lambda : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "<Lambda execution role for index function>", "AWS": "<Lambda execution role for search function>" }, "Action": "sts:AssumeRole"`	

Tâche	Description	Compétences requises
	<pre> }] }</pre>	

Tâche	Description	Compétences requises

Créez une politique IAM pour les locataires.	Exécutez la commande AWS CLI create-policy pour créer une politique de locataire qui accorde l'accès aux opérations d'Elasticsearch :
	`aws iam create-policy \ --policy-name tenant-policy \ --policy-document file://policy.json`
	Le fichier `policy.json` est un document JSON situé dans le dossier actuel qui accorde des autorisations sur Elasticsearch :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpDelete", "es:ESHttpGet", "es:ESHttpHead", "es:ESHttpPost", "es:ESHttpPut", "es:ESHttpPatch" ],`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

	<pre>"Resource":
	[
	"<ARN of
	Elasticsearch domain
	created earlier>"
	]
	}
	]
	}</pre>	

Associez la politique IAM du locataire aux rôles du locataire .	Exécutez la AWS CLI attach-role-policycommande pour associer la politique IAM du locataire aux deux rôles de locataire que vous avez créés à l'étape précédente :
	<pre>aws iam attach-role-policy \
	--policy-arn
	arn:aws:iam::account-id:policy/tenant-policy \
	--role-name Tenant-1-role
	
	aws iam attach-role-policy \
	--policy-arn
	arn:aws:iam::account-id:policy/tenant-policy \
	--role-name Tenant-2-role</pre>
	L'ARN de la politique provient du résultat de l'étape précédente.
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

Créez une politique IAM pour autoriser Lambda à assumer ce rôle.	Exécutez la commande AWS CLI create-policy pour créer une politique permettant à Lambda d'assumer le rôle de locataire :
	`aws iam create-policy \ --policy-name assume-tenant-role-policy \ --policy-document file://lambda_policy.json`
	Le fichier `lambda_policy.json` est un document JSON dans le dossier actuel qui accorde des autorisations pour `AssumeRole` :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "<ARN of tenant role created earlier>" } ] }`
	En `Resource` effet, vous pouvez utiliser un caractère
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	générique pour éviter de créer une nouvelle politique pour chaque locataire.	

Créez une politique IAM pour autoriser le rôle d'index Lambda à accéder à Amazon S3.	Exécutez la commande AWS CLI create-policy pour autoriser le rôle d'index Lambda à accéder aux objets du compartiment S3 :
	`aws iam create-policy \ --policy-name s3-permission-policy \ --policy-document file://s3_lambda_policy.json`
	Le fichier `s3_lambda_policy.json` est le document de politique JSON suivant dans le dossier actuel :
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "s3:GetObject", "Resource": "arn:aws:s3:::tenantrawdata/*" } ] }`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

Attachez la politique au rôle d'exécution Lambda.	Exécutez la AWS CLI attach-role-policycommande pour associer la politique créée à l'étape précédente à l'index Lambda et aux rôles d'exécution de recherche que vous avez créés précédemment :
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name index-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/assume-tenant-role-policy \`
	`  --role-name search-lambda-role`
	
	`aws iam attach-role-policy \`
	`  --policy-arn arn:aws:iam::account-id:policy/s3-permission-policy \`
	`  --role-name index-lambda-role`
	
	L'ARN de la politique provient du résultat de l'étape précédente.
		Architecte cloud, administrateur cloud

Création et configuration d'une API de recherche

Tâche	Description	Compétences requises
Créez une API REST dans API Gateway.	Exécutez la AWS CLI [create-rest-api](#)commande pour créer une ressource d'API REST : `aws apigateway create-rest-api \ --name Test-Api \ --endpoint-configuration "{ \"types\": [\"REGIONAL\"] }"` Pour le type de configuration du point de terminaison, vous pouvez spécifier `EDGE` au lieu d'`REGIONAL`utiliser des emplacements périphériques au lieu d'un emplacement particulier Région AWS. Notez la valeur du `id` champ à partir de la sortie de commande. Il s'agit de l'ID d'API que vous utiliserez dans les commandes suivantes.	Architecte cloud, administrateur cloud
Créez une ressource pour l'API de recherche.	La ressource API de recherche lance la fonction de recherche Lambda avec le nom de la ressource. `search` (Il n'est pas nécessaire de créer une API pour la fonction d'index Lambda, car elle s'exécute automatiquement lorsque des objets sont	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

	chargés dans le compartiment S3.)
	
	1. Exécutez la commande AWS CLI get-resources pour obtenir l'ID parent du chemin racine :
	
	`aws apigateway get-resources \ --rest-api-id <API-ID>`
	
	Notez la valeur du champ ID. Vous utiliserez cet ID parent dans la commande suivante.
	
	`{ "items": [ { "id": "zpsri964ck", "path": "/" } ] }`
	
	2. Exécutez la commande AWS CLI create-resource pour créer une ressource pour l'API de recherche. Pour `parent-id`, spécifiez l'ID de la commande précédente.	

Tâche	Description	Compétences requises
	`aws apigateway create-resource \ --rest-api-id <API-ID> \ --parent-id <Parent-ID> \ --path-part search`	
Créez une méthode GET pour l'API de recherche.	Exécutez la commande AWS CLI put-method pour créer une `GET` méthode pour l'API de recherche : `aws apigateway put-method \ --rest-api-id <API-ID> \ --resource-id <ID from the previous command output> \ --http-method GET \ --authorization-type "NONE" \ --no-api-key-required` Pour `resource-id` , spécifiez l'ID à partir de la sortie de la `create-resource` commande.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
Créez une réponse de méthode pour l'API de recherche.	Exécutez la AWS CLI put-method-responsecommande pour ajouter une réponse de méthode pour l'API de recherche : `aws apigateway put-method-response \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --status-code 200 \ --response-models "{\"application/json\": \"Empty\"}"` Pour`resource-id` , spécifiez l'ID issu de la sortie de la `create-resource` commande précédente.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
Configurez une intégration Lambda par proxy pour l'API de recherche.	Exécutez la commande AWS CLI put-integration pour configurer une intégration avec la fonction de recherche Lambda : `aws apigateway put-integration \ --rest-api-id <API-ID> \ --resource-id <ID from the create-resource command output> \ --http-method GET \ --type AWS_PROXY \ --integration-http-method GET \ --uri arn:aws:apigateway:region:lambda:path/2015-03-31/functions/arn:aws:lambda:<region>:<account-id>:function:<function-name>/invocations`  Pour `resource-id`, spécifiez l'ID de la `create-resource` commande précédente.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
Accordez à API Gateway l'autorisation d'appeler la fonction de recherche Lambda.	Exécutez AWS CLI la commande add permission pour autoriser API Gateway à utiliser la fonction de recherche : `aws lambda add-permission \ --function-name <function-name> \ --statement-id apigateway-get \ --action lambda:InvokeFunction \ --principal apigateway.amazonaws.com \ --source-arn "arn:aws:execute-api:<region>:<account-id>:api-id/*/GET/search"` Modifiez le `source-arn` chemin si vous avez utilisé un autre nom de ressource d'API au lieu de`search`.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

Déployez l'API de recherche.	Exécutez la commande AWS CLI create-deployment pour créer une ressource de stage nommée : `dev`
	
	`aws apigateway create-deployment \`
	`  --rest-api-id <API-ID> \`
	`  --stage-name dev`
	
	Si vous mettez à jour l'API, vous pouvez utiliser la même AWS CLI commande pour la redéployer au même stade.
		Architecte cloud, administrateur cloud

Création et configuration des rôles Kibana

Tâche	Description	Compétences requises
Connectez-vous à la console Kibana.	1. Trouvez le lien vers Kibana sur le tableau de bord de votre domaine sur la console OpenSearch de service. L'URL se présente sous la forme :`<domain-endpoint>/_plugin/kibana/` . 2. Utilisez l'hôte bastion que vous avez configuré dans le premier épisode épique pour accéder à la console Kibana.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	3. Connectez-vous à la console Kibana en utilisant le nom d'utilisateur et le mot de passe principaux indiqués à l'étape précédente, lorsque vous avez créé le domaine de OpenSearch service. 4. Lorsque vous êtes invité à sélectionner un locataire, choisissez Privé.	

Tâche	Description	Compétences requises
Créez et configurez des rôles Kibana.	Pour isoler les données et empêcher un locataire de récupérer les données d'un autre locataire, vous devez utiliser la sécurité des documents, qui permet aux locataires d'accéder uniquement aux documents contenant leur identifiant de locataire. 1. Sur la console Kibana, dans le volet de navigation, choisissez Security, Role. 2. Créez un nouveau rôle de locataire. 3. Définissez les autorisations du cluster sur `indices_all`, ce qui donne des autorisations de création, de lecture, de mise à jour et de suppression (CRUD) sur l'index des OpenSearch services. 4. Limitez les autorisations d'accès à l'`tenant-data` index. (Le nom de l'index doit correspondre au nom indiqué dans les fonctions de recherche et d'index Lambda.) 5. Définissez les autorisations d'indexation sur `indices_all`, pour permettre aux	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	utilisateurs d'effectuer toutes les opérations liées à l'index. (Vous pouvez restreindre les opérations pour un accès plus précis, en fonction de vos besoins.) 6. Pour la sécurité au niveau des documents, appliquez la politique suivante pour filtrer les documents par ID de locataire, afin d'isoler les données des locataires d'un index partagé : `{ "bool": { "must": { "match": { "TenantId": "Tenant-1" } } } }` Le nom, les propriétés et les valeurs de l'index distinguent les majuscules et minuscules.	

Tâche	Description	Compétences requises
Associez les utilisateurs aux rôles.	1. Choisissez l'onglet Utilisateurs mappés pour le rôle, puis sélectionnez Cartographier les utilisateurs. 2. Dans la section Rôles principaux, spécifiez l'ARN du rôle de locataire IAM que vous avez créé précédemment, puis choisissez Map. Cela fait correspondre le rôle de locataire IAM au rôle Kibana afin que la recherche spécifique au locataire renvoie des données pour ce locataire uniquement. Par exemple, si le nom du rôle IAM pour le locataire 1 est`Tenant-1-Role` , spécifiez l'ARN pour `Tenant-1-Role` (extrait de l'épique Créer et configurer les rôles de locataire) dans la zone Rôles principaux pour le rôle Kibana du locataire 1. 3. Répétez les étapes 1 et 2 pour le locataire 2. Nous vous recommandons d'automatiser la création des rôles de locataire et de Kibana	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	au moment de l'intégration des locataires.	
Créez l'index des données des locataires.	Dans le volet de navigation, sous Gestion, choisissez Dev Tools, puis exécutez la commande suivante. Cette commande crée l'`tenant-data` index pour définir le mappage de la `TenantId` propriété. `PUT /tenant-data { "mappings": { "properties": { "TenantId": { "type": "keyword"} } } }`	Architecte cloud, administrateur cloud

Créez des points de terminaison VPC pour Amazon S3 et AWS STS

Tâche	Description	Compétences requises
Créez un point de terminaison VPC pour Amazon S3.	Exécutez la AWS CLI create-vpc-endpointcommande pour créer un point de terminaison VPC pour Amazon S3. Le point de terminaison permet à la fonction d'index Lambda du VPC d'accéder à Amazon S3. `aws ec2 create-vpc-endpoint \`	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	`--vpc-id <VPC-ID> \ --service-name com.amazonaws.us-east-1.s3 \ --route-table-ids <route-table-ID>` Pour `vpc-id`, spécifiez le VPC que vous utilisez pour la fonction d'index Lambda. Pour `service-name`, utilisez l'URL correcte pour le point de terminaison Amazon S3. Pour `route-table-ids`, spécifiez la table de routage associée au point de terminaison du VPC.	

Tâche	Description	Compétences requises
Créez un point de terminaison VPC pour. AWS STS	Exécutez la AWS CLI create-vpc-endpointcommande pour créer un point de terminaison VPC pour AWS Security Token Service ()AWS STS. Le point de terminaison permet d'accéder à l'index Lambda et aux fonctions de recherche du VPC. AWS STS Les fonctions sont utilisées AWS STS lorsqu'elles assument le rôle IAM. `aws ec2 create-vpc-endpoint \ --vpc-id <VPC-ID> \ --vpc-endpoint-type Interface \ --service-name com.amazonaws.us-east-1.sts \ --subnet-id <subnet-ID> \ --security-group-id <security-group-ID>` Pour`vpc-id`, spécifiez le VPC que vous utilisez pour l'index Lambda et les fonctions de recherche. Pour`subnet-id` , indiquez le sous-réseau dans lequel ce point de terminaison doit être créé. Pour`security-group-id` , spécifiez le groupe de sécurité auquel associer ce point de	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	terminaison. (Il peut s'agir du même groupe de sécurité que celui utilisé par Lambda.)	

Testez la mutualisation et l'isolation des données

Tâche	Description	Compétences requises
Mettez à jour les fichiers Python pour les fonctions d'index et de recherche.	1. Dans le `index_lambda_package.zip` fichier, modifiez-le pour mettre à jour l' Compte AWS ID et les informations du point de terminaison Elasticsearch. `lamba_index.py` Région AWS 2. Dans le `search_lambda_package.zip` fichier, modifiez-le pour mettre à jour l' Compte AWS ID et les informations du point de terminaison Elasticsearch. `lambda_search.py` Région AWS Vous pouvez obtenir le point de terminaison Elasticsearch depuis l'onglet Vue d'ensemble de la console de OpenSearch service. Il a le format`<AWS-Regi`	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	`on>.es.amazonaws.com .`	

Mettez à jour le code Lambda.	Utilisez la AWS CLI update-function-codecommande pour mettre à jour le code Lambda avec les modifications que vous avez apportées aux fichiers Python :
	`aws lambda update-function-code \ --function-name index-lambda-function \ --zip-file fileb://index_lambda_package.zip`
	`aws lambda update-function-code \ --function-name search-lambda-function \ --zip-file fileb://search_lambda_package.zip`
		Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises

Téléchargez les données brutes dans le compartiment S3.	Utilisez la commande AWS CLI cp pour télécharger les données des objets Tenant-1 et Tenant-2 dans le `tenantrawdata` compartiment (spécifiez le nom du compartiment S3 que vous avez créé à cette fin) :
	`aws s3 cp tenant-1-data s3://tenantrawdata`
	`aws s3 cp tenant-2-data s3://tenantrawdata`
	Le compartiment S3 est configuré pour exécuter la fonction d'index Lambda chaque fois que des données sont téléchargées afin que le document soit indexé dans Elasticsearch.
		Architecte cloud, administrateur cloud

Recherchez des données depuis la console Kibana.	Sur la console Kibana, exécutez la requête suivante : `GET tenant-data/_search` Cette requête affiche tous les documents indexés dans Elasticsearch. Dans ce cas, vous devriez voir deux documents distincts pour le locataire 1 et le locataire 2.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

Testez l'API de recherche depuis API Gateway.	1. Dans la console API Gateway, ouvrez l'API de recherche, choisissez la `GET` méthode dans la ressource de recherche, puis choisissez Test.
	2. Dans la fenêtre de test, fournissez la chaîne de requête suivante (en distinguant majuscules et minuscules) pour l'ID du locataire, puis choisissez Test.
	`TenantId=Tenant-1`
	La fonction Lambda envoie une requête à OpenSearch Service qui filtre le document locataire en fonction de la sécurité au niveau du document. La méthode renvoie le document qui appartient à Tenant-1.
	3. Modifiez la chaîne de requête en :
	`TenantId=Tenant-2`
	Cette requête renvoie le document qui appartient à Tenant-2.
		Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	Pour les illustrations d'écran, consultez la section Informations supplémentaires.	
Nettoyez les ressources.	Nettoyez toutes les ressources que vous avez créées pour éviter des frais supplémentaires sur votre compte.	AWS DevOps, architecte cloud, administrateur cloud

Ressources connexes

- AWS SDK for Python (Boto)
- AWS Lambda documentation
- Documentation d'API Gateway
- Documentation Amazon S3
- Documentation Amazon OpenSearch Service
  - Contrôle d'accès précis dans Amazon Service OpenSearch
  - Création d'une application de recherche avec Amazon OpenSearch Service
  - Lancement de vos domaines Amazon OpenSearch Service au sein d'un VPC

Informations supplémentaires

Modèles de partitionnement des données

Il existe trois modèles courants de partitionnement des données utilisés dans les systèmes à locataires multiples : silo, pool et hybride. Le modèle que vous choisissez dépend de la conformité, du voisinage bruyant, des opérations et des besoins d'isolation de votre environnement.

Modèle de silo

Dans le modèle de silo, les données de chaque locataire sont stockées dans une zone de stockage distincte où il n'y a aucun mélange des données des locataires. Vous pouvez utiliser deux approches pour implémenter le modèle de silo avec OpenSearch Service : domaine par locataire et index par locataire.

- Domaine par locataire : vous pouvez utiliser un domaine de OpenSearch service distinct (synonyme d'un cluster Elasticsearch) par locataire. Le fait de placer chaque locataire dans son propre domaine offre tous les avantages associés au fait de disposer de données dans une structure autonome. Cependant, cette approche pose des défis en termes de gestion et d'agilité. En raison de sa nature distribuée, il est plus difficile d'agréger et d'évaluer la santé opérationnelle et l'activité des locataires. Il s'agit d'une option coûteuse qui nécessite que chaque domaine de OpenSearch service dispose au minimum de trois nœuds principaux et de deux nœuds de données pour les charges de travail de production.

- Index par locataire : vous pouvez placer les données des locataires dans des index distincts au sein d'un cluster OpenSearch de services. Avec cette approche, vous utilisez un identifiant de locataire lorsque vous créez et nommez l'index, en ajoutant l'identifiant de locataire au nom de l'index. L'approche de l'indice par locataire vous aide à atteindre vos objectifs de silo sans introduire de cluster complètement distinct pour chaque locataire. Cependant, vous risquez de rencontrer une pression sur la mémoire si le nombre d'index augmente, car cette approche nécessite davantage de partitions et le nœud maître doit gérer davantage d'allocations et de rééquilibrage.

Isolation dans le modèle de silo : dans le modèle de silo, vous utilisez des politiques IAM pour isoler les domaines ou les index contenant les données de chaque locataire. Ces politiques empêchent un locataire d'accéder aux données d'un autre locataire. Pour implémenter votre modèle d'isolation en silo, vous pouvez créer une politique basée sur les ressources qui contrôle l'accès à vos ressources locataires. Il s'agit souvent d'une politique d'accès au domaine qui spécifie les actions qu'un principal peut effectuer sur les sous-ressources du domaine, notamment les index Elasticsearch et. APIs Avec les politiques basées sur l'identité IAM, vous pouvez spécifier des actions autorisées ou refusées sur le domaine, les index ou au sein du Service. APIs OpenSearch L'`Action`élément d'une politique IAM décrit l'action ou les actions spécifiques autorisées ou refusées par la politique, et l'`Principal` élément spécifie les comptes, utilisateurs ou rôles concernés.

L'exemple de politique suivant accorde au Tenant-1 un accès complet (tel que spécifié par`es:*`) aux sous-ressources du domaine uniquement. `tenant-1` La fin de `/*` l'`Resource`élément indique que cette politique s'applique aux sous-ressources du domaine, et non au domaine lui-même. Lorsque

cette politique est en vigueur, les locataires ne sont pas autorisés à créer un nouveau domaine ou à modifier les paramètres d'un domaine existant.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::<aws-account-id>:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/tenant-1/*"
      }
   ]
}
```

Pour implémenter le modèle de silo tenant par index, vous devez modifier cet exemple de politique afin de restreindre davantage le Tenant-1 à l'index ou aux index spécifiés, en spécifiant le nom de l'index. L'exemple de politique suivant limite Tenant-1 à l'index. `tenant-index-1`

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Tenant-1"
         },
         "Action": "es:*",
         "Resource": "arn:aws:es:<Region>:<account-id>:domain/test-domain/tenant-
index-1/*"
      }
   ]
}
```

Modèle de piscine

Dans le modèle de pool, toutes les données des locataires sont stockées dans un index au sein du même domaine. L'identifiant du locataire est inclus dans les données (document) et utilisé comme clé de partition. Vous pouvez ainsi déterminer quelles données appartiennent à quel locataire. Ce modèle réduit les frais de gestion. L'exploitation et la gestion de l'index groupé sont plus faciles

et plus efficaces que la gestion de plusieurs index. Cependant, étant donné que les données des locataires sont mélangées au sein du même index, vous perdez l'isolation naturelle des locataires que fournit le modèle de silo. Cette approche peut également dégrader les performances en raison de l'effet de voisinage bruyant.

Isolation des locataires dans le modèle de piscine — En général, l'isolation des locataires est difficile à mettre en œuvre dans le modèle de piscine. Le mécanisme IAM utilisé avec le modèle de silo ne vous permet pas de décrire l'isolation en fonction de l'ID de locataire enregistré dans votre document.

Une autre approche consiste à utiliser le support de contrôle d'accès détaillé (FGAC) fourni par Open Distro pour Elasticsearch. Le FGAC vous permet de contrôler les autorisations au niveau d'un index, d'un document ou d'un champ. À chaque demande, le FGAC évalue les informations d'identification de l'utilisateur et authentifie l'utilisateur ou refuse l'accès. Si le FGAC authentifie l'utilisateur, il récupère tous les rôles mappés à cet utilisateur et utilise l'ensemble complet des autorisations pour déterminer comment traiter la demande.

Pour obtenir l'isolation requise dans le modèle groupé, vous pouvez utiliser la sécurité au niveau du document, qui vous permet de restreindre un rôle à un sous-ensemble de documents d'un index. L'exemple de rôle suivant limite les requêtes au Tenant-1. En appliquant ce rôle au locataire 1, vous pouvez obtenir l'isolation nécessaire.

```
{
   "bool": {
     "must": {
       "match": {
         "tenantId": "Tenant-1"
       }
     }
   }
 }
```

Modèle hybride

Le modèle hybride utilise une combinaison des modèles de silo et de pool dans le même environnement pour offrir des expériences uniques à chaque niveau de locataire (tels que les niveaux gratuit, standard et premium). Chaque niveau suit le même profil de sécurité que celui utilisé dans le modèle de pool.

Isolation des locataires dans le modèle hybride — Dans le modèle hybride, vous suivez le même profil de sécurité que dans le modèle de pool, où l'utilisation du modèle de sécurité FGAC au niveau du document assurait l'isolation des locataires. Bien que cette stratégie simplifie la gestion des clusters et offre de l'agilité, elle complique d'autres aspects de l'architecture. Par exemple, votre code nécessite une complexité supplémentaire pour déterminer quel modèle est associé à chaque locataire. Vous devez également vous assurer que les requêtes à locataire unique ne saturent pas l'ensemble du domaine et ne dégradent pas l'expérience des autres locataires.

Tests dans API Gateway

Fenêtre de test pour la requête Tenant-1

Fenêtre de test pour la requête Tenant-2

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Déployez des applications à piles multiples à l'aide d'AWS CDK avec TypeScript

Créée par le Dr Rahul Sharad Gaikwad (AWS)

Récapitulatif

Ce modèle fournit une step-by-step approche pour le déploiement d'applications sur Amazon Web Services (AWS) à l'aide d'AWS Cloud Development Kit (AWS CDK) avec TypeScript. À titre d'exemple, le modèle déploie une application d'analyse en temps réel sans serveur.

Le modèle crée et déploie des applications imbriquées. La CloudFormation pile AWS parent appelle les piles enfants, ou piles imbriquées. Chaque pile enfant crée et déploie les ressources AWS définies dans la CloudFormation pile. AWS CDK Toolkit, la commande d'interface de ligne de commande (CLI)`cdk`, est l'interface principale pour les CloudFormation piles.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Cloud privé virtuel (VPC) et sous-réseaux existants
- AWS CDK Toolkit installé et configuré
- Un utilisateur doté d'autorisations d'administrateur et d'un ensemble de clés d'accès.
- Node.js
- Interface de ligne de commande AWS (AWS CLI)

Limites

- Comme AWS CDK utilise AWS CloudFormation, les applications AWS CDK sont soumises à des quotas de CloudFormation service. Pour plus d'informations, consultez la section CloudFormation Quotas AWS.

Versions du produit

Ce modèle a été créé et testé à l'aide des outils et versions suivants.

- Boîte à outils AWS CDK 1.83.0

- Node.js 14,13.0
- npm 7,0,14

Le modèle doit fonctionner avec n'importe quelle version d'AWS CDK ou de npm. Notez que les versions 13.0.0 à 13.6.0 de Node.js ne sont pas compatibles avec le CDK AWS.

Architecture

Pile technologique cible

- Console AWS Amplify
- Amazon API Gateway
- AWS CDK
- Amazon CloudFront
- Amazon Cognito
- Amazon DynamoDB
- Amazon Data Firehose
- Amazon Kinesis Data Streams
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)

Architecture cible

Le schéma suivant montre le déploiement d'applications à piles multiples à l'aide d'AWS CDK avec. TypeScript

Le schéma suivant montre l'architecture de l'exemple d'application temps réel sans serveur.

Outils

Outils

- La console AWS Amplify est le centre de contrôle pour les déploiements complets d'applications Web et mobiles dans AWS. L'hébergement Amplify Console fournit un flux de travail basé sur

Git pour héberger des applications Web sans serveur Fullstack avec un déploiement continu. L'interface utilisateur d'administration est une interface visuelle permettant aux développeurs Web et mobiles de créer et de gérer des backends d'applications en dehors de la console AWS.

- Amazon API Gateway est un service AWS permettant de créer, de publier, de gérer, de surveiller et de sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS CDK Toolkit est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre application AWS CDK. La commande `cdk` CLI est le principal outil d'interaction avec votre application AWS CDK. Il exécute votre application, interroge le modèle d'application que vous avez défini et produit et déploie les CloudFormation modèles AWS générés par le CDK AWS.
- Amazon CloudFront est un service Web qui accélère la distribution de contenus Web statiques et dynamiques, tels que les fichiers .html, .css, .js et les fichiers image. CloudFront diffuse votre contenu via un réseau mondial de centres de données appelés emplacements périphériques pour réduire la latence et améliorer les performances.
- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour vos applications Web et mobiles. Vos utilisateurs peuvent se connecter directement ou par l'intermédiaire d'un tiers.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité sans faille.
- Amazon Data Firehose est un service entièrement géré permettant de diffuser des données de streaming en temps réel vers des destinations telles qu'Amazon S3, Amazon Redshift, OpenSearch Amazon Service, Splunk et tout point de terminaison HTTP personnalisé ou appartenant à des fournisseurs de services tiers pris en charge.
- Amazon Kinesis Data Streams est un service permettant de collecter et de traiter de grands flux d'enregistrements de données en temps réel.
- AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

Le code de ce modèle est joint.

Épopées

Installer le kit d'outils AWS CDK

Tâche	Description	Compétences requises
Installez le kit d'outils AWS CDK.	Pour installer AWS CDK Toolkit dans le monde entier, exécutez la commande suivante. `npm install -g aws-cdk`	DevOps
Vérifiez la version.	Pour vérifier la version d'AWS CDK Toolkit, exécutez la commande suivante. `cdk --version`	DevOps

Configurer les informations d'identification AWS

Tâche	Description	Compétences requises

Configurez les informations d'identification.	Pour configurer les informations d'identification, exécutez la `aws configure` commande et suivez les instructions.
	`$aws configure`
	`AWS Access Key ID [None]:`
	`AWS Secret Access Key [None]: your_secret_access_key`
		DevOps

Tâche	Description	Compétences requises
	`Default region name [None]:` `Default output format [None]:`	

Téléchargez le code du projet

Tâche	Description	Compétences requises
Téléchargez le code de projet ci-joint.	Pour plus d'informations sur le répertoire et la structure des fichiers, consultez la section Informations supplémentaires.	DevOps

Démarrez l'environnement AWS CDK

Tâche	Description	Compétences requises
Démarrez l'environnement.	Pour déployer le CloudFormation modèle AWS sur le compte et la région AWS que vous souhaitez utiliser, exécutez la commande suivante. `cdk bootstrap <account>/<Region>` Pour plus d'informations, consultez la documentation AWS.	DevOps

Créez et déployez le projet

Tâche	Description	Compétences requises
Générez le projet.	Pour créer le code du projet, exécutez la `npm run build` commande.	DevOps
Déployez le projet.	Pour déployer le code du projet, exécutez la `cdk deploy` commande.	

Vérifier les sorties

Tâche	Description	Compétences requises
Vérifiez la création de la pile.	Sur la console de gestion AWS, choisissez CloudFormation. Dans les piles du projet, vérifiez qu'une pile parent et deux piles enfants ont été créées.	DevOps

Tester l'application

Tâche	Description	Compétences requises
Envoyez des données vers Kinesis Data Streams.	Configurez votre compte AWS pour envoyer des données à Kinesis Data Streams à l'aide d'Amazon Kinesis Data Generator (KDG). Pour plus d'informations, consultez Amazon Kinesis Data Generator.	DevOps

Tâche	Description	Compétences requises
Créez un utilisateur Amazon Cognito.	Pour créer un utilisateur Amazon Cognito, téléchargez le modèle cognito-setup.json depuis la section Créer un utilisateur Amazon Cognito sur CloudFormation la page d'aide de Kinesis Data Generator. Lancez le modèle, puis entrez votre nom d'utilisateur et votre mot de passe Amazon Cognito. L'onglet Sorties répertori e l'URL du Kinesis Data Generator.	DevOps
Connectez-vous à Kinesis Data Generator	Pour vous connecter à KDG, utilisez les informati ons d'identification Amazon Cognito que vous avez fournies et l'URL du générateu r de données Kinesis.	DevOps
Testez l'application.	Dans KDG, dans Modèle d'enregistrement, Modèle 1, collez le code de test dans la section Informati ons supplémentaires, puis choisissez Envoyer des données.	DevOps
Testez API Gateway.	Une fois les données ingérées, testez API Gateway en utilisant la `GET` méthode de récupération des données.	DevOps

Ressources connexes

Références

- Kit de développement AWS Cloud
- AWS CDK activé GitHub
- Utilisation de piles imbriquées
- Exemple d'exemple AWS : analyse en temps réel sans serveur

Informations supplémentaires

Détails du répertoire et du fichier

Ce modèle définit les trois piles suivantes.

- `parent-cdk-stack.ts`— Cette pile agit en tant que pile parent et appelle les deux applications enfants en tant que piles imbriquées.
- `real-time-analytics-poc-stack.ts`— Cette pile imbriquée contient l'infrastructure et le code de l'application.
- `real-time-analytics-web-stack.ts`— Cette pile imbriquée contient uniquement le code statique de l'application Web.

Les fichiers importants et leurs fonctionnalités

- `bin/real-time-analytics-poc.ts`— Point d'entrée de l'application AWS CDK. Il charge toutes les piles définies `lib/` ci-dessous.
- `lib/real-time-analytics-poc-stack.ts`— Définition de la pile de l'application AWS CDK (`real-time-analytics-poc`).
- `lib/real-time-analytics-web-stack.ts`— Définition de la pile de l'application AWS CDK (`real-time-analytics-web-stack`).
- `lib/parent-cdk-stack.ts`— Définition de la pile de l'application AWS CDK (`parent-cdk`).
- `package.json`— le manifeste du module npm, qui inclut le nom, la version et les dépendances de l'application.
- `package-lock.json`— Maintenu par npm.
- `cdk.json`— Boîte à outils pour exécuter l'application.

- `tsconfig.json`— La TypeScript configuration du projet.
- `.gitignore`— Liste des fichiers que Git doit exclure du contrôle de source.
- `node_modules`— Maintenu par npm ; inclut les dépendances du projet.

La section de code suivante de la pile parent appelle les applications enfants sous la forme de piles AWS CDK imbriquées.

```
import * as cdk from '@aws-cdk/core';
import { Construct, Stack, StackProps } from '@aws-cdk/core';
import { RealTimeAnalyticsPocStack } from './real-time-analytics-poc-stack';
import { RealTimeAnalyticsWebStack } from './real-time-analytics-web-stack';


export class CdkParentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, props);


    new RealTimeAnalyticsPocStack(this, 'RealTimeAnalyticsPocStack');
    new RealTimeAnalyticsWebStack(this, 'RealTimeAnalyticsWebStack');
  }
}
```

Code pour les tests

```
session={{date.now('YYYYMMDD')}}|sequence={{date.now('x')}}|
reception={{date.now('x')}}|instrument={{random.number(9)}}|
l={{random.number(20)}}|price_0={{random.number({"min":10000,
 "max":30000})}}|price_1={{random.number({"min":10000, "max":30000})}}|
price_2={{random.number({"min":10000, "max":30000})}}|
price_3={{random.number({"min":10000, "max":30000})}}|
price_4={{random.number({"min":10000, "max":30000})}}|
price_5={{random.number({"min":10000, "max":30000})}}|
price_6={{random.number({"min":10000, "max":30000})}}|
price_7={{random.number({"min":10000, "max":30000})}}|
price_8={{random.number({"min":10000, "max":30000})}}|
```

Test de l'API Gateway

Sur la console API Gateway, testez API Gateway à l'aide de la `GET` méthode.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Automatisez le déploiement d'applications imbriquées à l'aide d'AWS SAM

Créée par le Dr Rahul Sharad Gaikwad (AWS), Dmitry Gulin (AWS), Ishwar Chauthaiwale (AWS) et Tabby Ward (AWS)

Récapitulatif

Sur Amazon Web Services (AWS), AWS Serverless Application Model (AWS SAM) est un framework open source qui fournit une syntaxe abrégée pour exprimer les fonctions APIs, les bases de données et les mappages de sources d'événements. Avec seulement quelques lignes pour chaque ressource, vous pouvez définir l'application que vous souhaitez et la modéliser à l'aide de YAML. Au cours du déploiement, SAM transforme et étend la syntaxe SAM en CloudFormation syntaxe AWS, que vous pouvez utiliser pour créer des applications sans serveur plus rapidement.

AWS SAM simplifie le développement, le déploiement et la gestion des applications sans serveur sur la plateforme AWS. Il fournit un cadre standardisé, un déploiement plus rapide, des capacités de test locales, une gestion des ressources, une intégration fluide avec les outils de développement et une communauté de soutien. Ces fonctionnalités en font un outil précieux pour créer des applications sans serveur de manière efficace.

Ce modèle utilise des modèles AWS SAM pour automatiser le déploiement d'applications imbriquées. Une application imbriquée est une application intégrée à une autre application. Les applications pour parents sont appelées applications pour enfants. Il s'agit de composants faiblement couplés d'une architecture sans serveur.

À l'aide d'applications imbriquées, vous pouvez créer rapidement des architectures sans serveur très sophistiquées en réutilisant des services ou des composants créés et gérés de manière indépendante, mais composés à l'aide d'AWS SAM et du Serverless Application Repository. Les applications imbriquées vous aident à créer des applications plus puissantes, à éviter les doublons et à garantir la cohérence et les meilleures pratiques au sein de vos équipes et organisations. Pour illustrer les applications imbriquées, le modèle déploie un exemple d'application de panier d'achat sans serveur AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cloud privé virtuel (VPC) et des sous-réseaux existants

- Un environnement de développement intégré tel que Visual Studio Code (pour plus d'informations, voir Outils pour créer sur AWS)
- bibliothèque Python Wheel installée à l'aide de pip install wheel, si elle n'est pas déjà installée

Limites

- Le nombre maximal d'applications pouvant être imbriquées dans une application sans serveur est de 200.
- Le nombre maximum de paramètres pour une application imbriquée peut être de 60.

Versions du produit

- Cette solution repose sur l'interface de ligne de commande AWS SAM (AWS SAM CLI) version 1.21.1, mais cette architecture devrait fonctionner avec les versions ultérieures de l'interface de ligne de commande AWS SAM.

Architecture

Pile technologique cible

- Amazon API Gateway
- AWS SAM
- Amazon Cognito
- Amazon DynamoDB
- AWS Lambda
- File d'attente Amazon Simple Queue Service (Amazon SQS)

Architecture cible

Le schéma suivant montre comment les demandes des utilisateurs sont adressées aux services d'achat en appelant APIs. La demande de l'utilisateur, y compris toutes les informations nécessaires, est envoyée à Amazon API Gateway et à l'autorisateur Amazon Cognito, qui met en œuvre les mécanismes d'authentification et d'autorisation pour le. APIs

Lorsqu'un élément est ajouté, supprimé ou mis à jour dans DynamoDB, un événement est placé dans DynamoDB Streams, qui à son tour lance une fonction Lambda. Pour éviter la suppression immédiate

d'anciens éléments dans le cadre d'un flux de travail synchrone, les messages sont placés dans une file d'attente SQS, qui lance une fonction de travail pour supprimer les messages.

Dans cette configuration de solution, l'interface de ligne de commande AWS SAM sert d'interface pour les CloudFormation piles AWS. Les modèles AWS SAM déploient automatiquement des applications imbriquées. Le modèle SAM parent appelle les modèles enfants, et la CloudFormation pile parent déploie les piles enfants. Chaque pile enfant crée les ressources AWS définies dans les CloudFormation modèles AWS SAM.

1. Construisez et déployez les piles.
2. La CloudFormation pile Auth contient Amazon Cognito.
3. La CloudFormation pile de produits contient une fonction Lambda et Amazon API Gateway
4. La CloudFormation pile Shopping contient une fonction Lambda, Amazon API Gateway, la file d'attente SQS et la base de données Amazon DynamoDB.

Outils

Outils

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour les applications Web et mobiles.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Serverless Application Model (AWS SAM) est un framework open source qui vous aide à créer des applications sans serveur dans le cloud AWS.

- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

Code

Le code de ce modèle est disponible dans le référentiel d'échantillons GitHub AWS SAM Nested Stack.

Épopées

Installation de l'interface de ligne de commande AWS SAM

Tâche	Description	Compétences requises
Installez l'interface de ligne de commande AWS SAM.	Pour installer l'interface de ligne de commande AWS SAM, consultez les instructions de la documentation AWS SAM.	DevOps ingénieur

Configurez les informations d'identification AWS.	Pour définir les informations d'identification AWS afin que l'interface de ligne de commande AWS SAM puisse appeler les services AWS en votre nom, exécutez la `aws configure` commande et suivez les instructions.
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: your_secret_access_key`
	`Default region name [None]:`
		DevOps ingénieur

Tâche	Description	Compétences requises
	`Default output format [None]:` Pour plus d'informations sur la configuration de vos informations d'identification, consultez Authentification et informations d'accès.	

Initialisation du projet AWS SAM

Tâche	Description	Compétences requises

Clonez le référentiel de code AWS SAM.	1. Clonez le référentiel d'échantillons aws sam nested stack pour ce modèle en saisissant la commande suivante.
	
	`git clone https://github.com/aws-samples/aws-sam-nested-stack-sample.git`
	
	2. Accédez au répertoire cloné en saisissant la commande suivante.
	
	`cd aws-sam-nested-stack-sample`
		DevOps ingénieur

Déployez des modèles pour initialiser le projet.	Pour initialiser le projet, exécutez la `SAM init` commande. Lorsque vous êtes invité à choisir une source de	DevOps ingénieur

Tâche	Description	Compétences requises
	modèle, choisissez`Custom Template Location`.	

Compiler et créer le code du modèle SAM

Tâche	Description	Compétences requises
Consultez les modèles d'applications AWS SAM.	Passez en revue les modèles pour les applications imbriquées. Cet exemple utilise les modèles d'application imbriqués suivants : • `auth.yaml` — Ce modèle configure les ressources liées à l'authentification, telles qu'Amazon Cognito et AWS Systems Manager Parameter Store. • `product-mock.yaml` — Ce modèle déploie des ressources liées au produit, telles que les fonctions Lambda et Amazon API Gateway. • `shoppingcart-service.yaml` — Ce modèle configure les ressources liées au panier d'achat, telles que AWS Identity and Access Management (IAM), les tables DynamoDB et les fonctions Lambda.	DevOps ingénieur

Tâche	Description	Compétences requises
Passez en revue le modèle parent.	Passez en revue le modèle qui invoquera les modèles d'applications imbriqués. Dans cet exemple, le modèle parent est`template.yml` . Toutes les applications distinctes sont imbriquées dans le modèle `template.yml` parent unique.	DevOps ingénieur
Compilez et générez le code du modèle AWS SAM.	À l'aide de l'interface de ligne de commande AWS SAM, exécutez la commande suivante. `sam build`	DevOps ingénieur

Déployer le modèle AWS SAM

Tâche	Description	Compétences requises
Déployez les applications.	Pour lancer le modèle de code SAM qui crée les CloudForm ation piles d'applications imbriquées et déploie le code dans l'environnement AWS, exécutez la commande suivante. `sam deploy --guided -- stack-name shopping- cart-nested-stack -- capabilities CAPABILIT`	DevOps ingénieur

Tâche	Description	Compétences requises
	`Y_IAM CAPABILIT Y_AUTO_EXPAND` La commande posera quelques questions. Répondez à toutes les questions avecy.	

Vérification du déploiement

Tâche	Description	Compétences requises
Vérifiez les piles.	Pour consulter les CloudForm ation piles AWS et les ressources AWS définies dans les modèles AWS SAM, procédez comme suit : 1. Connectez-vous à la console de gestion AWS, puis accédez à la CloudFormationconsole. 2. Vérifiez que les piles pour parents et enfants sont répertoriées. Dans cet exemple, `sam-shopping-cart` il s'agit de la pile parent qui appelle les piles Auth, Product et Shopping imbriquées. La pile de produits fournit le lien URL de l'API Gateway du produit en sortie.	DevOps ingénieur

Ressources connexes

Références

- Modèle d'application sans serveur AWS (AWS SAM)
- AWS SAM activé GitHub
- Microservice de panier d'achat sans serveur (exemple d'application AWS)

Tutoriels et vidéos

- Créez une application sans serveur
- Discussions techniques en ligne sur AWS : création et déploiement d'applications sans serveur avec AWS SAM

Informations supplémentaires

Une fois que tout le code est en place, l'exemple présente la structure de répertoire suivante :

- sam_stacks — Ce dossier contient la couche. `shared.py` Une couche est une archive de fichiers contenant des bibliothèques, un environnement d'exécution personnalisé ou d'autres dépendances. Avec les couches, vous pouvez utiliser des bibliothèques dans votre fonction sans avoir à les inclure dans un package de déploiement.
- product-mock-service— Ce dossier contient toutes les fonctions et tous les fichiers Lambda relatifs au produit.
- shopping-cart-service— Ce dossier contient toutes les fonctions et tous les fichiers Lambda liés au shopping.

Implémentez l'isolation des locataires SaaS pour Amazon S3 à l'aide d'un distributeur automatique de jetons AWS Lambda

Créée par Tabby Ward (AWS), Sravan Periyathambi (AWS) et Thomas Davis (AWS)

Récapitulatif

Les applications SaaS mutualisées doivent mettre en œuvre des systèmes garantissant le maintien de l'isolement des locataires. Lorsque vous stockez des données de locataires sur la même ressource Amazon Web Services (AWS), par exemple lorsque plusieurs locataires stockent des données dans le même compartiment Amazon Simple Storage Service (Amazon S3), vous devez vous assurer qu'aucun accès entre locataires ne peut avoir lieu. Les distributeurs automatiques de jetons (TVMs) constituent un moyen d'isoler les données des locataires. Ces machines fournissent un mécanisme permettant d'obtenir des jetons tout en faisant abstraction de la complexité de la façon dont ces jetons sont générés. Les développeurs peuvent utiliser un TVM sans avoir une connaissance détaillée de la façon dont il produit des jetons.

Ce modèle implémente un TVM à l'aide d'AWS Lambda. Le TVM génère un jeton composé d'informations d'identification temporaires du service de jeton de sécurité (STS) qui limitent l'accès aux données d'un seul locataire SaaS dans un compartiment S3.

TVMs, et le code fourni avec ce modèle, sont généralement utilisés avec des revendications dérivées de JSON Web Tokens (JWTs) pour associer les demandes de ressources AWS à une politique AWS Identity and Access Management (IAM) limitée au locataire. Vous pouvez utiliser le code de ce modèle comme base pour implémenter une application SaaS qui génère des informations d'identification STS temporaires et étendues sur la base des revendications fournies dans un jeton JWT.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI) version 1.19.0 ou ultérieure, installée et configurée sur macOS, Linux ou Windows. Vous pouvez également utiliser la version 2.1 ou ultérieure de l'interface de ligne de commande AWS.

Limites

- Ce code fonctionne en Java et ne prend actuellement pas en charge les autres langages de programmation.
- L'exemple d'application n'inclut pas la prise en charge interrégionale ou de reprise après sinistre (DR) d'AWS.
- Ce modèle montre comment un Lambda TVM pour une application SaaS peut fournir un accès étendu aux locataires. Il n'est pas destiné à être utilisé dans des environnements de production.

Architecture

Pile technologique cible

- AWS Lambda
- Amazon S3
- IAM
- AWS Security Token Service (AWS STS)

Architecture cible

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Security Token Service (AWS STS) vous aide à demander des informations d'identification temporaires à privilèges limités pour les utilisateurs.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

Le code source de ce modèle est disponible sous forme de pièce jointe et inclut les fichiers suivants :

- `s3UploadSample.jar`fournit le code source d'une fonction Lambda qui télécharge un document JSON dans un compartiment S3.
- `tvm-layer.zip`fournit une bibliothèque Java réutilisable qui fournit un jeton (informations d'identification temporaires STS) permettant à la fonction Lambda d'accéder au compartiment S3 et de télécharger le document JSON.
- `token-vending-machine-sample-app.zip`fournit le code source utilisé pour créer ces artefacts et les instructions de compilation.

Pour utiliser ces fichiers, suivez les instructions de la section suivante.

Épopées

Déterminer les valeurs des variables

Tâche	Description	Compétences requises
Déterminez les valeurs des variables.	L'implémentation de ce modèle inclut plusieurs noms de variables qui doivent être utilisés de manière cohérente . Déterminez les valeurs qui doivent être utilisées pour chaque variable et fournisse z cette valeur lorsque cela est demandé lors des étapes suivantes. – <AWS Account ID>L'iden tifiant de compte à 12 chiffres associé au compte AWS dans	Administrateur du cloud

Tâche	Description	Compétences requises
	lequel vous implémentez ce modèle. Pour savoir comment trouver votre identifiant de compte AWS, consultez Votre identifiant de compte AWS et son alias dans la documentation IAM. – <AWS Region>La région AWS dans laquelle vous implémentez ce modèle. Pour plus d'informations sur les régions AWS, consultez Régions et zones de disponibilité sur le site Web d'AWS. < sample-tenant-name > – Le nom du locataire à utiliser dans l'application. Pour des raisons de simplicité, nous vous recommandons de n'utiliser que des caractères alphanumériques dans cette valeur, mais vous pouvez utiliser n'importe quel nom valide pour une clé d'objet S3. < sample-tvm-role-name > – Nom du rôle IAM associé à la fonction Lambda qui exécute le TVM et un exemple d'application. Le nom du rôle est une chaîne composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez	

Tâche	Description	Compétences requises
	également inclure l'un des caractères suivants : trait de soulignement (_), signe plus (+), signe égal (=), virgule (,), point (.), signe arobase (@) et tiret (-). Le nom du rôle doit être unique dans le compte. **<** sample-app-role-name **>** – Nom du rôle IAM assumé par la fonction Lambda lorsqu'el le génère des informati ons d'identification STS temporaires et étendues. Le nom du rôle est une chaîne composée de caractères alphanumériques majuscules et minuscules sans espaces. Vous pouvez également inclure l'un des caractères suivants : trait de soulignem ent (_), signe plus (+), signe égal (=), virgule (,), point (.), signe arobase (@) et tiret (-). Le nom du rôle doit être unique dans le compte. **<** sample-app-function-name **>** – Nom de la fonction Lambda. Il s'agit d'une chaîne d'une longueur maximale de 64 caractères. **<** sample-app-bucket-name **>** – Le nom d'un compartiment S3 auquel il faut accéder avec	

Tâche	Description	Compétences requises
	des autorisations délimitées à un locataire spécifique. Noms des compartiments S3 : • Ils doivent comporter entre 3 et 63 caractères. • Doit être composé uniquement de lettres minuscules, de chiffres, de points (.) et de tirets (-). • Doit commencer et se terminer par une lettre ou un chiffre. • Ils ne doivent pas être formatés en tant qu'adresse IP (par exemple, 192.168.5 .4). • Doit être unique au sein d'une partition. Une partition est un groupement de régions. AWS possède actuellement trois partition s : `aws` (régions standard) , `aws-cn` (régions de Chine) et `aws-us-gov` (régions AWS GovCloud [États-Un is]).	

Création d’un compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3 pour l'exemple d'application.	Utilisez la commande AWS CLI suivante pour créer un	Administrateur du cloud

Tâche	Description	Compétences requises
	compartiment S3. Entrez la valeur **<** sample-app-bucket-name **>** dans l'extrait de code : `aws s3api create-bucket --bucket <sample-app-bucket-name>` L'exemple d'application Lambda télécharge des fichiers JSON dans ce compartiment.	

Création du rôle et de la politique IAM TVM

Tâche	Description	Compétences requises
Créez un rôle TVM.	Utilisez l'une des commandes de l'AWS CLI suivantes pour créer un rôle IAM. Entrez la valeur **<** sample-tvm-role-name **>** dans la commande. Pour les shells macOS ou Linux : `aws iam create-role \ --role-name <sample-tvm-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow",`	Administrateur du cloud

Tâche	Description	Compétences requises

	<pre>"Principa
	l": {
	
	"Service": "lambda.a
	mazonaws.com"
	},
	"Action":
	"sts:AssumeRole"
	}
	]}'</pre>
	Pour la ligne de commande Windows :
	<pre>aws iam create-role ^
	--role-name <sample-t
	vm-role-name> ^
	--assume-role-policy-
	document "{\"Versi
	on\": \"2012-10
	-17\", \"Statement
	\": [{\"Effect\":
	\"Allow\", \"Princip
	al\": {\"Service\":
	\"lambda.amazonaws
	.com\"}, \"Action\":
	\"sts:AssumeRole\"
	}]}"</pre>
	L'exemple d'application Lambda assume ce rôle lorsqu'elle est invoquée. La possibilité d'assumer le rôle d'application avec une politique étendue donne au code des autorisations plus étendues pour accéder au compartiment S3.	

Tâche	Description	Compétences requises

Créez une politique de rôle TVM intégrée.	Utilisez l'une des commandes de l'AWS CLI suivantes pour créer une politique IAM. Entrez les **<**AWS Account ID**>**valeurs **<** sample-tvm-role-name **>**, et **<** sample-app-role-name **>** dans la commande.
	
	Pour les shells macOS ou Linux :
	
	`aws iam put-role-policy \ --role-name <sample-tvm-role-name> \ --policy-name assume-app-role \ --policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "sts:AssumeRole", "Resource": "arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>" } ]}'`
	
	Pour la ligne de commande Windows :
	
	`aws iam put-role-policy ^`
		Administrateur du cloud

Tâche	Description	Compétences requises
	`--role-name <sample-tvm-role-name> ^ --policy-name assume-app-role ^ --policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Resource\": \"arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>\"}]}"` Cette politique est liée au rôle TVM. Cela donne au code la capacité d'assumer le rôle d'application, qui dispose d'autorisations plus larges pour accéder au compartiment S3.	

Tâche	Description	Compétences requises

Joignez la politique Lambda gérée.	Utilisez la commande AWS CLI suivante pour joindre la politique `AWSLambda BasicExecutionRole` IAM. Entrez la valeur **<** sample-tvm-role-name **>** dans la commande :
	`aws iam attach-role-policy \ --role-name <sample-tvm-role-name> \ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Pour la ligne de commande Windows :
	`aws iam attach-role-policy ^ --role-name <sample-tvm-role-name> ^ --policy-arn arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole`
	Cette politique gérée est associée au rôle TVM pour permettre à Lambda d'envoyer des journaux à Amazon. CloudWatch
		Administrateur du cloud

Création du rôle et de la politique de l'application IAM

Tâche	Description	Compétences requises
Créez le rôle d'application.	Utilisez l'une des commandes de l'AWS CLI suivantes pour créer un rôle IAM. Entrez les <AWS Account ID>valeurs < sample-app-role-name >, et < sample-tvm-role-name > dans la commande. Pour les shells macOS ou Linux : `aws iam create-role \ --role-name <sample-app-role-name> \ --assume-role-policy-document '{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>" }, "Action": "sts:AssumeRole" } ]}'` Pour la ligne de commande Windows :	Administrateur du cloud

Tâche	Description	Compétences requises
	`aws iam create-role ^ --role-name <sample-app-role-name> ^ --assume-role-policy-document "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\",\"Principal\": {\"AWS\": \"arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name>\"},\"Action\": \"sts:AssumeRole\" }]}"` L'exemple d'application Lambda assume ce rôle avec une politique définie pour obtenir un accès basé sur le locataire à un compartiment S3.	

Tâche	Description	Compétences requises
Créez une politique de rôle d'application en ligne.	Utilisez l'une des commandes de l'AWS CLI suivantes pour créer une politique IAM. Entrez les valeurs **<** sample-app-role-name **>** et **<** sample-app-bucket-name **>** dans la commande. Pour les shells macOS ou Linux : `aws iam put-role-policy \ --role-name <sample-app-role-name> \ --policy-name s3-bucket-access \ --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"], "Resource": "arn:aws:s3:::<sample-app-bucket-name>/*" }, { "Effect": "Allow",`	Administrateur du cloud

Tâche	Description	Compétences requises

	<pre>"Action":
	["s3:ListBucket"],
	"Resource
	": "arn:aws:s3:::<sam
	ple-app-bucket-name>"
	}
	]}'</pre>
	Pour la ligne de commande Windows :
	<pre>aws iam put-role-policy
	^
	--role-name <sample-a
	pp-role-name> ^
	--policy-name s3-bucket
	-access ^
	--policy-documen
	t "{\"Version\":
	\"2012-10-17\",
	\"Statement\":
	[{\"Effect\": \"Allow
	\", \"Action\":
	[\"s3:PutObject\",
	\"s3:GetObject\",
	\"s3:DeleteObject\
	"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-na
	me>/*\"}, {\"Effect\":
	\"Allow\", \"Action\
	": [\"s3:ListBucket
	\"], \"Resource\":
	\"arn:aws:s3:::<sa
	mple-app-bucket-name>
	\"}]}"</pre>
	Cette politique est associée au rôle d'application. Il fournit un accès étendu aux objets	

Tâche	Description	Compétences requises
	du compartiment S3. Lorsque l'exemple d'application assume le rôle, ces autorisations sont étendues à un locataire spécifique avec la politique générée dynamiquement par le TVM.	

Création de l'exemple d'application Lambda avec TVM

Tâche	Description	Compétences requises
Téléchargez les fichiers source compilés.	Téléchargez les `tvm-layer.zip` fichiers `s3UploadSample.jar` et, qui sont inclus sous forme de pièces jointes. Le code source utilisé pour créer ces artefacts et les instructions de compilation sont fournis dans. `token-vending-machine-sample-app.zip`	Administrateur du cloud
Créez la couche Lambda.	Utilisez la commande AWS CLI suivante pour créer une couche Lambda, qui rend le TVM accessible à Lambda. **Note** Si vous n'exécutez pas cette commande depuis l'emplacement où vous l'avez téléchargée `tvm-`	Administrateur cloud, développeur d'applications

Tâche	Description	Compétences requises

	`layer.zip` , indiquez le chemin d'accès correct `tvm-layer.zip` dans le `--zip-file` paramètre.
	
	`aws lambda publish-layer-version \ --layer-name sample-token-vending-machine \ --compatible-runtimes java11 \ --zip-file fileb://tvm-layer.zip`
	
	Pour la ligne de commande Windows :
	
	`aws lambda publish-layer-version ^ --layer-name sample-token-vending-machine ^ --compatible-runtimes java11 ^ --zip-file fileb://tvm-layer.zip`
	
	Cette commande crée une couche Lambda qui contient la bibliothèque TVM réutilisable.	

Tâche	Description	Compétences requises

Créez la fonction Lambda.	Utilisez la commande AWS CLI suivante pour créer une fonction Lambda. Indiquez les <AWS Account ID><AWS Region>valeurs < sample-app-function-name >,, < sample-tvm-role-name >, < sample-app-bucket-name > et < sample-app-role-name > dans la commande.
	
	Note
	Si vous n'exécutez pas cette commande depuis l'emplacement où vous l'avez téléchargées `s3UploadSample.jar`, indiquez le chemin d'accès correct `s3UploadSample.jar` dans le `--zip-file` paramètre.
	
	`aws lambda create-function \`
	`--function-name <sample-app-function-name> \`
	`--timeout 30 \`
	`--memory-size 256 \`
	`--runtime java11 \`
		Administrateur cloud, développeur d'applications

Tâche	Description	Compétences requises

	`--role arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name> \`
	`--handler com.amazon.aws.s3UploadSample.App \`
	`--zip-file fileb://s3UploadSample.jar \`
	`--layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 \`
	`--environment "Variables={S3_BUCKET=<sample-app-bucket-name>, ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}"`
	
	Pour la ligne de commande Windows :
	
	`aws lambda create-function ^`
	`--function-name <sample-app-function-name> ^`
	`--timeout 30 ^`
	`--memory-size 256 ^`
	`--runtime java11 ^`
	`--role arn:aws:iam::<AWS Account ID>:role/<sample-tvm-role-name> ^`
	`--handler com.amazon.aws.s3UploadSample.App ^`	

Tâche	Description	Compétences requises
	`--zip-file fileb://s3UploadSample.jar ^ --layers arn:aws:lambda:<AWS Region>:<AWS Account ID>:layer:sample-token-vending-machine:1 ^ --environment "Variables={S3_BUCKET=<sample-app-bucket-name>,ROLE=arn:aws:iam::<AWS Account ID>:role/<sample-app-role-name>}"` Cette commande crée une fonction Lambda avec l'exemple de code d'application et la couche TVM attachés. Il définit également deux variables d'environnement : `S3_BUCKET` et`ROLE`. L'exemple d'application utilise ces variables pour déterminer le rôle à assumer et le compartiment S3 dans lequel télécharger les documents JSON.	

Testez l'exemple d'application et le TVM

Tâche	Description	Compétences requises
Appelez l'exemple d'application Lambda.	Utilisez l'une des commandes de l'AWS CLI suivantes pour démarrer l'exemple d'applica	Administrateur cloud, développeur d'applications

Tâche	Description	Compétences requises

	tion Lambda avec la charge utile attendue. Entrez les valeurs **<** sample-app-function-name **>** et **<** sample-tenant-name **>** dans la commande.
	
	Pour les shells macOS et Linux :
	
	`aws lambda invoke \ --function <sample-app-function-name> \ --invocation-type RequestResponse \ --payload '{"tenant": "<sample-tenant-name>"}' \ --cli-binary-format raw-in-base64-out response.json`
	
	Pour la ligne de commande Windows :
	
	`aws lambda invoke ^ --function <sample-app-function-name> ^ --invocation-type RequestResponse ^ --payload "{\"tenant\": \"<sample-tenant-name>\"}" ^ --cli-binary-format raw-in-base64-out response.json`
	
	Cette commande appelle la fonction Lambda et renvoie le	

Tâche	Description	Compétences requises
	résultat dans un `response.json` document. Sur de nombreux systèmes basés sur Unix, vous pouvez passer `response.json /dev/stdout` à pour afficher les résultats directement dans votre shell sans créer un autre fichier. **Note** La modification de la valeur **<** sample-tenant-name **>** lors des appels ultérieurs de cette fonction Lambda modifie l'emplacement du document JSON et les autorisations fournies par le jeton.	

Tâche	Description	Compétences requises
Consultez le compartiment S3 pour voir les objets créés.	Accédez au compartiment S3 (< sample-app-bucket-name >) que vous avez créé précédemment. Ce compartiment contient un préfixe d'objet S3 dont la valeur est < sample-tenant-name >. Sous ce préfixe, vous trouverez un document JSON nommé avec un UUID. Le fait d'invoquer plusieurs fois l'exemple d'application permet d'ajouter d'autres documents JSON.	Administrateur du cloud

Tâche	Description	Compétences requises
Consultez les journaux Cloudwatch de l'exemple d'application.	Consultez les journaux Cloudwatch associés à la fonction Lambda nommée sample-app-function-name < >. Pour obtenir des instructions, consultez la section Accès aux CloudWatch journaux Amazon pour AWS Lambda dans la documentation AWS Lambda. Vous pouvez consulter la politique définie par le locataire générée par le TVM dans ces journaux. Cette politique limitée au locataire donne des autorisations pour l'exemple d'application à Amazon S3 PutObject,,, et GetObject DeleteObjectListBucket APIs, mais uniquement pour le préfixe d'objet associé à < >. sample-tenant-name Lors des appels ultérieurs de l'exemple d'application, si vous modifiez le < sample-tenant-name >, le TVM met à jour la politique étendue pour qu'elle corresponde au locataire fourni dans la charge utile d'invocation. Cette politique générée dynamiquement montre comment l'accès limité au locataire peut être	Administrateur du cloud

Tâche	Description	Compétences requises
	maintenu avec un TVM dans les applications SaaS. La fonctionnalité TVM est fournie dans une couche Lambda afin qu'elle puisse être associée à d'autres fonctions Lambda utilisées par une application sans avoir à répliquer le code. Pour une illustration de la politique générée dynamique ment, consultez la section Informations supplémentaires.	

Ressources connexes

- Isolation des locataires grâce à des politiques IAM générées dynamiquement (article de blog)
- Appliquer des politiques d'isolation générées dynamiquement dans un environnement SaaS (article de blog)
- AWS SaaS Boost (environnement de référence open source qui vous aide à transférer votre offre SaaS vers AWS)

Informations supplémentaires

Le journal Amazon Cloudwatch suivant montre la politique générée dynamiquement par le code TVM selon ce modèle. Dans cette capture d'écran, le < sample-app-bucket-name > est `DOC-EXAMPLE-BUCKET` et le < sample-tenant-name > est`test-tenant-1`. Les informations d'identification STS renvoyées par cette politique étendue ne peuvent effectuer aucune action sur les objets du compartiment S3, à l'exception des objets associés au préfixe de clé `test-tenant-1` d'objet.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Implémentez le modèle de saga sans serveur à l'aide d'AWS Step Functions

Créée par Tabby Ward (AWS), Joe Kern (AWS) et Rohan Mehta (AWS)

Récapitulatif

Dans une architecture de microservices, l'objectif principal est de créer des composants découplés et indépendants afin de promouvoir l'agilité, la flexibilité et d'accélérer la mise sur le marché de vos applications. Grâce au découplage, chaque composant de microservice possède sa propre couche de persistance des données. Dans une architecture distribuée, les transactions commerciales peuvent couvrir plusieurs microservices. Comme ces microservices ne peuvent pas utiliser une seule transaction ACID (atomicité, cohérence, isolation, durabilité), vous risquez de vous retrouver avec des transactions partielles. Dans ce cas, une certaine logique de contrôle est nécessaire pour annuler les transactions déjà traitées. Le modèle de saga distribué est généralement utilisé à cette fin.

Le modèle saga est un modèle de gestion des défaillances qui permet d'établir la cohérence dans les applications distribuées et de coordonner les transactions entre plusieurs microservices afin de maintenir la cohérence des données. Lorsque vous utilisez le modèle saga, chaque service qui effectue une transaction publie un événement qui déclenche les services suivants pour effectuer la transaction suivante de la chaîne. Cela continue jusqu'à ce que la dernière transaction de la chaîne soit terminée. Si une transaction commerciale échoue, Saga orchestre une série de transactions compensatoires qui annulent les modifications apportées par les transactions précédentes.

Ce modèle montre comment automatiser la configuration et le déploiement d'un exemple d'application (qui gère les réservations de voyages) à l'aide de technologies sans serveur telles qu'AWS Step Functions, AWS Lambda et Amazon DynamoDB. L'exemple d'application utilise également Amazon API Gateway et Amazon Simple Notification Service (Amazon SNS) pour implémenter un coordinateur d'exécution de saga. Le modèle peut être déployé avec un framework d'infrastructure en tant que code (IaC) tel que l'AWS Cloud Development Kit (AWS CDK), l'AWS Serverless Application Model (AWS Serverless Application Model) (AWS SAM) ou Terraform.

Pour plus d'informations sur le modèle saga et les autres modèles de persistance des données, consultez le guide Enabling data persistence in microservices sur le site Web AWS Prescriptive Guidance.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Autorisations pour créer une CloudFormation pile AWS. Pour plus d'informations, consultez la section Contrôle de l'accès dans la CloudFormation documentation.
- Framework IaC de votre choix (AWS CDK, AWS SAM ou Terraform) configuré avec votre compte AWS afin que vous puissiez utiliser la CLI du framework pour déployer l'application.
- NodeJS, utilisé pour créer l'application et l'exécuter localement.
- Un éditeur de code de votre choix (tel que Visual Studio Code, Sublime ou Atom).

Versions du produit

- NodeJS version 14
- Version 2.37.1 du kit de développement logiciel AWS
- Version 1.71.0 d'AWS SAM
- Terraform version 1.3.7

Limites

Le sourcing d'événements est un moyen naturel d'implémenter le modèle d'orchestration de la saga dans une architecture de microservices où tous les composants sont faiblement couplés et ne se connaissent pas directement les uns les autres. Si votre transaction comporte un petit nombre d'étapes (trois à cinq), le modèle de la saga pourrait convenir parfaitement. Cependant, la complexité augmente avec le nombre de microservices et le nombre d'étapes.

Les tests et le débogage peuvent devenir difficiles lorsque vous utilisez cette conception, car tous les services doivent être exécutés pour simuler le modèle de transaction.

Architecture

Architecture cible

L'architecture proposée utilise AWS Step Functions pour créer un modèle de saga permettant de réserver des vols, de réserver des locations de voitures et de traiter les paiements pour les vacances.

Le schéma de flux de travail suivant illustre le flux typique du système de réservation de voyages. Le flux de travail consiste à réserver un voyage en avion (« ReserveFlight »), à réserver une voiture (« ReserveCarRental »), à traiter les paiements (« ProcessPayment »), à confirmer les réservations de vol (« ConfirmFlight ») et à confirmer la location de voiture (« ConfirmCarRental »), suivis d'une

notification de réussite lorsque ces étapes sont terminées. Cependant, si le système rencontre des erreurs lors de l'exécution de l'une de ces transactions, il commence à échouer en arrière. Par exemple, une erreur dans le traitement du paiement (« ProcessPayment ») déclenche un remboursement (« RefundPayment »), qui déclenche ensuite l'annulation de la voiture de location et du vol (« CancelRentalReservation » et « CancelFlightReservation »), mettant fin à l'ensemble de la transaction avec un message d'échec.

Ce modèle déploie des fonctions Lambda distinctes pour chaque tâche mise en évidence dans le diagramme, ainsi que trois tables DynamoDB pour les vols, les locations de voitures et les paiements. Chaque fonction Lambda crée, met à jour ou supprime les lignes des tables DynamoDB respectives, selon qu'une transaction est confirmée ou annulée. Le modèle utilise Amazon SNS pour envoyer des messages texte (SMS) aux abonnés, les informant de l'échec ou de la réussite des transactions.

Automatisation et évolutivité

Vous pouvez créer la configuration de cette architecture en utilisant l'un des frameworks IaC. Utilisez l'un des liens suivants pour accéder à votre iAc préféré.

- Déployez avec AWS CDK
- Déploiement avec AWS SAM
- Déployez avec Terraform

Outils

Services AWS

- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions AWS Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise. La console graphique Step Functions vous permet de voir le flux de travail de votre application comme une série d'étapes pilotées par des événements.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles avec une évolutivité sans faille. Vous pouvez utiliser DynamoDB pour créer une table de base de données capable de stocker et de récupérer n'importe quelle quantité de données, ainsi que de traiter n'importe quel niveau de trafic des demandes.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à

l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.

- Amazon API Gateway est un service AWS permettant de créer, de publier, de gérer, de surveiller et de sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages aux abonnés par les éditeurs.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel permettant de définir les ressources de vos applications cloud à l'aide de langages de programmation courants tels que Python TypeScript JavaScript, Java et C#/Net.
- AWS Serverless Application Model (AWS SAM) est un framework open source permettant de créer des applications sans serveur. Il fournit une syntaxe abrégée pour exprimer les fonctions APIs, les bases de données et les mappages de sources d'événements.

Code

Le code d'un exemple d'application illustrant le modèle saga, y compris le modèle IaC (AWS CDK, AWS SAM ou Terraform), les fonctions Lambda et les tables DynamoDB se trouve dans les liens suivants. Suivez les instructions du premier épisode pour les installer.

- Déployez avec AWS CDK
- Déploiement avec AWS SAM
- Déployez avec Terraform

Épopées

Installer des packages, compiler et compiler

Tâche	Description	Compétences requises
Installez les packages NPM.	Créez un nouveau répertoire, naviguez jusqu'à ce répertoire dans un terminal et clonez le GitHub référentiel de votre choix à partir de la section Code plus haut dans ce modèle.	Développeur, architecte cloud

Tâche	Description	Compétences requises
	Dans le dossier racine contenant le `package.json` fichier, exécutez la commande suivante pour télécharger et installer tous les packages Node Package Manager (NPM) : `npm install`	
Compilez des scripts.	Dans le dossier racine, exécutez la commande suivante pour demander au TypeScript transpileur de créer tous les fichiers nécessaires JavaScript : `npm run build`	Développeur, architecte cloud
Surveillez les modifications et recompilez.	Dans le dossier racine, exécutez la commande suivante dans une fenêtre de terminal séparée pour surveiller les modifications de code et compilez le code lorsqu'il détecte une modification : `npm run watch`	Développeur, architecte cloud

Tâche	Description	Compétences requises
Exécutez des tests unitaires (AWS CDK uniquement).	Si vous utilisez le AWS CDK, dans le dossier racine, exécutez la commande suivante pour effectuer les tests unitaires Jest : `npm run test`	Développeur, architecte cloud

Déployer des ressources sur le compte AWS cible

Tâche	Description	Compétences requises
Déployez la pile de démonstration sur AWS.	**Important** L'application est indépendante de la région AWS. Si vous utilisez un profil, vous devez déclarer la région de manière explicite dans le profil AWS Command Line Interface (AWS CLI) ou via des variables d'environnement de l'AWS CLI. Dans le dossier racine, exécutez la commande suivante pour créer un assembly de déploiement et le déployer sur le compte et la région AWS par défaut.	Développeur, architecte cloud

Tâche	Description	Compétences requises

	KIT AWS :
	`cdk bootstrap`
	`cdk deploy`
	IDENTIFIANT AWS :
	`sam build`
	`sam deploy --guided`
	Terraforme :
	`terraform init`
	`terraform apply`
	Cette étape peut prendre plusieurs minutes. Cette commande utilise les informations d'identification par défaut configurées pour l'AWS CLI.
	Notez l'URL de l'API Gateway qui s'affiche sur la console une fois le déploiement terminé. Vous aurez besoin de ces informations pour tester le flux d'exécution de la saga.	

Tâche	Description	Compétences requises

Comparez la pile déployée avec l'état actuel.	Dans le dossier racine, exécutez la commande suivante pour comparer la pile déployée à l'état actuel après avoir modifié le code source :
	
	KIT AWS :
	
	`cdk diff`
	
	IDENTIFIANT AWS :
	
	`sam deploy`
	
	Terraforme :
	
	`terraform plan`
		Développeur, architecte cloud

Tester le flux d'exécution

Tâche	Description	Compétences requises
Testez le flux d'exécution de la saga.	Accédez à l'URL API Gateway que vous avez notée à l'étape précédente, lorsque vous avez déployé la pile. Cette URL déclenche le démarrage de la machine à états. Pour plus d'informations sur la manière de manipuler le flux de la machine à états en transmett ant différents paramètres d'URL, consultez la section Informations supplémentaires.	Développeur, architecte cloud

Tâche	Description	Compétences requises
	Pour consulter les résultats , connectez-vous à l'AWS Management Console et accédez à la console Step Functions. Ici, vous pouvez voir chaque étape de la machine à états de la saga. Vous pouvez également consulter la table DynamoDB pour voir les enregistr ements insérés, mis à jour ou supprimés. Si vous actualise z fréquemment l'écran, vous pouvez voir le statut de la transaction passer de `pending` à`confirmed` . Vous pouvez vous abonner à la rubrique SNS en mettant à jour le code contenu dans le `stateMachine.ts` fichier avec votre numéro de téléphone portable pour recevoir des SMS en cas de réservation réussie ou échouée. Pour plus d'informa tions, consultez Amazon SNS dans la section Informations supplémentaires.	

Nettoyage

Tâche	Description	Compétences requises

Nettoyez les ressources.	Pour nettoyer les ressources déployées pour cette application, vous pouvez utiliser l'une des commandes suivantes.
	
	KIT AWS :
	
	`cdk destroy`
	
	IDENTIFIANT AWS :
	
	`sam delete`
	
	Terraforme :
	
	`terraform destroy`
		Développeur d'applications, architecte cloud

Ressources connexes

Papiers techniques

- Implémentation de microservices sur AWS
- Objectif d'application sans serveur
- Activer la persistance des données dans les microservices

Documentation des services AWS

- Commencer à utiliser le kit AWS CDK
- Commencer à utiliser AWS SAM
- AWS Step Functions
- Amazon DynamoDB

- AWS Lambda
- Amazon API Gateway
- Amazon SNS

Didacticiels

- Ateliers pratiques sur l'informatique sans serveur

Informations supplémentaires

Code

À des fins de test, ce modèle déploie API Gateway et une fonction Lambda de test qui déclenche la machine d'état Step Functions. Avec Step Functions, vous pouvez contrôler les fonctionnalités du système de réservation de voyages en transmettant un `run_type` paramètre pour imiter les défaillances dans «ReserveFlight, » «ReserveCarRental, » «ProcessPayment, » «ConfirmFlight, » et « »ConfirmCarRental.

La fonction `saga` Lambda (`sagaLambda.ts`) prend en compte les paramètres de requête dans l'URL de l'API Gateway, crée l'objet JSON suivant et le transmet à Step Functions pour exécution :

```
let input = {
"trip_id": tripID, //  value taken from query parameter, default is AWS request ID
"depart_city": "Detroit",
"depart_time": "2021-07-07T06:00:00.000Z",
"arrive_city": "Frankfurt",
"arrive_time": "2021-07-09T08:00:00.000Z",
"rental": "BMW",
"rental_from": "2021-07-09T00:00:00.000Z",
"rental_to": "2021-07-17T00:00:00.000Z",
"run_type": runType // value taken from query parameter, default is "success"
};
```

Vous pouvez tester différents flux de la machine d'état Step Functions en transmettant les paramètres d'URL suivants :

- Exécution réussie — https://{api gateway url}
- Le vol de réservation échoue — https://{api gateway url} ? Type d'exécution = failFlightsReservation
- Confirmer l'échec du vol — https://{api gateway url} ? Type d'exécution = failFlightsConfirmation

- La réservation de location de voiture échoue – https://{api gateway url} ? RunType= Réservation failCarRental
- Confirmer l'échec de la location de voiture – https://{api gateway url} ? RunType= Confirmation failCarRental
- Échec du processus de paiement – https://{api gateway url} ? RunType=FailPayment
- Transmettre un code de voyage – https://{api gateway url} ? tripID= {par défaut, l'ID de trajet sera l'ID de demande AWS}

Modèles iAc

Les référentiels liés incluent des modèles IaC que vous pouvez utiliser pour créer l'intégralité de l'exemple d'application de réservation de voyages.

- Déployez avec AWS CDK
- Déploiement avec AWS SAM
- Déployez avec Terraform

Tables DynamoDB

Voici les modèles de données pour les vols, les locations de voitures et les tableaux de paiements.

```
Flight Data Model:
 var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: flightReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: flightReservationID},
        'depart_city' : {S: event.depart_city},
        'depart_time': {S: event.depart_time},
        'arrive_city': {S: event.arrive_city},
        'arrive_time': {S: event.arrive_time},
        'transaction_status': {S: 'pending'}
      }
    };

Car Rental Data Model:
var params = {
```

```
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: carRentalReservationID},
        'trip_id' : {S: event.trip_id},
        'id': {S: carRentalReservationID},
        'rental': {S: event.rental},
        'rental_from': {S: event.rental_from},
        'rental_to': {S: event.rental_to},
        'transaction_status': {S: 'pending'}
      }
    };

Payment Data Model:
var params = {
      TableName: process.env.TABLE_NAME,
      Item: {
        'pk' : {S: event.trip_id},
        'sk' : {S: paymentID},
        'trip_id' : {S: event.trip_id},
        'id': {S: paymentID},
        'amount': {S: "750.00"}, // hard coded for simplicity as implementing any
 monetary transaction functionality is beyond the scope of this pattern
        'currency': {S: "USD"},
        'transaction_status': {S: "confirmed"}
      }
    };
```

Fonctions Lambda

Les fonctions suivantes seront créées pour prendre en charge le flux et l'exécution de la machine à états dans Step Functions :

- Réserver des vols : insère un enregistrement dans le tableau des vols DynamoDB avec `transaction_status` un « `pending` de » pour réserver un vol.
- Confirmer le vol : met à jour l'enregistrement dans le tableau DynamoDB Flights, en le réglant sur`transaction_status`, `confirmed` afin de confirmer le vol.
- Annuler la réservation de vols : Supprime l'enregistrement du tableau des vols DynamoDB pour annuler le vol en attente.
- Réserver une location de voiture : insère un enregistrement dans la table CarRentals DynamoDB avec `transaction_status` un « de » pour réserver une location `pending` de voiture.

- Confirmer les locations de voitures : met à jour l'enregistrement dans la table CarRentals DynamoDB, pour le `transaction_status` définir sur, afin de confirmer `confirmed` la location de voiture.
- Annuler la réservation de location de voiture : Supprime l'enregistrement de la table CarRentals DynamoDB pour annuler la location de voiture en attente.
- Traitement du paiement : insère un enregistrement dans la table des paiements DynamoDB pour le paiement.
- Annuler le paiement : Supprime l'enregistrement du paiement de la table DynamoDB Payments.

Amazon SNS

L'exemple d'application crée le sujet et l'abonnement suivants pour envoyer des SMS et informer le client de la réussite ou de l'échec des réservations. Si vous souhaitez recevoir des SMS pendant que vous testez l'exemple d'application, mettez à jour l'abonnement SMS avec votre numéro de téléphone valide dans le fichier de définition de la machine d'état.

Extrait de code AWS CDK (ajoutez le numéro de téléphone dans la deuxième ligne du code suivant) :

```
const topic = new  sns.Topic(this, 'Topic');
topic.addSubscription(new subscriptions.SmsSubscription('+11111111111'));
const snsNotificationFailure = new tasks.SnsPublish(this ,'SendingSMSFailure', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation Failed'),
});

const snsNotificationSuccess = new tasks.SnsPublish(this ,'SendingSMSSuccess', {
topic:topic,
integrationPattern: sfn.IntegrationPattern.REQUEST_RESPONSE,
message: sfn.TaskInput.fromText('Your Travel Reservation is Successful'),
});
```

Extrait de code AWS SAM (remplacez les +1111111111 chaînes par votre numéro de téléphone valide) :

```
  StateMachineTopic11111111111:
    Type: 'AWS::SNS::Subscription'
    Properties:
      Protocol: sms
```

```
      TopicArn:
        Ref: StateMachineTopic
      Endpoint: '+11111111111'
    Metadata:
      'aws:sam:path': SamServerlessSagaStack/StateMachine/Topic/+11111111111/Resource
```

Extrait de code Terraform (remplacez la +111111111 chaîne par votre numéro de téléphone valide) :

```
resource "aws_sns_topic_subscription" "sms-target" {
  topic_arn = aws_sns_topic.topic.arn
  protocol  = "sms"
  endpoint  = "+11111111111"
}
```

Réservations réussies

Le flux suivant illustre une réservation réussie avec «ReserveFlight, » «ReserveCarRental, » et « ProcessPayment » suivis de « ConfirmFlight » et « »ConfirmCarRental. Le client est informé de la réussite de la réservation par le biais de messages SMS envoyés à l'abonné du sujet SNS.

Réservations échouées

Ce flux est un exemple d'échec dans le schéma de la saga. Si, après avoir réservé des vols et des locations de voitures, « ProcessPayment » échoue, les étapes sont annulées dans l'ordre inverse. Les réservations sont annulées et le client est informé de l'échec par le biais de messages SMS envoyés à l'abonné de la rubrique SNS.

Gérez les applications de conteneur sur site en configurant Amazon ECS Anywhere avec le kit AWS CDK

Créée par le Dr Rahul Sharad Gaikwad (AWS)

Récapitulatif

Amazon ECS Anywhere est une extension d'Amazon Elastic Container Service (Amazon ECS). Vous pouvez utiliser ECS Anywhere pour déployer des tâches Amazon ECS natives dans un environnement sur site ou géré par le client. Cette fonctionnalité permet de réduire les coûts et d'atténuer l'orchestration et les opérations complexes des conteneurs locaux. Vous pouvez utiliser ECS Anywhere pour déployer et exécuter des applications de conteneur dans des environnements sur site et dans le cloud. Ainsi, votre équipe n'a plus besoin d'apprendre plusieurs domaines et compétences, ou de gérer elle-même des logiciels complexes.

Ce modèle décrit les étapes de configuration d'ECS Anywhere à l'aide des piles AWS Cloud Development Kit (AWS CDK).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée. (Voir Installation, mise à jour et désinstallation de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS.)
- AWS CDK Toolkit, installé et configuré. (Consultez le kit d'outils AWS CDK dans la documentation AWS CDK et suivez les instructions pour installer la version 2 dans le monde entier.)
- Gestionnaire de packages de nœuds (npm), installé et configuré pour le AWS CDK dans. TypeScript (Voir Téléchargement et installation de Node.js et de npm dans la documentation de npm.)

Limites

- Pour connaître les limites et les considérations, consultez la section Instances externes (Amazon ECS Anywhere) dans la documentation Amazon ECS.

Versions du produit

- Kit d'outils AWS CDK version 2
- npm version 7.20.3 ou ultérieure
- Node.js version 16.6.1 ou ultérieure

Architecture

Pile technologique cible

- AWS CloudFormation
- AWS CDK
- Amazon ECS Anywhere
- AWS Identity and Access Management (IAM)

Architecture cible

Le schéma suivant illustre une architecture système de haut niveau d'ECS Anywhere configurée à l'aide d'AWS CDK avec TypeScript, telle qu'implémentée par ce modèle.

1. Lorsque vous déployez la pile AWS CDK, elle crée une CloudFormation pile sur AWS.
2. La CloudFormation pile fournit un cluster Amazon ECS et les ressources AWS associées.
3. Pour enregistrer une instance externe auprès d'un cluster Amazon ECS, vous devez installer l'agent AWS Systems Manager (agent SSM) sur votre machine virtuelle (VM) et enregistrer la machine virtuelle en tant qu'instance gérée par AWS Systems Manager.
4. Vous devez également installer l'agent de conteneur Amazon ECS et Docker sur votre machine virtuelle pour l'enregistrer en tant qu'instance externe auprès du cluster Amazon ECS.
5. Lorsque l'instance externe est enregistrée et configurée avec le cluster Amazon ECS, elle peut exécuter plusieurs conteneurs sur votre machine virtuelle, qui est enregistrée en tant qu'instance externe.

Automatisation et mise à l'échelle

Le GitHub référentiel fourni avec ce modèle utilise le CDK AWS comme outil d'infrastructure en tant que code (IaC) pour créer la configuration de cette architecture. AWS CDK vous aide à orchestrer les ressources et à configurer ECS Anywhere.

Outils

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

Code

Le code source de ce modèle est disponible sur GitHub, dans le référentiel Amazon ECS Anywhere CDK Samples. Pour cloner et utiliser le référentiel, suivez les instructions de la section suivante.

Épopées

Vérifier la configuration d'AWS CDK

Tâche	Description	Compétences requises
Vérifiez la version du kit AWS CDK.	Vérifiez la version du kit d'outils AWS CDK en exécutant la commande suivante : `cdk --version` Ce modèle nécessite la version 2 d'AWS CDK. Si vous disposez d'une version antérieure du CDK AWS, suivez les instructions de la documentation du CDK AWS pour la mettre à jour.	DevOps ingénieur
Configurez les informations d'identification AWS.	Pour configurer les informations d'identification, exécutez la `aws configure`	DevOps ingénieur

Tâche	Description	Compétences requises

	commande et suivez les instructions :
	
	`$aws configure`
	`AWS Access Key ID`
	` [None]: <your-access-key-ID>`
	`AWS Secret Access Key`
	` [None]: <your-secret-access-key>`
	`Default region name`
	` [None]: <your-Region-name>`
	`Default output format`
	` [None]:`	

Démarrez l'environnement AWS CDK

Tâche	Description	Compétences requises
Clonez le référentiel de code AWS CDK.	Clonez le référentiel de GitHub code pour ce modèle à l'aide de la commande : `git clone https://github.com/aws-samples/amazon-ecs-anywhere-cdk-samples.git`	DevOps ingénieur
Démarrez l'environnement.	Pour déployer le CloudFormation modèle AWS sur le compte et la région AWS que vous souhaitez utiliser, exécutez la commande suivante :	DevOps ingénieur

Tâche	Description	Compétences requises
	`cdk bootstrap <account-number>/<Region>` Pour plus d'informations, consultez la section Bootstrapping dans la documentation AWS CDK.	

Créez et déployez le projet

Tâche	Description	Compétences requises

Installez les dépendances des packages et compilez TypeScript les fichiers.	Installez les dépendances du package et compilez les TypeScript fichiers en exécutant les commandes suivantes :
	
	`$cd amazon-ecs-anywhere-cdk-samples`
	`$npm install`
	`$npm fund`
	
	Ces commandes installent tous les packages du référentiel d'échantillons.
	
	⚠ Important
	Si vous recevez des erreurs concernant des packages manquants, utilisez
		DevOps ingénieur

Tâche	Description	Compétences requises

	l'une des commandes suivantes :
	
	`$npm ci`
	
	—ou—
	
	`$npm install -g @aws-cdk/<package_name>`
	
	Pour plus d'informations, consultez npm ci et npm install dans la documentation de npm.	

Générez le projet.	Pour créer le code du projet, exécutez la commande suivante : `npm run build` Pour plus d'informations sur la création et le déploiement du projet, consultez Votre première application AWS CDK dans la documentation du CDK AWS.	DevOps ingénieur
Déployez le projet.	Pour déployer le code du projet, exécutez la commande suivante : `cdk deploy`	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez la création et la sortie de la pile.	Ouvrez la CloudFormation console AWS à l'https://console.aws.amazon.comadresse /cloudformation et choisissez la `EcsAnywhereStack` pile. L'onglet Sorties affiche les commandes à exécuter sur votre machine virtuelle externe.	DevOps ingénieur

Configuration d'une machine sur site

Tâche	Description	Compétences requises
Configurez votre machine virtuelle à l'aide de Vagrant.	À des fins de démonstration, vous pouvez utiliser HashiCorp Vagrant pour créer une machine virtuelle. Vagrant est un utilitaire open source permettant de créer et de maintenir des environnements de développement de logiciels virtuels portables. Créez une machine virtuelle Vagrant en exécutant la `vagrant up` commande depuis le répertoire racine dans lequel Vagrantfile est placé. Pour plus d'informations, consultez la documentation de Vagrant.	DevOps ingénieur
Enregistrez votre machine virtuelle en tant qu'instance externe.	1. Connectez-vous à la machine virtuelle Vagrant à l'aide de la `vagrant`	DevOps ingénieur

Tâche	Description	Compétences requises

	`ssh` commande. Pour plus d'informations, consultez la documentation de Vagrant.
	
	2. Créez un code d'activation et un identifiant que vous pouvez utiliser pour enregistrer votre machine virtuelle auprès d'AWS Systems Manager et pour activer votre instance externe. Le résultat de cette commande inclut les `ActivationCode` valeurs `ActivationId` et suivantes :
	
	`aws ssm create-activation --iam-role EcsAnywhereInstanceRole | tee ssm-activation.json`
	
	3. Exportez l'ID d'activation et les valeurs du code :
	
	`export ACTIVATION_ID=<activation-ID>`
	`export ACTIVATION_CODE=<activation-code>`
	
	4. Téléchargez le script d'installation sur votre serveur ou machine virtuelle sur site :
	
	`curl -o "ecs-anywhere-install.sh" "https://`	

Tâche	Description	Compétences requises

	`amazon-ecs-agent.s3.amazonaws.com/ecs-anywhere-install-latest.sh" && sudo chmod +x ecs-anywhere-install.sh`
	
	5. Exécutez le script d'installation sur votre serveur ou machine virtuelle sur site :
	
	`sudo ./ecs-anywhere-install.sh \ --cluster test-ecs-anywhere \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <Region>`
	
	Pour plus d'informations sur la configuration et l'enregistrement de votre machine virtuelle, consultez la section Enregistrement d'une instance externe dans un cluster dans la documentation Amazon ECS.	

Tâche	Description	Compétences requises

Vérifiez l'état d'ECS Anywhere et de la machine virtuelle externe.	Pour vérifier si votre boîte virtuelle est connectée au plan de contrôle Amazon ECS et en cours d'exécution, utilisez les commandes suivantes :
	`aws ssm describe-instance-information`
	`aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps ingénieur

Nettoyage

Tâche	Description	Compétences requises
Nettoyez et supprimez les ressources.	Après avoir suivi ce schéma, vous devez supprimer les ressources que vous avez créées pour éviter d'encouri r des frais supplémentaires. Pour nettoyer, exécutez la commande suivante : `cdk destroy`	DevOps ingénieur

Ressources connexes

- Documentation Amazon ECS Anywhere
- Démo d'Amazon ECS Anywhere
- Exemples d'ateliers Amazon ECS Anywhere

Modernisez les applications ASP.NET Web Forms sur AWS

Créée par Vijai Anand Ramalingam (AWS) et Sreelaxmi Pai (AWS)

Récapitulatif

Ce modèle décrit les étapes de modernisation d'une ancienne application ASP.NET Web Forms monolithe en la portant vers ASP.NET Core sur AWS.

Le portage des applications ASP.NET Web Forms vers ASP.NET Core vous permet de tirer parti des performances, des économies et de l'écosystème robuste de Linux. Cependant, il peut s'agir d'un effort manuel important. Dans ce modèle, l'ancienne application est modernisée progressivement en utilisant une approche progressive, puis conteneurisée dans le cloud AWS.

Envisagez une ancienne application monolithe pour un panier d'achats. Supposons qu'il a été créé en tant qu'application ASP.NET Web Forms et qu'il se compose de pages .aspx avec un fichier code-behind (). `aspx.cs` Le processus de modernisation comprend les étapes suivantes :

1. Divisez le monolithe en microservices en utilisant les modèles de décomposition appropriés. Pour plus d'informations, consultez le guide Décomposer les monolithes en microservices sur le site Web AWS Prescriptive Guidance.
2. Portez votre ancienne application ASP.NET Web Forms (.NET Framework) vers ASP.NET Core dans .NET 5 ou version ultérieure. Dans ce modèle, vous utilisez l'assistant de portage pour .NET pour analyser votre application ASP.NET Web Forms et identifier les incompatibilités avec ASP.NET Core. Cela réduit l'effort de portage manuel.
3. Redéveloppez la couche d'interface utilisateur Web Forms à l'aide de React. Ce modèle ne couvre pas le réaménagement de l'interface utilisateur. Pour obtenir des instructions, voir Créer une nouvelle application React dans la documentation React.
4. Redéveloppez le fichier de code Web Forms (interface professionnelle) en tant qu'API Web ASP.NET Core. Ce modèle utilise des NDepend rapports pour aider à identifier les fichiers et les dépendances requis.
5. Mettez à niveau les projets partagés/communs, tels que Business Logic et Data Access, de votre ancienne application vers .NET 5 ou version ultérieure à l'aide de l'assistant de portage pour .NET.
6. Ajoutez des services AWS pour compléter votre application. Par exemple, vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder aux journaux de votre application, et AWS Systems Manager pour stocker les paramètres de votre application.

7. Conteneurisez l'application ASP.NET Core modernisée. Ce modèle crée un fichier Docker qui cible Linux dans Visual Studio et utilise Docker Desktop pour le tester localement. Cette étape suppose que votre ancienne application est déjà exécutée sur une instance Windows sur site ou Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez le modèle Exécuter un conteneur Docker d'API Web ASP.NET Core sur une instance Amazon EC2 Linux.
8. Déployez l'application principale ASP.NET modernisée sur Amazon Elastic Container Service (Amazon ECS). Ce modèle ne couvre pas l'étape de déploiement. Pour obtenir des instructions, consultez l'atelier Amazon ECS.

> **Note**
>
> Ce modèle ne couvre pas le développement de l'interface utilisateur, la modernisation de la base de données ou les étapes de déploiement de conteneurs.

Conditions préalables et limitations

Prérequis

- Visual Studio ou Visual Studio Code, téléchargé et installé.
- Accès à un compte AWS à l'aide de la console de gestion AWS et de l'interface de ligne de commande AWS (AWS CLI) version 2. (Consultez les instructions de configuration de l'interface de ligne de commande AWS.)
- Le kit d'outils AWS pour Visual Studio (voir les instructions de configuration).
- Docker Desktop, téléchargé et installé.
- SDK .NET, téléchargé et installé.
- NDepend outil, téléchargé et installé. Pour installer l' NDepend extension pour Visual Studio, exécutez `NDepend.VisualStudioExtension.Installer` (voir les instructions). Vous pouvez sélectionner Visual Studio 2019 ou 2022, selon vos besoins.
- Assistant de portage pour .NET, téléchargé et installé.

Architecture

Modernisation de l'application de panier

Le schéma suivant illustre le processus de modernisation d'une ancienne application de panier d'achat ASP.NET.

Architecture cible

Le schéma suivant illustre l'architecture de l'application de panier d'achat modernisée sur AWS. APIs Les sites Web ASP.NET Core sont déployés sur un cluster Amazon ECS. Les services de journalisation et de configuration sont fournis par Amazon CloudWatch Logs et AWS Systems Manager.

Outils

Services AWS

- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif permettant d'exécuter, d'arrêter et de gérer des conteneurs sur un cluster. Vous pouvez exécuter vos tâches et services sur une infrastructure sans serveur gérée par AWS Fargate. Pour mieux contrôler votre infrastructure, vous pouvez également exécuter vos tâches et services sur un cluster d' EC2 instances que vous gérez.
- Amazon CloudWatch Logs — Amazon CloudWatch Logs centralise les journaux de tous les systèmes, applications et services AWS que vous utilisez. Vous pouvez consulter et surveiller les journaux, y rechercher des codes ou modèles d'erreur spécifiques, les filtrer en fonction de champs spécifiques ou les archiver en toute sécurité pour une analyse future.
- AWS Systems Manager – AWS Systems Manager est un service AWS que vous pouvez utiliser pour visualiser et contrôler votre infrastructure sur AWS. À l'aide de la console Systems Manager, vous pouvez consulter les données opérationnelles de plusieurs services AWS et automatiser les tâches opérationnelles sur l'ensemble de vos ressources AWS. Systems Manager vous aide à maintenir la sécurité et la conformité en scannant vos instances gérées et en signalant (ou en prenant des mesures correctives) les violations des politiques détectées.

Outils

- Visual Studio ou Visual Studio Code : outils permettant de créer des applications .NET, des applications Web APIs et d'autres programmes.
- AWS Toolkit for Visual Studio : extension pour Visual Studio qui permet de développer, de déboguer et de déployer des applications .NET utilisant les services AWS.

- Docker Desktop : outil qui simplifie la création et le déploiement d'applications conteneurisées.
- NDepend— Un analyseur qui surveille le code .NET pour détecter les dépendances, les problèmes de qualité et les modifications de code.
- Assistant de portage pour .NET : outil d'analyse qui analyse le code .NET afin d'identifier les incompatibilités avec .NET Core et d'estimer l'effort de migration.

Épopées

Portez votre ancienne application vers .NET 5 ou version ultérieure

Tâche	Description	Compétences requises
Mettez à niveau votre ancienne application .NET Framework vers .NET 5.	Vous pouvez utiliser l'assistant de portage pour .NET pour convertir votre ancienne application ASP.NET Web Forms en .NET 5 ou version ultérieure. Suivez les instructions de la documentation de l'assistant de portage pour .NET.	Développeur d’applications
Générez NDepend des rapports.	Lorsque vous modernisez votre application ASP.NET Web Forms en la décomposant en microservices, il se peut que vous n'ayez pas besoin de tous les fichiers .cs de l'ancienne application. Vous pouvez l'utiliser NDepend pour générer un rapport pour n'importe quel fichier code-behind (.cs), afin d'obtenir tous les appelants et appelés. Ce rapport vous aide à identifier et à utiliser uniquement	Développeur d’applications

Tâche	Description	Compétences requises
	les fichiers requis dans vos microservices. Après l'installation NDepend (voir la section Conditions préalables), ouvrez la solution (fichier .sln) pour votre ancienne application dans Visual Studio et procédez comme suit : 1. Créez l'ancienne application dans Visual Studio. 2. Dans la barre de menu de Visual Studio NDepend, choisissez Attacher un nouveau NDepend projet à la solution VS actuelle. 3. Choisissez Analyser les assemblages .NET. 4. Lorsque l'analyse est terminée, accédez au projet dans l'Explorateur de solutions. Cliquez avec le bouton droit sur un fichier code-behind (par exemple,`listproducts.aspx.cs`) pour lequel vous souhaitez générer le rapport, puis choisissez Afficher sur le graphe de dépendance. 5. Dans la barre de navigation, sélectionnez Appelants	

Tâche	Description	Compétences requises
	et appelés, puis Modifier la requête de code. 6. Dans le volet d'édition des requêtes et des règles, cliquez sur la flèche de téléchargement, puis sélectionnez Exporter vers Excel. Ce processus génère un rapport pour le fichier code-behind qui répertorie tous les appelants et appelés. Pour plus d'informations sur le graphe de dépendance, consultez la NDepend documentation.	

Tâche	Description	Compétences requises
Créez une nouvelle solution .NET 5.	Pour créer une nouvelle structure .NET 5 (ou version ultérieure) pour votre site Web ASP.NET Core modernisé : APIs 1. Ouvrez Visual Studio. 2. Créez une nouvelle solution vide. 3. Créez de nouveaux projets qui ciblent .NET 5 (ou version ultérieure), en fonction de votre ancienne application. Pour des exemples d'anciens et de nouveaux projets pour une application de panier d'achat, consultez la section Informations supplémentaires. 4. Utilisez le NDepend rapport de l'étape précédente pour identifier tous les fichiers requis. Copiez ces fichiers depuis l'application que vous avez mise à niveau précédemment et ajoutez-les à la nouvelle solution. 5. Développez la solution et corrigez tous les problèmes. Pour plus d'informations sur la création de projets et de solutions, consultez	Développeur d’applications

Tâche	Description	Compétences requises
	la documentation de Visual Studio. **Note** Au fur et à mesure que vous créez la solution et que vous vérifiez ses fonctionnalités, vous pouvez identifier plusieurs fichiers supplémentaires à ajouter à la solution, en plus des fichiers NDepend identifiés.	

Mettez à jour le code de votre application

Tâche	Description	Compétences requises
Implémentez le Web APIs avec ASP.NET Core.	Supposons que l'un des microservices que vous avez identifiés dans votre ancienne application de panier d'achat monolithe soit Products. Vous avez créé un nouveau projet d'API Web ASP.NET Core pour les produits dans l'épopée précédente. Au cours de cette étape, vous identifiez et modernisez tous les formulaires Web (pages .aspx) liés aux produits. Supposons que les produits se composent	Développeur d’applications

Tâche	Description	Compétences requises
	de quatre formulaires Web, comme illustré précédemment dans la section Architecture : • Liste des produits • Afficher le produit • Ajouter/modifier un produit • Supprimer le produit Vous devez analyser chaque formulaire Web, identifie r toutes les demandes envoyées à la base de données pour appliquer une certaine logique et obtenir des réponses. Vous pouvez implémenter chaque demande en tant que point de terminais on d'API Web. Compte tenu de ses formulaires Web, les produits peuvent avoir les points de terminaison suivants : • `/api/products` • `/api/products/{id}` • `/api/products/add` • `/api/products/upda te/{id}` • `/api/products/dele te/{id}`	

Tâche	Description	Compétences requises
	Comme indiqué précédemment, vous pouvez également réutiliser tous les autres projets que vous avez mis à niveau vers .NET 5, notamment Business Logic, Data Access et les projets partagés/communs.	
Configurez Amazon CloudWatch Logs.	Vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder aux journaux de votre application. Vous pouvez enregistrer des données dans Amazon CloudWatch Logs à l'aide d'un SDK AWS. Vous pouvez également intégrer des applications .NET à CloudWatch Logs en utilisant des frameworks de journalisation .NET courants tels que NLogLog4Net et ASP.NET Core. Pour plus d'informations sur cette étape, consultez le billet de blog Amazon CloudWatch Logs and .NET Logging Frameworks.	Développeur d’applications

Tâche	Description	Compétences requises
Configurez le magasin de paramètres AWS Systems Manager.	Vous pouvez utiliser AWS Systems Manager Parameter Store pour stocker les paramètres de l'application, tels que les chaînes de connexion, séparément du code de votre application. Le NuGet package Amazon.Extensions.Configuration.SystemsManagersimplifie la façon dont votre application charge ces paramètres depuis l'AWS Systems Manager Parameter Store dans le système de configuration .NET Core. Pour plus d'informations sur cette étape, consultez le billet de blog sur le fournisseur de configuration .NET Core pour AWS Systems Manager.	Développeur d’applications

Ajouter l'authentification et l'autorisation

Tâche	Description	Compétences requises
Utilisez un cookie partagé pour l'authentification.	La modernisation d'une ancienne application monolithe est un processus itératif qui nécessite la coexistence du monolithe et de sa version modernisée. Vous pouvez utiliser un cookie	Développeur d’applications

Tâche	Description	Compétences requises
	partagé pour garantir une authentification fluide entre les deux versions. L'ancienne application ASP.NET continue de valider les informations d'identification de l'utilisateur et émet le cookie tandis que l'application ASP.NET Core modernisée valide le cookie. Pour obtenir des instructi ons et un exemple de code, consultez l'exemple de GitHub projet.	

Créez et exécutez le conteneur localement

Tâche	Description	Compétences requises
Créez une image Docker à l'aide de Visual Studio.	Au cours de cette étape, vous allez créer un fichier Docker à l'aide de l'API Web Visual Studio pour .NET Core. 1. Ouvrez Visual Studio. 2. Dans l'Explorateur de solutions, dans le menu contextuel (clic droit) de votre projet, choisissez Ajouter, Docker Support. 3. Sélectionnez Linux comme système d'exploitation cible.	Développeur d’applications

Tâche	Description	Compétences requises
	Visual Studio crée un fichier Docker pour votre projet. Pour un exemple de fichier Docker, voir Visual Studio Container Tools pour Docker sur le site Web de Microsoft.	

Tâche	Description	Compétences requises

Créez et exécutez le conteneur à l'aide de Docker Desktop.	Vous pouvez désormais créer, créer et exécuter le conteneur dans Docker Desktop.
	1. Ouvrez une fenêtre d'invite de commande. Accédez au dossier de solution dans lequel se trouve le fichier Docker. Exécutez la commande suivante pour créer l'image Docker :
	`docker build -t aspnetcorewebapiimage -f Dockerfile .`
	2. Exécutez la commande suivante pour afficher toutes les images Docker :
	`docker images`
	3. Exécutez la commande suivante pour créer et exécuter un conteneur :
	`docker run -d -p 8080:80 --name aspnetcorewebapicontainer aspnetcorewebapiimage`
	4. Ouvrez Docker Desktop, puis choisissez Conteneurs/Apps. Vous pouvez voir un nouveau conteneur nommé
		Développeur d'applications

Tâche	Description	Compétences requises
	`aspnetcorewebapicontainer` running.	

Ressources connexes

- Exécuter un conteneur Docker d'API Web ASP.NET Core sur une instance Amazon EC2 Linux (AWS Prescriptive Guidance)
- Atelier Amazon ECS
- Effectuez des déploiements d'ECS bleu/vert à l'aide d' CodeDeploy AWS (documentation CloudFormation AWS) CloudFormation
- Mise en route avec NDepend (NDepend documentation)
- Assistant de portage pour .NET

Informations supplémentaires

Les tableaux suivants fournissent des exemples de projets pour une ancienne application de panier d'achat et les projets équivalents dans votre application ASP.NET Core modernisée.

Solution héritée :

Nom du projet	Modèle de projet	Infrastructure cible
Interface commerciale	Bibliothèque de classes	.NET Framework
BusinessLogic	Bibliothèque de classes	.NET Framework
WebApplication	Application Web ASP.NET Framework	.NET Framework
UnitTests	NUnit Projet de test	.NET Framework
Partagé -> Commun	Bibliothèque de classes	.NET Framework
Framework partagé	Bibliothèque de classes	.NET Framework

Nouvelle solution :

Nom du projet	Modèle de projet	Infrastructure cible
BusinessLogic	Bibliothèque de classes	.NET 5.0
<WebAPI>	API Web ASP.NET Core	.NET 5.0
<WebAPI>. UnitTests	NUnit 3 Projet de test	.NET 5.0
Partagé -> Commun	Bibliothèque de classes	.NET 5.0
Framework partagé	Bibliothèque de classes	.NET 5.0

Exécutez des charges de travail planifiées et pilotées par des événements à grande échelle avec AWS Fargate

Créée par HARI OHM PRASATH RAJAGOPAL (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle décrit comment exécuter des charges de travail planifiées et basées sur des événements à grande échelle sur le cloud Amazon Web Services (AWS) à l'aide d'AWS Fargate.

Dans le cas d'utilisation défini par ce modèle, le code est scanné pour détecter les informations sensibles d'AWS, telles que le numéro de compte AWS et les informations d'identification, chaque fois qu'une pull request est soumise. La pull request lance une fonction Lambda. La fonction Lambda appelle une tâche Fargate qui prend en charge le scan du code. Lambda est lancé chaque fois qu'une nouvelle pull request est émise. Si le scan détecte des informations sensibles, Amazon Simple Notification Service (Amazon SNS) envoie les résultats du scan par e-mail.

Ce modèle est utile dans les cas d'utilisation professionnelle suivants :

- Si votre entreprise doit exécuter de nombreuses charges de travail planifiées et basées sur des événements qui ne peuvent pas être exécutées par AWS Lambda en raison de limites d'exécution (limite de 15 minutes) ou de mémoire
- Si vous souhaitez qu'AWS gère les instances mises en service pour ces charges de travail

Lorsque vous utilisez ce modèle, vous avez la possibilité de créer un nouveau cloud privé virtuel (VPC). Ce modèle utilise également AWS CodeCommit.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- AWS CodeCommit pour héberger la base de code et créer des pull requests
- Interface de ligne de commande AWS (AWS CLI) version 1.7 ou ultérieure, installée et configurée sur macOS, Linux ou Windows
- Charges de travail exécutées dans des conteneurs

- Exécutable Apache Maven configuré dans classpath

Architecture

Le flux global comprend les étapes suivantes.

1. Chaque fois qu'une nouvelle pull request est soumise CodeCommit, une fonction Lambda est lancée. La fonction Lambda écoute l'événement `CodeCommit Pull Request State Change` via Amazon. EventBridge
2. La fonction Lambda soumet une nouvelle tâche Fargate avec les paramètres d'environnement suivants pour extraire le code et le scanner.

   ```
   RUNNER # <<TaskARN>>
   SNS_TOPIC # <<SNSTopicARN>>
   SUBNET # <<Subnet in which Fargate task gets launched>>
   ```

   Si le scan détecte des informations sensibles dans le code, Fargate envoie un nouveau message à la rubrique Amazon SNS.
3. Un abonné SNS lit le message du sujet et envoie un e-mail.

Technologie

- AWS CodeCommit
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon EventBridge
- AWS Fargate
- AWS Lambda
- Amazon SNS
- Docker

Outils

Outils

- AWS CLI — L'interface de ligne de commande (CLI) AWS est un outil unifié permettant de gérer vos services AWS.
- AWS CodeCommit — AWS CodeCommit est un service de contrôle de source entièrement géré qui héberge des référentiels sécurisés basés sur Git. Grâce à CodeCommit cela, les équipes peuvent collaborer sur le code dans un environnement sécurisé et hautement évolutif.
- Amazon ECR — Amazon Elastic Container Registry (Amazon ECR) est un registre entièrement géré que les développeurs peuvent utiliser pour stocker, gérer et déployer des images de conteneurs Docker.
- Amazon ECS — Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs rapide et hautement évolutif. Vous pouvez utiliser Amazon ECS pour exécuter, arrêter et gérer des conteneurs sur un cluster.
- AWS Fargate — AWS Fargate est une technologie que vous pouvez utiliser avec Amazon ECS pour exécuter des conteneurs sans avoir à gérer des serveurs ou des clusters d'instances Amazon. EC2
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service géré qui permet aux éditeurs de transmettre des messages aux abonnés (également appelés producteurs et consommateurs). Les éditeurs communiquent de façon asynchrone avec les abonnés en envoyant un message à une rubrique, qui est un point d'accès logique et un canal de communication. Les clients qui s'abonnent à la rubrique SNS reçoivent les messages publiés à l'aide d'un protocole compatible, tel que Lambda, le courrier électronique, les notifications push mobiles et les SMS.
- Docker — Docker vous aide à créer, tester et fournir des applications dans des packages appelés conteneurs.
- Client Git : ligne de commande ou outil de bureau pour récupérer les artefacts requis
- Maven — Apache Maven est un outil de gestion de projet permettant de gérer de manière centralisée le build, les rapports et la documentation d'un projet.

Épopées

Configuration du référentiel local

Tâche	Description	Compétences requises
Téléchargez le code.	Dans la section Pièces jointes, téléchargez le fichier .zip et extrayez les fichiers.	Développeur, administrateur système AWS
Configurez le dépôt.	Exécutez `mvn clean install` sur le dossier racine.	Développeur, administrateur système AWS

Créez une image Amazon ECR et publiez l'image

Tâche	Description	Compétences requises
Créez un référentiel Amazon ECR et connectez-vous.	Ouvrez la console Amazon ECR. Dans le volet de navigation, choisissez Repositories, puis Create repository. Pour obtenir de l'aide sur ce sujet et sur d'autres articles, consultez la section Ressources connexes.	Développeur, administrateur système AWS
Envoyez votre image de conteneur.	Ouvrez le référentiel, choisisse z Afficher les commandes push et connectez-vous à Docker. Une fois connecté, exécutez les commandes , avec les substitutions requises, qui se trouvent sous Envoyer l'image du conteneur dans la section Informations supplémentaires. Cela télécharge l'image du	Développeur, administrateur système AWS

Tâche	Description	Compétences requises
	conteneur Docker qui est utilisée pour effectuer le scan du code. Une fois le télécharg ement terminé, copiez l'URL de la dernière version dans le référentiel Amazon ECR.	

Création du CodeCommit référentiel

Tâche	Description	Compétences requises
Créez le CodeCommit référentiel.	Pour créer un nouveau CodeCommit référentiel AWS, exécutez la commande sous Créer le CodeCommit référenti el dans la section Informations supplémentaires.	Développeur, administrateur système AWS

Créez le VPC (facultatif)

Tâche	Description	Compétences requises
Créez un VPC.	Si vous souhaitez utiliser un nouveau VPC plutôt qu'un VPC existant, exécutez les commandes sous Créer un VPC dans la section Informati ons supplémentaires. Le script AWS Cloud Development Kit (AWS CDK) produira le IDs VPC et le sous-réseau créés.	Développeur, administrateur système AWS

Création du cluster Amazon ECS et de la tâche Fargate

Tâche	Description	Compétences requises
Créez le cluster et la tâche.	Pour créer un cluster Amazon ECS et définir une tâche Fargate, exécutez les commandes sous Créer le cluster et la tâche dans la section Informations supplémentaires. Assurez-vous que l'ID VPC et l'URI du dépôt Amazon ECR corrects sont transmis en tant que paramètre lors de l'exécution du script shell. Le script crée une définition de tâche Fargate qui pointe vers l'image Docker (responsable de la numérisation). Le script crée ensuite une tâche et un rôle d'exécution associé.	Développeur, administrateur système AWS
Vérifiez le cluster Amazon ECS.	Ouvrez la console Amazon ECS. Dans le volet de navigation, choisissez Clusters, puis le cluster Amazon ECS nouvellement créé nommé Fargate-Job-Cluster. Ensuite, choisissez Définition de tâche dans le volet de navigation et vérifiez qu'il existe une nouvelle définition de tâche avec le préfixe `awscdkfargateecsTaskDef` .	Développeur, administrateur système AWS

Créez le sujet et l'abonné SNS

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Pour créer une rubrique SNS, exécutez la commande sous Créer la rubrique SNS dans la section Informations supplémentaires. Une fois la création réussie, notez leSNS ARN, qui est utilisé à l'étape suivante.	Développeur, administrateur système AWS
Créez l'abonné SNS.	Pour créer un abonné par e-mail pour la rubrique SNS, exécutez la commande sous Créer un abonné SNS dans la section Informations supplémentaires. Assurez-vous de les remplacer `TopicARN` et de les `Email address` utiliser dans la commande CLI. Pour recevoir des notifications par e-mail, assurez-vous de confirmer l'adresse e-mail utilisée en tant qu'abonné.	Développeur, administrateur système AWS

Création de la fonction Lambda et du déclencheur CodeCommit

Tâche	Description	Compétences requises
Créez la fonction et le déclencheur.	Pour créer une fonction Lambda avec un CodeCommi t déclencheur, exécutez la commande sous Fonction	Développeur, administrateur système AWS

Tâche	Description	Compétences requises
	Lambda et CodeCommit déclencheur dans la section Informations supplémentaires. Assurez-vous de remplacer les paramètres par les valeurs correspondantes avant d'exécuter la commande. Le script crée la fonction Lambda et la configure pour qu'elle soit invoquée lors d'une nouvelle pull request.	

Tester l'application

Tâche	Description	Compétences requises
Testez l'application.	Si vous consignez des informations sensibles d'AWS dans le CodeCommit dépôt, la fonction Lambda doit être lancée. La fonction Lambda lance la tâche Fargate, qui analyse le code et envoie les résultats de l'analyse dans une notification par e-mail.	Développeur, administrateur système AWS

Ressources connexes

- Création d'un référentiel Amazon ECR
- Transférer des images Docker vers Amazon ECR

Informations supplémentaires

Appuyez sur l'image du conteneur

```
> cd 1-ecr-image-push
> ./run.sh <<ecr-repository>>
```

Création du CodeCommit référentiel

```
aws codecommit create-repository --repository-name test-repo --repository-description
 "My Test repository"
```

Créer un VPC

```
> cd 2-create-vpc
> ./run.sh
```

Sortie

```
aws-batch-cdk-vpc-efs-launch-template.privatesubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.publicsubnet = subnet-<<id>>
aws-batch-cdk-vpc-efs-launch-template.vpcid = vpc-<<id>>
```

Création du cluster et de la tâche

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 3-create-ecs-task
> ./run.sh <<vpc-id>> <<ecr-repo-uri>>
```

Sortie

```
aws-cdk-fargate-ecs.CLUSTERNAME = Fargate-Job-Cluster
aws-cdk-fargate-ecs.ClusterARN = <<cluster_arn>>
aws-cdk-fargate-ecs.ContainerARN = Fargate-Container
aws-cdk-fargate-ecs.TaskARN = <<task_arn>>
aws-cdk-fargate-ecs.TaskExecutionRole = <<execution_role_arn>>
aws-cdk-fargate-ecs.TaskRole = <<task_role_arn>>
```

Création de la rubrique SNS

```
aws sns create-topic --name code-commit-topic
```

Créez l'abonné SNS

```
aws sns subscribe \
    --topic-arn <<topic_arn>> \
    --protocol email \
    --notification-endpoint <<email_address>>
```

Fonction Lambda et déclencheur CodeCommit

```
> export CDK_DEFAULT_ACCOUNT = <<aws_account_id>>
> export CDK_DEFAULT_REGION = <<aws_region>>
> cd 5-Lambda-CodeCommit-Trigger
> ./run.sh <<taskarn>> <<snstopicarn>> subnet-<<id>> <<codecommitarn>>
```

Sortie

```
aws-cdk-fargate-lambda-event.Cloudwatchrule = <<cloudwatchrule>>
aws-cdk-fargate-lambda-event.CodeCommitLambda = AWS-Code-Scanner-Function
aws-cdk-fargate-lambda-event.LambdaRole = <<lambdaiamrole>>
```

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Intégration des locataires dans l'architecture SaaS pour le modèle de silo à l'aide de C# et d'AWS CDK

Créée par Tabby Ward (AWS), Susmitha Reddy Gankidi (AWS) et Vijai Anand Ramalingam (AWS)

Récapitulatif

Les applications SaaS (Software as a Service) peuvent être créées à l'aide de différents modèles architecturaux. Le modèle de silo fait référence à une architecture dans laquelle les locataires disposent de ressources dédiées.

Les applications SaaS s'appuient sur un modèle fluide pour introduire de nouveaux locataires dans leur environnement. Cela nécessite souvent l'orchestration d'un certain nombre de composants pour approvisionner et configurer correctement tous les éléments nécessaires à la création d'un nouveau locataire. Ce processus, dans l'architecture SaaS, est appelé intégration des locataires. L'intégration doit être entièrement automatisée pour chaque environnement SaaS en utilisant l'infrastructure sous forme de code dans votre processus d'intégration.

Ce modèle vous guide à travers un exemple de création d'un locataire et de mise en service d'une infrastructure de base pour le locataire sur Amazon Web Services (AWS). Le modèle utilise le C# et l'AWS Cloud Development Kit (AWS CDK).

Étant donné que ce modèle crée une alarme de facturation, nous vous recommandons de déployer la pile dans la région AWS de l'est des États-Unis (Virginie du Nord), ou us-east-1. Pour plus d'informations, consultez la documentation AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un responsable AWS Identity and Access Management (IAM) disposant d'un accès IAM suffisant pour créer des ressources AWS correspondant à ce modèle. Pour en savoir plus, consultez Rôles IAM.
- Installez l'interface de ligne de commande Amazon (AWS CLI) et configurez l'interface de ligne de commande AWS pour effectuer le déploiement d'AWS CDK.
- Visual Studio 2022 a été téléchargé et installé ou Visual Studio Code a été téléchargé et installé.
- Configuration d'AWS Toolkit pour Visual Studio.

- .NET Core 3.1 ou version ultérieure (requis pour les applications C# AWS CDK)
- Amazon.Lambda.Tools installé.

Limites

- AWS CDK utilise AWS CloudFormation. Les applications AWS CDK sont donc soumises à des quotas de CloudFormation service. Pour plus d'informations, consultez la section CloudFormation Quotas AWS.
- La CloudFormation pile de locataires est créée avec un rôle de CloudFormation service `infra-cloudformation-role` avec des caractères génériques sur les actions (`sns*` et`sqs*`) mais avec des ressources limitées au `tenant-cluster` préfixe. Pour un cas d'utilisation en production, évaluez ce paramètre et fournissez uniquement l'accès requis à ce rôle de service. La fonction `InfrastructureProvision` Lambda utilise également un caractère générique (`cloudformation*`) pour approvisionner la CloudFormation pile, mais les ressources sont limitées au préfixe. `tenant-cluster`
- La version docker de cet exemple de code est utilisée `--platform=linux/amd64` pour forcer les images`linux/amd64`. Cela permet de garantir que les artefacts d'image finaux seront adaptés à Lambda, qui utilise par défaut l'architecture x86-64. Si vous devez modifier l'architecture Lambda cible, veillez à modifier à la fois les codes Dockerfiles et AWS CDK. Pour plus d'informations, consultez le billet de blog Migration des fonctions AWS Lambda vers les processeurs AWS Graviton2 basés sur ARM.
- Le processus de suppression de la pile ne nettoie pas CloudWatch les journaux (groupes de journaux et journaux) générés par la pile. Vous devez nettoyer manuellement les journaux via la console Amazon AWS Management CloudWatch Console ou via l'API.

Ce modèle est configuré à titre d'exemple. Pour une utilisation en production, évaluez les configurations suivantes et apportez des modifications en fonction des besoins de votre entreprise :

- Dans cet exemple, la gestion des versions du bucket AWS Simple Storage Service (Amazon S3) n'est pas activée pour des raisons de simplicité. Évaluez et mettez à jour la configuration selon les besoins.
- Cet exemple configure les points de terminaison de l'API REST Amazon API Gateway sans authentification, autorisation ou limitation pour des raisons de simplicité. Pour une utilisation en production, nous recommandons d'intégrer le système à l'infrastructure de sécurité de l'entreprise. Évaluez ce paramètre et ajoutez les paramètres de sécurité requis selon les besoins.

- Pour cet exemple d'infrastructure client, Amazon Simple Notification Service (Amazon SNS) et Amazon Simple Queue Service (Amazon SQS) ne proposent que des configurations minimales. L'AWS Key Management Service (AWS KMS) de chaque locataire ouvre la voie aux services Amazon CloudWatch et Amazon SNS du compte à utiliser conformément à la politique clé d'AWS KMS. La configuration n'est qu'un exemple d'espace réservé. Ajustez les configurations selon vos besoins en fonction de votre cas d'utilisation professionnel.
- L'ensemble de la configuration, qui inclut, sans s'y limiter, les points de terminaison d'API et le provisionnement et la suppression des locataires du backend à l'aide d'AWS CloudFormation, ne couvre que le cas de base du happy path. Évaluez et mettez à jour la configuration avec la logique de nouvelle tentative nécessaire, la logique de gestion des erreurs supplémentaire et la logique de sécurité en fonction des besoins de votre entreprise.
- L'exemple de code est testé avec up-to-date cdk-nag pour vérifier les politiques au moment de la rédaction de cet article. De nouvelles politiques pourraient être appliquées à l'avenir. Ces nouvelles politiques peuvent vous obliger à modifier manuellement la pile en fonction des recommandations avant que la pile ne puisse être déployée. Passez en revue le code existant pour vous assurer qu'il correspond aux exigences de votre entreprise.
- Le code s'appuie sur le CDK AWS pour générer un suffixe aléatoire au lieu de s'appuyer sur des noms physiques assignés de manière statique pour la plupart des ressources créées. Cette configuration permet de garantir que ces ressources sont uniques et n'entrent pas en conflit avec d'autres piles. Pour plus d'informations, consultez la documentation AWS CDK. Ajustez cela en fonction des besoins de votre entreprise.
- Cet exemple de code regroupe les artefacts .NET Lambda dans des images basées sur Docker et s'exécute avec le moteur d'exécution d'images Container fourni par Lambda. L'environnement d'exécution de l'image du conteneur présente des avantages pour les mécanismes de transfert et de stockage standard (registres de conteneurs) et pour les environnements de test locaux plus précis (via l'image du conteneur). Vous pouvez modifier le projet pour utiliser les environnements d'exécution .NET fournis par Lambda afin de réduire le temps de génération des images Docker, mais vous devrez ensuite configurer les mécanismes de transfert et de stockage et vous assurer que la configuration locale correspond à la configuration Lambda. Ajustez le code pour l'aligner sur les exigences commerciales des utilisateurs.

Versions du produit

- AWS CDK version 2.45.0 ou ultérieure
- Visual Studio 2022

Architecture

Pile technologique

- Amazon API Gateway
- AWS CloudFormation
- Amazon CloudWatch
- Amazon DynamoDB
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS

Architecture

Le schéma suivant montre le flux de création de la pile de locataires. Pour plus d'informations sur les piles technologiques du plan de contrôle et des locataires, consultez la section Informations supplémentaires.

Flux de création d'une pile de locataires

1. L'utilisateur envoie une demande d'API POST avec la nouvelle charge utile du locataire (nom du locataire, description du locataire) au format JSON à une API REST hébergée par Amazon API Gateway. L'API Gateway traite la demande et la transmet à la fonction principale Lambda Tenant Onboarding. Dans cet exemple, il n'y a aucune autorisation ni authentification. Dans une configuration de production, cette API doit être intégrée au système de sécurité de l'infrastructure SaaS.
2. La fonction d'intégration des locataires vérifie la demande. Il tente ensuite de stocker l'enregistrement du locataire, qui inclut le nom du locataire, l'identifiant unique universel (UUID) généré et la description du locataire, dans la table d'intégration des locataires Amazon DynamoDB.
3. Une fois que DynamoDB a enregistré l'enregistrement, un flux DynamoDB lance la fonction Lambda Tenant Infrastructure en aval.

4. La fonction Lambda de l'infrastructure Tenant agit en fonction du flux DynamoDB reçu. Si le flux est destiné à l'événement INSERT, la fonction utilise la NewImage section du flux (dernier enregistrement de mise à jour, champ Nom du tenant) CloudFormation pour créer une nouvelle infrastructure locataire à l'aide du modèle stocké dans le compartiment S3. Le CloudFormation modèle nécessite le paramètre Tenant Name.
5. AWS CloudFormation crée l'infrastructure du locataire en fonction du CloudFormation modèle et des paramètres d'entrée.
6. Chaque configuration de l'infrastructure du locataire comporte une CloudWatch alarme, une alarme de facturation et un événement d'alarme.
7. L'événement d'alarme devient un message envoyé à un sujet SNS, qui est chiffré par la clé AWS KMS du locataire.
8. La rubrique SNS transmet le message d'alarme reçu à la file d'attente SQS, qui est chiffrée par la clé de chiffrement AWS KMS du locataire.

D'autres systèmes peuvent être intégrés à Amazon SQS pour effectuer des actions en fonction des messages en file d'attente. Dans cet exemple, pour que le code reste générique, les messages entrants restent en file d'attente et doivent être supprimés manuellement.

Flux de suppression de la pile de locataires

1. L'utilisateur envoie une demande d'API DELETE avec la nouvelle charge utile du locataire (nom du locataire, description du locataire) au format JSON à l'API REST hébergée par Amazon API Gateway, qui traitera la demande et la transmettra à la fonction d'intégration des locataires. Dans cet exemple, il n'y a aucune autorisation ni authentification. Dans une configuration de production, cette API sera intégrée au système de sécurité de l'infrastructure SaaS.
2. La fonction d'intégration des locataires vérifiera la demande, puis tentera de supprimer le dossier du locataire (nom du locataire) de la table d'accueil des locataires.
3. Une fois que DynamoDB a correctement supprimé l'enregistrement (l'enregistrement existe dans la table et est supprimé), un flux DynamoDB lance la fonction Lambda Tenant Infrastructure en aval.
4. La fonction Lambda de l'infrastructure Tenant agit en fonction de l'enregistrement de flux DynamoDB reçu. Si le flux est destiné à l'événement REMOVE, la fonction utilise la OldImage section de l'enregistrement (informations sur l'enregistrement et champ Nom du locataire, avant la dernière modification, qui est la suppression) pour lancer la suppression d'une pile existante sur la base de ces informations d'enregistrement.
5. AWS CloudFormation supprime la pile de locataires cible en fonction de l'entrée.

Outils

Services AWS

- Amazon API Gateway vous aide à créer, publier, gérer, surveiller et sécuriser REST, HTTP, et ce, WebSocket APIs à n'importe quelle échelle.
- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS CDK Toolkit est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre application AWS Cloud Development Kit (AWS CDK).
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.

- AWS Toolkit for Visual Studio est un plugin pour l'environnement de développement intégré (IDE) Visual Studio. Le Toolkit for Visual Studio prend en charge le développement, le débogage et le déploiement d'applications .NET utilisant les services AWS.

Autres outils

- Visual Studio est un IDE qui inclut des compilateurs, des outils de complétion de code, des concepteurs graphiques et d'autres fonctionnalités qui prennent en charge le développement de logiciels.

Code

Le code de ce modèle se trouve dans le référentiel d'exemples APG d'intégration des locataires dans l'architecture SaaS pour Silo Model.

Épopées

Configuration d'AWS CDK

Tâche	Description	Compétences requises
Vérifiez l'installation de Node.js.	Pour vérifier que Node.js est installé sur votre ordinateur local, exécutez la commande suivante. `node --version`	Administrateur AWS, AWS DevOps
Installez le kit d'outils AWS CDK.	Pour installer AWS CDK Toolkit sur votre machine locale, exécutez la commande suivante. `npm install -g aws-cdk`	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	Si npm n'est pas installé, vous pouvez l'installer depuis le site Node.js.	
Vérifiez la version d'AWS CDK Toolkit.	Pour vérifier que la version d'AWS CDK Toolkit est correctement installée sur votre machine, exécutez la commande suivante. `cdk --version`	Administrateur AWS, AWS DevOps

Vérifiez le code du plan de contrôle d'embarquement du locataire

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le référentiel et naviguez jusqu'au `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example` dossier. Dans Visual Studio 2022, ouvrez la `\src\TenantOnboardingInfra.sln` solution. Ouvrez le `TenantOnboardingInfraStack.cs` fichier et examinez le code. Les ressources suivantes sont créées dans le cadre de cette pile :	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	• Tableau DynamoDB • Compartiment S3 (chargez le CloudFormation modèle dans le compartiment S3.) • Rôle d'exécution Lambda • fonction Lambda • API Gateway • Source d'événement de la fonction Lambda	
Passez en revue le CloudFormation modèle.	Dans le `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\template` dossier`infra.yaml` , ouvrez et examinez le CloudFormation modèle. Ce modèle sera hydraté avec le nom du locataire extrait de la table DynamoDB d'accueil du locataire. Le modèle fournit l'infrastructure spécifique au locataire. Dans cet exemple, il fournit la clé AWS KMS, Amazon SNS, Amazon SQS et l'alarme. CloudWatch	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
Passez en revue la fonction d'intégration des locataires.	Ouvrez `Function.cs` et examinez le code de la fonction d'intégration des locataires, qui est créée avec le modèle Visual Studio AWS Lambda Project (.NET Core-C#) avec le plan .NET 6 (Container Image). Ouvrez le `Dockerfile` et passez en revue le code. `Dockerfile` Il s'agit d'un fichier texte contenant des instructions pour créer l'image du conteneur Lambda. Notez que les NuGet packages suivants sont ajoutés en tant que dépendances au `TenantOnboardingFunction` projet : • `Amazon.Lambda.APIGatewayEvents` • `AWSSDK.DynamoDBv2` • `Newtonsoft.Json`	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
Passez en revue la InfraProvisioning fonction Tenant.	Accédez à `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\InfraProvisioningFunction` . Ouvrez `Function.cs` et examinez le code de la fonction de provisionnement de l'infrastructure locataire, qui est créé avec le modèle Visual Studio AWS Lambda Project (.NET Core- C#) avec le plan .NET 6 (Container Image). Ouvrez le `Dockerfile` et passez en revue le code. Notez que les NuGet packages suivants sont ajoutés en tant que dépendances au `InfraProvisioningFunction` projet : • `Amazon.Lambda.DynamoDBEvents` • `AWSSDK.DynamoDBv2` • `AWSSDK.Cloudformation`	Développeur d'applications, AWS DevOps

Déployer les ressources AWS

Tâche	Description	Compétences requises
Créez la solution.	Pour créer la solution, effectuez les opérations suivantes : 1. Dans Visual Studio 2022, ouvrez la `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra.sln` solution. 2. Ouvrez le menu contextuel (clic droit) de la solution, puis choisissez Créer une solution. **Note** Assurez-vous de mettre à jour le `Amazon.CDK.Lib` `NuGet` package avec la dernière version du `\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example\src\TenantOnboardingInfra`	Développeur d'applications

Tâche	Description	Compétences requises
	projet avant de créer la solution.	

Démarrez l'environnement AWS CDK.	Ouvrez l'invite de commande Windows et accédez au dossier racine de l'application AWS CDK dans lequel le `cdk.json` fichier est disponible (`\tenant-onboarding-in-saas-architecture-for-silo-model-apg-example`). Exécutez la commande suivante pour le démarrage.
	`cdk bootstrap`
	Si vous avez créé un profil AWS pour les informations d'identification, utilisez la commande avec votre profil.
	`cdk bootstrap --profile <profile name>`
		Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

Répertoriez les piles de CDK AWS.	Pour répertorier toutes les piles à créer dans le cadre de ce projet, exécutez la commande suivante.
	`cdk ls`
	`cdk ls --profile <profile name>`
	Si vous avez créé un profil AWS pour les informations d'identification, utilisez la commande avec votre profil.
	`cdk ls --profile <profile name>`
		Administrateur AWS, AWS DevOps

Vérifiez quelles ressources AWS seront créées.	Pour consulter toutes les ressources AWS qui seront créées dans le cadre de ce projet, exécutez la commande suivante.
	`cdk diff`
	Si vous avez créé un profil AWS pour les informations d'identification, utilisez la commande avec votre profil.
	`cdk diff --profile <profile name>`
		Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

Déployez toutes les ressources AWS à l'aide d'AWS CDK.	Pour déployer toutes les ressources AWS, exécutez la commande suivante.
	`cdk deploy --all --require-approval never`
	Si vous avez créé un profil AWS pour les informations d'identification, utilisez la commande avec votre profil.
	`cdk deploy --all --require-approval never --profile <profile name>`
	Une fois le déploiement terminé, copiez l'URL de l'API depuis la section des sorties de l'invite de commande, comme illustré dans l'exemple suivant.
	`Outputs: TenantOnboardingInfraStack.TenantOnboardingAPIEndpoint42E526D7 = https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/`
		Administrateur AWS, AWS DevOps

Vérifiez la fonctionnalité

Tâche	Description	Compétences requises

Créez un nouveau locataire.	Pour créer le nouveau locataire, envoyez la demande curl suivante.
	`curl -X POST <TenantOnboardingAPIEndpoint* from CDK Output>tenant -d '{"Name":"Tenant123", "Description":"Stack for Tenant123"}'`
	Remplacez l'espace `<TenantOnboardingAPIEndpoint* from CDK Output>` réservé par la valeur réelle d'AWS CDK, comme indiqué dans l'exemple suivant.
	`curl -X POST https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant -d '{"Name": "Tenant123", "Description":"test12"}'`
	L'exemple suivant montre le résultat.
	`{"message": "A new tenant added - 5/4/2022 7:11:30 AM"}`
		Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
Vérifiez les informations du locataire nouvellement créé dans DynamoDB.	Pour vérifier les informations du locataire nouvellement créé dans DynamoDB, effectuez les étapes suivantes. 1. Ouvrez AWS Management Console et accédez au service Amazon DynamoDB. 2. Dans le menu de navigation de gauche, choisissez Explorer les éléments, puis choisissez le `TenantOnboarding` tableau. **Note** Le nom du locataire sera précédé de. `tenantcluster-` Pour plus d'informations, consultez la section Informations supplémentaires. 3. Vérifiez qu'un nouvel article est créé avec les informations du locataire.	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
Vérifiez la création de la pile pour le nouveau locataire.	Vérifiez que la nouvelle pile a été créée avec succès et dotée d'une infrastructure pour le locataire nouvellement créé conformément au CloudFormation modèle. 1. Ouvrez la CloudFormation console. 2. Dans le volet de navigation de gauche, choisissez Stacks et vérifiez qu'une pile portant le nom du locataire a été créée avec succès. 3. Choisissez la pile de locataires nouvellement créée, puis choisissez l'onglet Ressources. Notez la ressource d'alarme et la ressource Amazon SQS. 4. Ouvrez un nouveau terminal avec les informations d'identification AWS configurées et pointez sur la bonne région. Pour déclencher une alarme de test, entrez le code suivant, en le `<alarm resource name>` remplaçant par le nom de la ressource d'alarme indiqué à l'étape 3.	Développeur d'applications, administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises

	`aws cloudwatch set-alarm-state --alarm-name <alarm resource name> --state-value ALARM --state-reason 'Test setup'`
	
	L'exemple suivant montre le code avec un nom de ressource d'alarme.
	
	`aws cloudwatch set-alarm-state --alarm-name tenantcluster-tenant123-alarm --state-value ALARM --state-reason 'Test setup'`
	
	5. Ouvrez la console et accédez à la console Amazon SQS. Choisissez le nom de ressource Amazon SQS identifié à l'étape 3. Suivez les instructions de la documentation AWS pour recevoir et supprimer le message de test de l'alarme déclenchée à l'étape 4.	

Tâche	Description	Compétences requises

Supprimez la pile de locataires.	Pour supprimer la pile de locataires, envoyez la demande curl suivante.
	
	`curl -X DELETE <TenantOnboardingAPIEndpoint* from CDK Output>tenant/<Tenant Name from previous step>`
	
	Remplacez l'espace `<TenantOnboardingAPIEndpoint* from CDK Output>` réservé par la valeur réelle d'AWS CDK, puis par la valeur réelle de l'étape précédente de création du locataire, comme indiqué dans l'exemple suivant. `<Tenant Name from previous step>`
	
	`curl -X DELETE https://j2qmp8ds21i1i.execute-api.us-west-2.amazonaws.com/prod/tenant/Tenant123`
	
	L'exemple suivant montre le résultat.
	
	`{"message": "Tenant destroyed - 5/4/2022 7:14:48 AM"}`
		Développeur d'applications, AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises
Vérifiez la suppression de la pile pour le locataire existant.	Pour vérifier que la pile de locataires existante a été supprimée, effectuez les étapes suivantes : 1. Ouvrez la console et naviguez jusqu'à la CloudFormation console. 2. Dans le volet de navigation de gauche, vérifiez que la pile existante portant le nom du locataire n'est plus dans la CloudFormation console (si la console est configurée pour afficher uniquement les piles actives) ou qu'elle est en cours de suppression. Si la pile ne se trouve plus dans la CloudFormation console, utilisez la liste déroulante pour modifier le paramètre de la console de Actif à Supprimé afin de voir la pile supprimée et de vérifier qu'elle a bien été supprimée .	Développeur d'applications, administrateur AWS, AWS DevOps

Nettoyage

Tâche	Description	Compétences requises
Détruisez l'environnement.	Avant le nettoyage de la pile, assurez-vous de ce qui suit :	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	• Tous les enregistrements de DynamoDB sont supprimés soit par le biais de l'opération de suppression du locataire précédente, soit par le biais de la console ou de l'API DynamoDB. Chaque suppression d'enregis trement de locataire initiera le nettoyage de son CloudFormation équivalent AWS. • Toutes les CloudFormation piles AWS basées sur des locataires sont nettoyées (au cas où la logique de nettoyage du déclencheur DynamoDB échouerait) sur la console AWS. CloudForm ation Une fois les tests effectués , AWS CDK peut être utilisé pour détruire toutes les piles et les ressources associées en exécutant la commande suivante. `cdk destroy --all;` Si vous avez créé un profil AWS pour les informations d'identification, utilisez-le.	

Tâche	Description	Compétences requises
	Confirmez l'invite de suppression de la pile pour supprimer la pile.	
Nettoyez Amazon CloudWatch Logs.	Le processus de suppression de la pile ne nettoie pas CloudWatch les journaux (groupes de journaux et journaux) générés par la pile. Nettoyez manuellement les CloudWatch ressources à l'aide de la CloudWatch console ou de l'API.	Développeur d'applications, AWS DevOps, administrateur AWS

Ressources connexes

- Atelier AWS CDK .NET
- Utilisation du kit AWS CDK en C#
- Référence CDK .NET

Informations supplémentaires

Pile technologique de plan de contrôle

Le code CDK écrit en .NET est utilisé pour approvisionner l'infrastructure du plan de contrôle, qui comprend les ressources suivantes :

1. API Gateway

   Sert de point d'entrée de l'API REST pour la pile du plan de contrôle.
2. Intégration des locataires à la fonction Lambda

   Cette fonction Lambda est initiée par API Gateway à l'aide de la méthode m.

   Une demande d'API de méthode POST entraîne l'insertion de (`tenant name`,`tenant description`) dans la table `Tenant Onboarding` DynamoDB.

Dans cet exemple de code, le nom du tenant est également utilisé dans le cadre du nom de la pile de locataires et des noms des ressources de cette pile. Cela permet de faciliter l'identification de ces ressources. Ce nom de locataire doit être unique dans l'ensemble de la configuration pour éviter les conflits ou les erreurs. La configuration détaillée de la validation des entrées est expliquée dans la documentation des rôles IAM et dans la section Limitations.

Le processus de persistance de la table DynamoDB n'aboutira que si le nom du locataire n'est utilisé dans aucun autre enregistrement de la table.

Dans ce cas, le nom du locataire est la clé de partition de cette table, car seule la clé de partition peut être utilisée comme expression de `PutItem` condition.

Si le nom du locataire n'a jamais été enregistré auparavant, l'enregistrement sera correctement enregistré dans la table.

Toutefois, si le nom du locataire est déjà utilisé par un enregistrement existant dans la table, l'opération échouera et déclenchera une exception `ConditionalCheckFailedException` DynamoDB. L'exception sera utilisée pour renvoyer un message d'échec (`HTTP BadRequest`) indiquant que le nom du locataire existe déjà.

Une demande d'API de `DELETE` méthode supprimera l'enregistrement d'un nom de locataire spécifique de la table `Tenant Onboardin` g.

Dans cet exemple, la suppression de l'enregistrement DynamoDB réussira même si l'enregistrement n'existe pas.

Si l'enregistrement cible existe et est supprimé, il créera un enregistrement de flux DynamoDB. Dans le cas contraire, aucun enregistrement en aval ne sera créé.

3. Intégration du locataire à DynamoDB, avec Amazon DynamoDB Streams activé

   Cela enregistre les informations de métadonnées du locataire, et toute sauvegarde ou suppression d'enregistrement enverra un flux en aval à la fonction `Tenant Infrastructure` Lambda.

4. Fonction Lambda de l'infrastructure locataire

   Cette fonction Lambda est initiée par l'enregistrement de flux DynamoDB de l'étape précédente. Si l'enregistrement concerne un `INSERT` événement, il invoque AWS CloudFormation pour créer une nouvelle infrastructure locataire avec le CloudFormation modèle stocké dans un compartiment

S3. Si l'enregistrement est pour`REMOVE`, il initie la suppression d'une pile existante en fonction du `Tenant Name` champ de l'enregistrement du flux.

5. Compartiment S3

   C'est pour stocker le CloudFormation modèle.

6. Des rôles IAM pour chaque fonction Lambda et un rôle de service pour CloudFormation

   Chaque fonction Lambda possède un rôle IAM unique avec des autorisations de moindre privilège pour accomplir sa tâche. Par exemple, la fonction `Tenant On-boarding` Lambda dispose d'un accès en lecture/écriture à DynamoDB, et la fonction `Tenant Infrastructure` Lambda ne peut lire que le flux DynamoDB.

   Un rôle CloudFormation de service personnalisé est créé pour le provisionnement de la pile des locataires. Ce rôle de service contient des autorisations supplémentaires pour le provisionnement des CloudFormation piles (par exemple, la clé AWS KMS). Cela permet de répartir les rôles entre Lambda et d' CloudFormation éviter toutes les autorisations sur un seul rôle (rôle Lambda d'infrastructure).

   Les autorisations qui autorisent des actions puissantes (telles que la création et la suppression de CloudFormation piles) sont verrouillées et autorisées uniquement sur les ressources commençant `tenantcluster-` par. L'exception est AWS KMS, en raison de sa convention de dénomination des ressources. Le nom du locataire ingéré provenant de l'API sera ajouté au début, `tenantcluster-` ainsi que d'autres contrôles de validation (alphanumérique avec tiret uniquement, et limité à moins de 30 caractères pour s'adapter à la plupart des noms de ressources AWS). Cela garantit que le nom du locataire n'entraînera pas accidentellement une perturbation des infrastructures ou des ressources de base.

Pile technologique pour locataires

Un CloudFormation modèle est stocké dans le compartiment S3. Le modèle fournit la clé AWS KMS spécifique au locataire, une CloudWatch alarme, une rubrique SNS, une file d'attente SQS et une politique SQS.

La clé AWS KMS est utilisée pour le chiffrement des données par Amazon SNS et Amazon SQS pour leurs messages. Les pratiques de sécurité pour AwsSolutions- SNS2 et AwsSolutions - vous SQS2 recommandent de configurer Amazon SNS et Amazon SQS avec le chiffrement. Toutefois, les CloudWatch alarmes ne fonctionnent pas avec Amazon SNS lorsque vous utilisez une clé gérée par

AWS. Dans ce cas, vous devez utiliser une clé gérée par le client. Pour plus d'informations, consultez le centre de connaissances AWS.

La politique SQS est utilisée dans la file d'attente Amazon SQS pour permettre à la rubrique SNS créée de transmettre le message à la file d'attente. Sans la politique SQS, l'accès sera refusé. Pour plus d'informations, consultez la documentation Amazon SNS.

Décomposez les monolithes en microservices en utilisant le CQRS et le sourcing d'événements

Créée par Rodolfo Jr. Cerrada (AWS), Dmitry Gulin (AWS) et Tabby Ward (AWS)

Récapitulatif

Ce modèle combine deux modèles, en utilisant à la fois le modèle de séparation des responsabilités des requêtes de commande (CQRS) et le modèle de source d'événements. Le modèle CQRS sépare les responsabilités des modèles de commande et de requête. Le modèle d'approvisionnement en événements tire parti de la communication asynchrone axée sur les événements pour améliorer l'expérience utilisateur globale.

Vous pouvez utiliser les services CQRS et Amazon Web Services (AWS) pour gérer et dimensionner chaque modèle de données indépendamment tout en refactorisant votre application monolithe en architecture de microservices. Vous pouvez ensuite utiliser le modèle d'origine des événements pour synchroniser les données de la base de commandes vers la base de données de requêtes.

Ce modèle utilise un exemple de code qui inclut un fichier de solution (*.sln) que vous pouvez ouvrir à l'aide de la dernière version de Visual Studio. L'exemple contient le code de l'API Reward pour montrer comment le CQRS et le sourcing d'événements fonctionnent dans les applications AWS sans serveur, traditionnelles ou sur site.

Pour en savoir plus sur le CQRS et le sourcing événementiel, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Amazon CloudWatch
- Tables Amazon DynamoDB
- Amazon DynamoDB Streams
- Clé d'accès et clé secrète d'AWS Identity and Access Management (IAM) ; pour plus d'informations, regardez la vidéo dans la section Ressources connexes
- AWS Lambda
- Connaissance de Visual Studio

- Connaissance d'AWS Toolkit for Visual Studio ; pour plus d'informations, consultez la vidéo de démonstration d'AWS Toolkit for Visual Studio dans la section Ressources connexes

Versions du produit

- Édition communautaire de Visual Studio 2019.
- Boîte à outils AWS pour Visual Studio 2019.
- .NET Core 3.1. Ce composant est une option de l'installation de Visual Studio. Pour inclure .NET Core lors de l'installation, sélectionnez NET Core cross-platform development.

Limites

- L'exemple de code pour une application locale traditionnelle (API Web ASP.NET Core et objets d'accès aux données) n'est pas fourni avec une base de données. Cependant, il est fourni avec l'objet `CustomerData` en mémoire, qui agit comme une base de données fictive. Le code fourni est suffisant pour que vous puissiez tester le modèle.

Architecture

Pile technologique source

- Projet d'API Web ASP.NET Core
- Serveur Web IIS
- Objet d'accès aux données
- Modèle CRUD

Architecture source

Dans l'architecture source, le modèle CRUD contient à la fois des interfaces de commande et de requête dans une seule application. Pour un exemple de code, voir `CustomerDA0.cs` (ci-joint).

Pile technologique cible

- Amazon DynamoDB
- Amazon DynamoDB Streams

- AWS Lambda
- (Facultatif) Amazon API Gateway
- (Facultatif) Amazon Simple Notification Service (Amazon SNS)

Architecture cible

Dans l'architecture cible, les interfaces de commande et de requête sont séparées. L'architecture illustrée dans le schéma suivant peut être étendue avec API Gateway et Amazon SNS. Pour plus d'informations, consultez la section Informations supplémentaires.

1. Les fonctions Command Lambda exécutent des opérations d'écriture, telles que la création, la mise à jour ou la suppression, sur la base de données.
2. Les fonctions Query Lambda exécutent des opérations de lecture, telles que get ou select, sur la base de données.
3. Cette fonction Lambda traite les flux DynamoDB à partir de la base de données de commandes et met à jour la base de données Query en fonction des modifications.

Outils

Outils

- Amazon DynamoDB — Amazon DynamoDB est un service de base de données NoSQL entièrement géré qui fournit des performances rapides et prévisibles ainsi qu'une évolutivité sans faille.
- Amazon DynamoDB Streams — DynamoDB Streams capture une séquence chronologique de modifications au niveau des éléments dans n'importe quelle table DynamoDB. Il enregistre ensuite ces informations dans un journal pendant 24 heures au maximum. Le chiffrement au repos chiffre les données dans les flux DynamoDB Streams.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- AWS Management Console — L'AWS Management Console est une application Web qui comprend un large éventail de consoles de service pour gérer les services AWS.

- Visual Studio 2019 Community Edition — Visual Studio 2019 est un environnement de développement intégré (IDE). L'édition communautaire est gratuite pour les contributeurs open source. Dans ce modèle, vous utiliserez Visual Studio 2019 Community Edition pour ouvrir, compiler et exécuter un exemple de code. Pour l'affichage uniquement, vous pouvez utiliser n'importe quel éditeur de texte ou Visual Studio Code.
- AWS Toolkit for Visual Studio — Le kit AWS Toolkit pour Visual Studio est un plugin pour l'IDE Visual Studio. L'AWS Toolkit for Visual Studio facilite le développement, le débogage et le déploiement d'applications .NET utilisant les services AWS.

Code

L'exemple de code est joint. Pour obtenir des instructions sur le déploiement de l'exemple de code, consultez la section Epics.

Épopées

Ouvrez et créez la solution

Tâche	Description	Compétences requises
Ouvrez la solution.	1. Téléchargez l'exemple de code source (`CQRS-ES Code.zip`) depuis la section Pièces jointes et extrayez les fichiers. 2. Dans l'IDE Visual Studio, choisissez Fichier, Ouvrir, Solution de projet, puis accédez au dossier dans lequel vous avez extrait le code source. 3. Choisissez AWS.APG.CQRSES.sln, puis Open. La solution complète est chargée dans Visual Studio.	Développeur d’applications

Tâche	Description	Compétences requises
Créez la solution.	Ouvrez le menu contextuel (clic droit) de la solution, puis choisissez Build Solution. Cela permettra de créer et de compiler tous les projets de la solution. Il devrait être compilé avec succès. L'explorateur de solutions Visual Studio doit afficher la structure du répertoire. • `CQRS On-Premises Code Sample`contient un exemple d'utilisation du CQRS sur site. • `CQRS AWS Serverless` contient tous les exemples de code CQRS et de sourcing d'événements utilisant les services sans serveur AWS.	Développeur d’applications

Création des tables DynamoDB

Tâche	Description	Compétences requises
Fournissez des informations d'identification.	Si vous n'avez pas encore de clé d'accès, regardez la vidéo dans la section Ressources connexes. 1. Dans l'explorateur de solutions, développez CQRS AWS Serverless,	Développeur d'applications, ingénieur de données, DBA

Tâche	Description	Compétences requises
	puis développez le dossier Build solution. 2. Développez le projet aws.apg.cqrses.build et visualisez le fichier. `Program.cs` 3. Faites défiler l'écran vers le haut `Program.cs` et recherchez`Program()` . 4. `YOUR ACCESS KEY`Remplacez-la par la clé d'accès à votre compte et `YOUR SECRET KEY` remplacez-la par la clé secrète de votre compte. Notez que dans un environnement de production, vous ne devez pas coder vos clés en dur. Vous pouvez plutôt utiliser AWS Secrets Manager pour stocker et récupérer les informations d'identification.	
Générez le projet.	Pour créer le projet, ouvrez le menu contextuel (clic droit) du projet aws.apg.cqrses.build, puis choisissez Build.	Développeur d'applications, ingénieur de données, DBA

Tâche	Description	Compétences requises
Créez et remplissez les tables.	Pour créer les tables et les remplir avec des données de départ, ouvrez le menu contextuel (clic droit) du projet aws.apg.cqrses.build, puis choisissez Debug, Start New Instance.	Développeur d'applications, ingénieur de données, DBA
Vérifiez la construction de la table et les données.	Pour vérifier, accédez à AWS Explorer et développe z Amazon DynamoDB. Il doit afficher les tableaux. Ouvrez chaque table pour afficher les exemples de données.	Développeur d'applications, ingénieur de données, DBA

Exécuter des tests locaux

Tâche	Description	Compétences requises
Construisez le projet CQRS.	1. Ouvrez la solution et accédez au dossier de la Services/CQRS/Tests solution CQRS AWS. 2. Dans le fichier AWS.APG.C QRSES. CQRSLambd a.Teste le projet, ouvrez BaseFunctionTest.cs et remplacez AccessKeyet par SecretKeyles clés IAM que vous avez créées. 3. Enregistrez les Modificat ions. 4. Pour compiler et créer le projet de test, ouvrez le	Développeur d'applications, ingénieur de test

Tâche	Description	Compétences requises
	menu contextuel (clic droit) du projet, puis choisissez Construire.	
Construisez le projet d'approvisionnement en événements.	1. Accédez au dossier de la Services/Event Source/Tests solution AWS CQRS. 2. Dans le fichier AWS.APG.CQRSES. EventSourceLambda.Teste le projet, ouvrez BaseFunctionTest.cs et remplacez AccessKey et par SecretKeyles clés IAM que vous avez créées. 3. Enregistrez les Modifications. 4. Pour compiler et créer le projet de test, ouvrez le menu contextuel (clic droit) du projet, puis choisissez Construire.	Développeur d'applications, ingénieur de test
Exécutez les tests.	Pour exécuter tous les tests, choisissez Afficher, Explorateur de tests, puis sélectionnez Exécuter tous les tests en mode Affichage. Tous les tests doivent réussir, ce qui est indiqué par une icône en forme de coche verte.	Développeur d'applications, ingénieur de test

Publiez les fonctions Lambda du CQRS sur AWS

Tâche	Description	Compétences requises
Publiez la première fonction Lambda.	1. Dans l'Explorateur de solutions, ouvrez le menu contextuel (clic droit) du fichier AWS.APG.CQRSES. CommandCreateLambd a projet, puis choisissez Publier sur AWS Lambda. 2. Sélectionnez le profil que vous souhaitez utiliser, la région AWS dans laquelle vous souhaitez déployer la fonction Lambda, ainsi que le nom de la fonction. 3. Pour les autres champs, conservez les valeurs par défaut et choisissez Next. 4. Dans la liste déroulante Nom du rôle, sélectionnez AWSLambdaFullAccess. 5. Pour fournir vos clés de compte, choisissez Ajouter, puis entrez `AcessKey` comme variable et votre clé d'accès comme valeur. Choisissez ensuite à nouveau Ajouter, entrez `SecretKey` comme variable et votre clé secrète comme valeur. 6. Pour les autres champs, conservez les valeurs par défaut et choisissez Upload.	Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises
	Une fois la fonction de test Lambda chargée, elle apparaît automatiquement dans Visual Studio. 7. Répétez les étapes 1 à 6 pour les projets suivants : • AWS.APG.CARSES.CommandDeleteLambda • AWS.APG.CARSES.CommandUpdateLambda • AWS.APG.CARSES.CommandAddRewardLambda • AWS.APG.CARSES.CommandRedeemRewardLambda • AWS.APG.CARSES.QueryCustomerListLambda • AWS.APG.CARSES.QueryRewqardLambda	
Vérifiez le téléchargement de la fonction.	(Facultatif) Vous pouvez vérifier que la fonction a été correctement chargée en accédant à AWS Explorer et en développant AWS Lambda. Pour ouvrir la fenêtre de test, choisissez la fonction Lambda (double-clic).	Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises
Testez la fonction Lambda.	1. Entrez les données de la demande ou copiez un exemple de données de demande à partir des données de test dans la section Informations supplémentaires. Assurez-vous de sélectionner les données correspondant à la fonction que vous testez. 2. Pour exécuter le test, choisissez Invoquer. La réponse et les erreurs éventuelles sont affichées dans la zone de texte Réponse, et les journaux sont affichés dans la zone de texte Journaux ou dans CloudWatch Journaux. 3. Pour vérifier les données, dans AWS Explorer, choisissez la table DynamoDB (double-cliquez). Tous les projets Lambda du CQRS se trouvent dans `CQRS AWS Serverless\CQRS \Command Microservice` les dossiers `CQRS AWS Serverless\CQRS\Command Microservice` et solution. Pour le répertoire des solutions et les projets,	Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises
	voir Répertoire du code source dans la section Informations supplémentaires.	
Publiez les fonctions restantes .	Répétez les étapes précédentes pour les projets suivants : • AWS.APG.CARSES.CommandDeleteLambda • AWS.APG.CARSES.CommandUpdateLambda • AWS.APG.CARSES.CommandAddRewardLambda • AWS.APG.CARSES.CommandRedeemRewardLambda • AWS.APG.CARSES.QueryCustomerListLambda • AWS.APG.CARSES.QueryRewqardLambda	Développeur d'applications, DevOps ingénieur

Configurer la fonction Lambda en tant qu'écouteur d'événements

Tâche	Description	Compétences requises
Publiez les gestionnaires d'événements Lambda destinés aux clients et aux récompenses.	Pour publier chaque gestionnaire d'événements, suivez les étapes décrites dans l'épopée précédente. Les projets se trouvent dans les dossiers `CQRS AWS Serverless\Event`	Développeur d’applications

Tâche	Description	Compétences requises
	`Source\Customer Event` et `CQRS AWS Serverless \Event Source\Reward Event` solutions. Pour plus d'informations, consultez le répertoire du code source dans la section Informations supplémentaires.	

Tâche	Description	Compétences requises
Joignez l'écouteur d'événements Lambda de source d'événements.	1. Connectez-vous à l'AWS Management Console en utilisant le même compte que celui que vous utilisez lorsque vous publiez les projets Lambda. 2. Pour la région, sélectionnez US East 1 ou la région dans laquelle vous avez déployé les fonctions Lambda dans l'épopée précédente. 3. Accédez au service Lambda. 4. Sélectionnez la fonction `EventSourceCustomer` Lambda. 5. Choisissez Ajouter un déclencheur. 6. Dans la liste déroulante Configuration du déclencheur, sélectionnez DynamoDB. 7. Dans la liste déroulante du tableau DynamoDB, sélectionnez. cqrses-customer-cmd 8. Dans la liste déroulante Position de départ, sélectionnez Découper l'horizon à partir de. Le découpage de l'horizon signifie que le déclencheur DynamoDB commence	Développeur d’applications

Tâche	Description	Compétences requises
	à lire le dernier enregistrement de flux (non découpé), qui est le plus ancien enregistrement de la partition. 9. Cochez la case Activer le déclencheur. 10. Pour les autres champs, conservez les valeurs par défaut et choisissez Ajouter. Une fois que l'écouteur est correctement attaché à la table DynamoDB, il s'affiche sur la page du concepteur Lambda.	
Publiez et attachez la fonction EventSourceReward Lambda.	Pour publier et associer la fonction `EventSourceReward` Lambda, répétez les étapes décrites dans les deux articles précédents, en sélectionnant dans la liste déroulante cqrses-reward-cmddu tableau DynamoDB.	Développeur d’applications

Testez et validez les flux DynamoDB et le déclencheur Lambda

Tâche	Description	Compétences requises
Testez le flux et le déclencheur Lambda.	1. Dans Visual Studio, accédez à AWS Explorer. 2. Développez AWS Lambda et choisissez la	Développeur d’applications

Tâche	Description	Compétences requises
	CommandRedeemRewardfonction (double-cliquez). Dans la fenêtre de fonction qui s'ouvre, vous pouvez tester la fonction. 3. Dans la zone de texte Demande, entrez les données de la demande au format JSON (JavaScript Object Notation). Pour un exemple de demande, voir Données de test dans la section Informations supplémentaires. 4. Sélectionnez Invoquer .	
Validez à l'aide de la table de requêtes de récompenses DynamodDB.	1. Ouvrez la cqrses-reward-querytable. 2. Vérifiez les points du client qui a utilisé la récompense. Les points échangés doivent être soustraits du total des points cumulés du client.	Développeur d’applications

Tâche	Description	Compétences requises
Validez à l'aide CloudWatch des journaux.	1. Accédez aux groupes de journaux CloudWatch et choisissez-les. 2. Le groupe/aws/lambda/EventSourceRewardlog contient les journaux du `EventSourceReward` déclencheur. Tous les appels Lambda sont enregistrés, y compris les messages que vous avez placés dans `context.Logger.LogLine` et `Console.Writeline` dans le code Lambda.	Développeur d’applications
Validez le EventSourceCustomer déclencheur.	Pour valider le `EventSourceCustomer` déclencheur, répétez les étapes de cette épopée en utilisant le tableau des clients et les CloudWatch journaux correspondants du `EventSourceCustomer` déclencheur.	Développeur d’applications

Ressources connexes

Références

- Téléchargements de Visual Studio 2019 Community Edition
- Téléchargement d'AWS Toolkit pour Visual Studio
- Guide de l'utilisateur d'AWS Toolkit pour Visual Studio
- Sans serveur sur AWS
- Cas d'utilisation et modèles de conception de DynamoDB

- Martin Fowler CQRS
- Martin Fowler Recherche d'événements

Vidéos

- Démo d'AWS Toolkit pour Visual Studio
- Comment créer un identifiant de clé d'accès pour un nouvel utilisateur IAM ?

Informations supplémentaires

CQRS et approvisionnement événementiel

CARS

Le modèle CQRS sépare un modèle d'opérations conceptuel unique, tel qu'un modèle CRUD (création, lecture, mise à jour, suppression) d'un objet d'accès aux données, en modèles d'opérations de commande et de requête. Le modèle de commande fait référence à toute opération, telle que la création, la mise à jour ou la suppression, qui modifie l'état. Le modèle de requête fait référence à toute opération qui renvoie une valeur.

1. Le modèle Customer CRUD inclut les interfaces suivantes :
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`

Au fur et à mesure que vos exigences se complexifient, vous pouvez abandonner cette approche à modèle unique. Le CQRS utilise un modèle de commande et un modèle de requête pour séparer les responsabilités d'écriture et de lecture des données. Ainsi, les données peuvent être maintenues et gérées de manière indépendante. Grâce à une séparation claire des responsabilités, les

améliorations apportées à chaque modèle n'ont aucune incidence sur l'autre. Cette séparation améliore la maintenance et les performances et réduit la complexité de l'application à mesure qu'elle grandit.

1. Interfaces dans le modèle de commande client :
   - `Create Customer()`
   - `UpdateCustomer()`
   - `DeleteCustomer()`
   - `AddPoints()`
   - `RedeemPoints()`
2. Interfaces dans le modèle de requête client :
   - `GetVIPCustomers()`
   - `GetCustomerList()`
   - `GetCustomerPoints()`
   - `GetMonthlyStatement()`

Pour un exemple de code, voir Répertoire du code source.

Le modèle CQRS découple ensuite la base de données. Ce découplage conduit à l'indépendance totale de chaque service, qui est l'ingrédient principal de l'architecture des microservices.

En utilisant le CQRS dans le cloud AWS, vous pouvez optimiser davantage chaque service. Par exemple, vous pouvez définir différents paramètres de calcul ou choisir entre un microservice sans serveur ou un microservice basé sur des conteneurs. Vous pouvez remplacer votre mise en cache sur site par Amazon. ElastiCache Si vous disposez d'un message de publication/d'abonnement sur site, vous pouvez le remplacer par Amazon Simple Notification Service (Amazon SNS). En outre, vous pouvez profiter de la pay-as-you-go tarification et de la vaste gamme de services AWS selon lesquels vous ne payez que pour ce que vous utilisez.

Le CQRS inclut les avantages suivants :

- Mise à l'échelle indépendante : la stratégie de mise à l'échelle de chaque modèle peut être ajustée pour répondre aux exigences et à la demande du service. Comme pour les applications hautes performances, la séparation de la lecture et de l'écriture permet au modèle d'évoluer

indépendamment pour répondre à chaque demande. Vous pouvez également ajouter ou réduire des ressources de calcul pour répondre à la demande d'évolutivité d'un modèle sans affecter l'autre.

- Maintenance indépendante : la séparation des modèles de requête et de commande améliore la maintenabilité des modèles. Vous pouvez apporter des modifications et des améliorations au code d'un modèle sans affecter l'autre.
- Sécurité — Il est plus facile d'appliquer les autorisations et les politiques à des modèles distincts pour la lecture et l'écriture.
- Lectures optimisées : vous pouvez définir un schéma optimisé pour les requêtes. Par exemple, vous pouvez définir un schéma pour les données agrégées et un schéma distinct pour les tables de faits.
- Intégration — Le CQRS s'adapte parfaitement aux modèles de programmation basés sur les événements.
- Complexité gérée — La séparation en modèles de requête et de commande convient aux domaines complexes.

Lorsque vous utilisez le CQRS, gardez à l'esprit les mises en garde suivantes :

- Le modèle CQRS ne s'applique qu'à une partie spécifique d'une application et non à l'ensemble de l'application. Si elle est mise en œuvre dans un domaine qui ne correspond pas au modèle, elle peut réduire la productivité, augmenter les risques et introduire de la complexité.
- Le modèle fonctionne mieux pour les modèles fréquemment utilisés dont les opérations de lecture et d'écriture sont déséquilibrées.
- Pour les applications nécessitant beaucoup de lecture, telles que les rapports volumineux dont le traitement prend du temps, le CQRS vous permet de sélectionner la bonne base de données et de créer un schéma pour stocker vos données agrégées. Cela améliore le temps de réponse lors de la lecture et de l'affichage du rapport en traitant les données du rapport une seule fois et en les enregistrant dans le tableau agrégé.
- Pour les applications nécessitant beaucoup d'écriture, vous pouvez configurer la base de données pour les opérations d'écriture et autoriser le microservice de commande à évoluer indépendamment lorsque la demande d'écriture augmente. Pour des exemples, consultez les `AWS.APG.CQRSES.CommandAddRewardLambda` microservices `AWS.APG.CQRSES.CommandRedeemRewardLambda` et.

Approvisionnement d’événement

L'étape suivante consiste à utiliser la source d'événements pour synchroniser la base de données de requêtes lorsqu'une commande est exécutée. Par exemple, considérez les événements suivants :

- Un point de récompense client est ajouté, ce qui nécessite la mise à jour du total ou du cumul des points de récompense du client dans la base de données de requêtes.
- Le nom de famille d'un client est mis à jour dans la base de données de commandes, ce qui nécessite la mise à jour des informations du client de substitution dans la base de données de requêtes.

Dans le modèle CRUD traditionnel, vous garantissez la cohérence des données en verrouillant les données jusqu'à la fin d'une transaction. Lors de l'approvisionnement en événements, les données sont synchronisées grâce à la publication d'une série d'événements qui seront utilisés par un abonné pour mettre à jour ses données respectives.

Le modèle d'approvisionnement en événements garantit et enregistre une série complète d'actions entreprises sur les données et les publie par le biais d'une séquence d'événements. Ces événements représentent un ensemble de modifications apportées aux données que les abonnés à cet événement doivent traiter pour maintenir leur dossier à jour. Ces événements sont consommés par l'abonné, synchronisant les données de la base de données de l'abonné. Dans ce cas, il s'agit de la base de données de requêtes.

Le schéma suivant montre le sourcing d'événements utilisé avec CQRS sur AWS.

1. Les fonctions Command Lambda exécutent des opérations d'écriture, telles que la création, la mise à jour ou la suppression, sur la base de données.
2. Les fonctions Query Lambda exécutent des opérations de lecture, telles que get ou select, sur la base de données.
3. Cette fonction Lambda traite les flux DynamoDB à partir de la base de données de commandes et met à jour la base de données Query en fonction des modifications. Vous pouvez également utiliser cette fonction pour publier un message sur Amazon SNS afin que ses abonnés puissent traiter les données.
4. (Facultatif) L'abonné à l'événement Lambda traite le message publié par Amazon SNS et met à jour la base de données Query.
5. (Facultatif) Amazon SNS envoie une notification par e-mail concernant l'opération d'écriture.

Sur AWS, la base de données de requêtes peut être synchronisée par DynamoDB Streams. DynamoDB capture une séquence chronologique de modifications au niveau des éléments dans une table DynamoBDB en temps quasi réel et stocke les informations de manière durable dans les 24 heures.

L'activation de DynamoDB Streams permet à la base de données de publier une séquence d'événements qui rend possible le modèle d'approvisionnement des événements. Le modèle d'approvisionnement des événements ajoute l'abonné à l'événement. L'application d'abonnement à l'événement consomme l'événement et le traite sous la responsabilité de l'abonné. Dans le schéma précédent, l'abonné à l'événement envoie les modifications à la base de données Query DynamoDB afin de maintenir les données synchronisées. L'utilisation d'Amazon SNS, du courtier de messages et de l'application d'abonnement aux événements permet de découpler l'architecture.

Le sourcing événementiel inclut les avantages suivants :

- Cohérence des données transactionnelles
- Une piste d'audit fiable et un historique des actions, qui peuvent être utilisés pour surveiller les actions entreprises dans les données
- Permet aux applications distribuées telles que les microservices de synchroniser leurs données dans l'environnement
- Publication fiable des événements chaque fois que l'État change
- Reconstruire ou rejouer des états passés
- Entités faiblement couplées qui échangent des événements pour la migration d'une application monolithique vers des microservices
- Réduction des conflits provoqués par des mises à jour simultanées ; le sourcing d'événements évite de devoir mettre à jour les objets directement dans le magasin de données
- Flexibilité et extensibilité grâce au découplage de la tâche et de l'événement
- Mises à jour externes du système
- Gestion de plusieurs tâches en un seul événement

Lorsque vous utilisez le sourcing d'événements, gardez à l'esprit les mises en garde suivantes :

- En raison du retard dans la mise à jour des données entre les bases de données d'abonnés sources, le seul moyen d'annuler une modification est d'ajouter un événement compensateur au magasin d'événements.

- La mise en œuvre du sourcing d'événements a une courbe d'apprentissage en raison de son style de programmation différent.

Données de test

Utilisez les données de test suivantes pour tester la fonction Lambda après un déploiement réussi.

CommandCreate Client

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Done",  "CompanyName":"AnyCompany",
 "Address": "USA",  "VIP":true }
```

CommandUpdate Client

```
{  "Id":1501,  "Firstname":"John",  "Lastname":"Doe",  "CompanyName":"Example Corp.",
 "Address": "Seattle, USA",  "VIP":true }
```

CommandDelete Client

Entrez l'identifiant du client en tant que donnée de demande. Par exemple, si l'ID client est 151, entrez 151 comme données de demande.

```
151
```

QueryCustomerList

C'est vide. Lorsqu'il est invoqué, il renvoie tous les clients.

CommandAddReward

Cela ajoutera 40 points au client ayant l'ID 1 (Richard).

```
{
  "Id":10101,
  "CustomerId":1,
  "Points":40
}
```

CommandRedeemReward

Cela déduira 15 points au client ayant l'ID 1 (Richard).

```
{
  "Id":10110,
  "CustomerId":1,
  "Points":15
}
```

QueryReward

Entrez l'identifiant du client. Par exemple, entrez 1 pour Richard, 2 pour Arnav et 3 pour Shirley.

```
2
```

Répertoire du code source

Utilisez le tableau suivant comme guide de la structure de répertoires de la solution Visual Studio.

Répertoire d'exemples de solutions de code sur site du CQRS

Modèle CRUD du client

Exemple de code sur site CQRS \ Modèle CRUD \ Projet AWS.APG.CQRSES.DAL

Version CQRS du modèle CUSTOMER CRUD

- Commande du client : `CQRS On-Premises Code Sample\CQRS Model\Command Microservice\AWS.APG.CQRSES.Command` projet
- Demande du client : `CQRS On-Premises Code Sample\CQRS Model\Query Microservice \AWS.APG.CQRSES.Query` projet

Microservices de commande et de requête

Le microservice Command se trouve dans le dossier `CQRS On-Premises Code Sample\CQRS Model\Command Microservice` de solutions :

- `AWS.APG.CQRSES.CommandMicroservice`Le projet d'API ASP.NET Core constitue le point d'entrée où les consommateurs interagissent avec le service.
- `AWS.APG.CQRSES.Command`Le projet .NET Core est un objet qui héberge des objets et des interfaces liés aux commandes.

Le microservice de requête se trouve dans le dossier `CQRS On-Premises Code Sample\CQRS Model\Query Microservice` de solution :

- `AWS.APG.CQRSES.QueryMicroservice`Le projet d'API ASP.NET Core constitue le point d'entrée où les consommateurs interagissent avec le service.
- `AWS.APG.CQRSES.Query`Le projet .NET Core est un objet qui héberge des objets et des interfaces liés aux requêtes.

Répertoire de solutions de code sans serveur AWS CQRS

Ce code est la version AWS du code sur site utilisant les services sans serveur AWS.

Dans C# .NET Core, chaque fonction Lambda est représentée par un projet .NET Core. Dans l'exemple de code de ce modèle, il existe un projet distinct pour chaque interface dans les modèles de commande et de requête.

CQRS utilisant les services AWS

Le répertoire des solutions racine pour CQRS utilisant les services sans serveur AWS se trouve dans le `CQRS AWS Serverless\CQRS` dossier. L'exemple inclut deux modèles : client et récompense.

Les fonctions de commande Lambda pour Customer et Reward se trouvent sous `CQRS\Command Microservice\Customer` et `CQRS\Command Microservice\Reward` dans des dossiers. Ils contiennent les projets Lambda suivants :

- Commande du client : `CommandCreateLambda``CommandDeleteLambda`, et `CommandUpdateLambda`
- Commande de récompense : `CommandAddRewardLambda` et `CommandRedeemRewardLambda`

Les fonctions de requête Lambda pour Customer et Reward se trouvent dans les dossiers `CQRS \Query Microservice\Customer` et`CQRS\QueryMicroservice\Reward`. Ils contiennent les projets Lambda `QueryCustomerListLambda` et `QueryRewardLambda` Lambda.

Projet de test CQRS

Le projet de test se trouve sous le `CQRS\Tests` dossier. Ce projet contient un script de test pour automatiser le test des fonctions Lambda du CQRS.

Recherche d'événements à l'aide des services AWS

Les gestionnaires d'événements Lambda suivants sont lancés par les flux DynamoDB Customer et Reward pour traiter et synchroniser les données dans les tables de requêtes.

- La fonction `EventSourceCustomer` Lambda est mappée au flux `cqrses-customer-cmd` DynamoDB de la table client ().
- La fonction `EventSourceReward` Lambda est mappée au flux `cqrses-reward-cmd` DynamoDB de la table des récompenses ().

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Plus de modèles

- Accédez à des applications de conteneur en privé sur Amazon EKS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Automatisez l'ajout ou la mise à jour d'entrées de registre Windows à l'aide d'AWS Systems Manager
- Automatisez le basculement et le retour en arrière entre régions à l'aide de DR Orchestrator Framework
- Automatically build and deploy a Java application to Amazon EKS using a CI/CD pipeline
- Créez automatiquement des pipelines CI/CD et des clusters Amazon ECS pour les microservices à l'aide d'AWS CDK
- Sauvegardez et archivez les données du mainframe sur Amazon S3 à l'aide de BMC AMI Cloud Data
- Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager
- Créez un maillage de données d'entreprise avec Amazon DataZone AWS CDK, et AWS CloudFormation
- Enchaînez les services AWS en utilisant une approche sans serveur
- Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age
- Déployez en continu une application Web AWS Amplify moderne à partir d'un référentiel AWS CodeCommit
- Convertissez et décompressez les données EBCDIC en ASCII sur AWS à l'aide de Python
- Convertissez des fichiers de données du mainframe avec des mises en page d'enregistrement complexes à l'aide de Micro Focus
- Création d'un pipeline et d'une AMI à l'aide de CodePipeline and HashiCorp Packer
- Créez un pipeline et déployez des mises à jour d'artefacts sur des instances locales à l'aide de EC2 CodePipeline
- Créez un portail pour les micro-frontends en utilisant AWS Amplify Angular et Module Federation
- Déploiement et débogage de clusters Amazon EKS
- Déployez des conteneurs à l'aide d'Elastic Beanstalk
- Émulez Oracle DR à l'aide d'une base de données globale Aurora compatible avec PostgreSQL
- Générez des informations sur les données en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight

- Générez des informations sur les données Db2 z/OS à l'aide d' AWS Mainframe Modernization Amazon Q dans QuickSight
- Identifiez automatiquement les images de conteneur dupliquées lors de la migration vers un référentiel Amazon ECR
- Implémentez la gestion des versions d'API basée sur les chemins en utilisant des domaines personnalisés dans Amazon API Gateway
- Migrez progressivement d'Amazon RDS for Oracle vers Amazon RDS for PostgreSQL à l'aide d'Oracle SQL Developer et d'AWS SCT
- Intégrez le contrôleur universel Stonebranch à la modernisation du mainframe AWS
- Gérez les produits AWS Service Catalog dans plusieurs comptes AWS et régions AWS
- Migrer un compte de membre AWS depuis AWS Organizations vers AWS Control Tower
- Migrez et répliquez des fichiers VSAM vers Amazon RDS ou Amazon MSK à l'aide de Connect from Precisely
- Migrez de SAP ASE vers Amazon RDS for SQL Server à l'aide d'AWS DMS
- Migrer des tables externes Oracle vers des tables compatibles avec Amazon Aurora PostgreSQL
- Modernisez l'application CardDemo mainframe en utilisant AWS Transform
- Modernisez les charges de travail d'impression par lots du mainframe AWS en utilisant Rocket Enterprise Server et LRS VPSX/MFI
- Modernisez les charges de travail d'impression en ligne du mainframe sur AWS à l'aide de Micro Focus Enterprise Server et de LRS VPSX/MFI
- Modernisez la gestion des sorties du mainframe AWS en utilisant Rocket Enterprise Server et PageCenter LRS X
- Déplacez les fichiers du mainframe directement vers Amazon S3 à l'aide de Transfer Family
- Optimisation des images Docker générées par AWS App2Container
- Optimisez les déploiements multicomptes sans serveur en utilisant les flux de travail et AWS CDK Actions GitHub
- Automatisez les déploiements bleu/vert des bases de données mondiales Amazon Aurora en utilisant les principes de l'IaC
- Répliquez des bases de données mainframe sur AWS à l'aide de Precisely Connect
- Exécutez des tâches Amazon ECS sur Amazon WorkSpaces avec Amazon ECS Anywhere
- Envoyez des données de télémétrie de AWS Lambda vers OpenSearch pour des analyses et des visualisations en temps réel

- Configuration d'un référentiel de graphiques Helm v3 dans Amazon S3
- Configurer la détection des AWS CloudFormation dérives dans une organisation multirégionale et multi-comptes
- Structurer un projet Python dans une architecture hexagonale à l'aide d'AWS Lambda
- AWS Infrastructure de test à l'aide LocalStack de tests Terraform
- Mettez à niveau les clusters SAP Pacemaker de ENSA1 ENSA2
- Utilisez Amazon Q Developer comme assistant de codage pour augmenter votre productivité
- Validez le code Account Factory pour Terraform (AFT) localement

ordinateurs centraux

Rubriques

- Accès Services AWS depuis IBM z/OS en installant le AWS CLI
- Sauvegardez et archivez les données du mainframe sur Amazon S3 à l'aide de BMC AMI Cloud Data
- Créez des programmes COBOL DB2 en utilisant et AWS Mainframe ModernizationAWS CodeBuild
- Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager
- Créez un visualiseur de fichiers mainframe avancé dans le cloud AWS
- Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age
- Convertissez et décompressez les données EBCDIC en ASCII sur AWS à l'aide de Python
- Convertissez des fichiers mainframe du format EBCDIC au format ASCII délimité par des caractères dans Amazon S3 à l'aide d'AWS Lambda
- Convertissez des fichiers de données du mainframe avec des mises en page d'enregistrement complexes à l'aide de Micro Focus
- Déployez un environnement pour les applications Blu Age conteneurisées à l'aide de Terraform
- Générez des informations sur les données Db2 z/OS à l'aide d' AWS Mainframe Modernization Amazon Q dans QuickSight
- Générez des informations sur les données en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight
- Intégrez le contrôleur universel Stonebranch à la modernisation du mainframe AWS
- Migrez et répliquez des fichiers VSAM vers Amazon RDS ou Amazon MSK à l'aide de Connect from Precisely
- Modernisez la gestion des sorties du mainframe AWS en utilisant Rocket Enterprise Server et PageCenter LRS X
- Modernisez l'application CardDemo mainframe en utilisant AWS Transform
- Modernisez les charges de travail d'impression par lots du mainframe AWS en utilisant Rocket Enterprise Server et LRS VPSX/MFI
- Modernisation du mainframe : DevOps activée AWS avec Rocket Software Enterprise Suite
- Modernisez les charges de travail d'impression en ligne du mainframe sur AWS à l'aide de Micro Focus Enterprise Server et de LRS VPSX/MFI

- Déplacez les fichiers du mainframe directement vers Amazon S3 à l'aide de Transfer Family
- Sécurisez et rationalisez l'accès des utilisateurs dans une base de données de fédération DB2 sur AWS en utilisant des contextes fiables
- Transférez des données Db2 z/OS à grande échelle vers Amazon S3 dans des fichiers CSV
- Plus de modèles

Accès Services AWS depuis IBM z/OS en installant le AWS CLI

Créée par Souma Ghosh (AWS), Phil de Valence (AWS) et Paulo Vitor Pereira (AWS)

Récapitulatif

The AWS Command Line Interface (AWS CLI) est un outil open source permettant de gérer plusieurs AWS services à l'aide de commandes dans un shell de ligne de commande. Avec une configuration minimale, vous pouvez exécuter des commandes à partir de sessions de ligne de commande telles que l'invite de commande, le terminal et le shell bash pour implémenter des fonctionnalités équivalentes à celles fournies par le navigateur AWS Management Console.

Toutes les fonctions d'administration, de gestion et d'accès de l' AWS infrastructure en tant que service (IaaS) AWS Management Console sont disponibles dans l' AWS API et. AWS CLI Vous pouvez l'installer AWS CLI sur un mainframe IBM z/OS pour y accéder, le gérer et interagir directement Services AWS depuis z/OS. AWS CLI Permet aux utilisateurs et aux applications d'effectuer diverses tâches, telles que :

- Transfert de fichiers ou d'ensembles de données entre z/OS et le stockage d'objets Amazon Simple Storage Service (Amazon S3) et affichage du contenu des buckets
- Démarrage et arrêt de différentes AWS ressources ; par exemple, démarrage d'une tâche par lots dans un AWS Mainframe Modernization environnement
- Appel d'une AWS Lambda fonction pour implémenter une logique métier commune
- Intégration à l'intelligence artificielle, à l'apprentissage automatique (IA/ML) et aux services d'analyse

Ce modèle décrit comment installer, configurer et utiliser AWS CLI le sous z/OS. Vous pouvez l'installer globalement, afin qu'il soit accessible à tous les utilisateurs de z/OS, ou au niveau de chaque utilisateur. Le modèle explique également comment l'utiliser AWS CLI dans une session de ligne de commande interactive à partir de z/OS Unix System Services (USS) ou en tant que travail par lots.

Conditions préalables et limitations

Prérequis

- Communication réseau entre z/OS et AWS

Par défaut, les demandes sont AWS CLI envoyées à l'aide Services AWS du protocole HTTPS sur le port TCP 443. Pour l'utiliser AWS CLI correctement, vous devez être en mesure d'établir des connexions sortantes sur le port TCP 443. Vous pouvez utiliser l'une des commandes z/OS USS suivantes (certaines d'entre elles ne sont peut-être pas installées dans votre environnement) pour tester la connectivité réseau entre z/OS et : AWS

```
ping amazonaws.com
dig amazonaws.com
traceroute amazonaws.com
curl -k https://docs.aws.amazon.com/cli/v1/userguide/cli-chap-welcome.html
```

- AWS credentials

  Pour communiquer avec les AWS Cloud services depuis z/OS, vous devez configurer certaines informations d'identification avec des privilèges pour accéder à la cible Compte AWS. AWS CLI Pour les commandes programmatiques AWS, vous pouvez utiliser des clés d'accès, qui se composent d'un identifiant de clé d'accès et d'une clé d'accès secrète. Si vous ne disposez pas des clé d'accès, vous pouvez les créer à partir de l' AWS Management Console. Il est recommandé de n'utiliser les clés d'accès de l'utilisateur Compte AWS root pour aucune tâche, sauf si l'utilisateur root est requis. Créez plutôt un nouvel utilisateur administrateur IAM et préparez-vous à obtenir des autorisations de moindre privilège afin de configurer l'utilisateur avec des clés d'accès. Après avoir créé l'utilisateur, vous pouvez créer un identifiant de clé d'accès et une clé d'accès secrète pour cet utilisateur.

  > ⚠ Warning
  >
  > AWS Identity and Access Management Les utilisateurs (IAM) possèdent des informati ons d'identification à long terme qui présentent un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires.

- IBM Python pour z/OS

  AWS CLI Nécessite Python 3.8 ou version ultérieure. IBM a permis à Python de fonctionner sous z/OS avec IBM Open Enterprise Python for z/OS. IBM Open Enterprise Python est disponible gratuitement via Shopz SMP/E, ou vous pouvez télécharger le fichier PAX depuis le site Web

d'IBM. Pour obtenir des instructions, consultez la documentation d'installation et de configuration d'IBM Open Enterprise Python for z/OS.

Limites

- Les instructions d'installation fournies dans ce modèle s'appliquent uniquement àAWS CLI la version 1. La dernière version AWS CLI est la version 2. Toutefois, ce modèle utilise l'ancienne version car les méthodes d'installation sont différentes pour la version 2 et les exécutables binaires disponibles pour la version 2 ne sont pas compatibles avec le système z/OS.

Versions du produit

- AWS CLI version 1
- Python 3.8 ou version ultérieure

Architecture

Pile technologique

- Mainframe exécutant z/OS
- Services système UNIX pour mainframe z/OS (USS)
- Mainframe Open MVS (OMVS) — Interface de commande de l'environnement shell z/OS UNIX
- Disque central, tel qu'un périphérique de stockage à accès direct (DASD)
- AWS CLI

Architecture cible

Le schéma suivant montre un AWS CLI déploiement sur IBM z/OS. Vous pouvez l'invoquer AWS CLI à partir d'une session utilisateur interactive, telle que des sessions SSH et Telnet. Vous pouvez également l'invoquer depuis un traitement par lots en utilisant le langage de contrôle des tâches (JCL) ou depuis n'importe quel programme capable d'appeler une commande shell z/OS Unix.

Il AWS CLI communique avec les Service AWS terminaux via un réseau TCP/IP. Cette connexion réseau peut se faire via Internet ou via une AWS Direct Connect connexion privée entre le centre de

données du client et les centres de AWS Cloud données. La communication est authentifiée avec des AWS informations d'identification et cryptée.

Automatisation et évolutivité

Vous pouvez explorer les fonctionnalités d'un Service AWS avec AWS CLI et développer des scripts shell USS pour gérer vos AWS ressources à partir de z/OS. Vous pouvez également exécuter des AWS CLI commandes et des scripts shell à partir de l'environnement batch z/OS, et vous pouvez automatiser les tâches par lots pour qu'elles s'exécutent selon un calendrier spécifique en les intégrant aux planificateurs mainframe. AWS CLI les commandes ou les scripts peuvent être codés dans les paramètres (PARMs) et les procédures (PROCs), et peuvent être mis à l'échelle en suivant l'approche standard qui consiste à appeler le PARM ou le PROC à partir de différents traitements par lots avec différents paramètres.

Outils

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.

Bonnes pratiques

- Pour des raisons de sécurité, limitez les autorisations d'accès au répertoire USS où les détails de la clé AWS d'accès sont stockés. N'autorisez l'accès qu'aux utilisateurs ou aux programmes qui utilisent le AWS CLI.
- N'utilisez les clés d'accès de l'utilisateur Compte AWS root pour aucune tâche. Créez plutôt un nouvel utilisateur administrateur IAM pour vous-même et configurez-le avec des clés d'accès.

> **Warning**
>
> Les utilisateurs IAM disposent d'informations d'identification à long terme qui présentent un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires.

Épopées

Installation de AWS CLI la version 1 sur z/OS USS

Tâche	Description	Compétences requises
Installez Python 3.8 ou version ultérieure.	1. Connectez-vous à l'interface d'invite de commande z/OS USS en utilisant l'une des méthodes suivantes : • Utilisez une commande OMVS avec option de partage du temps (TSO) depuis le panneau ISPF (Interactive System Productivity Facility), ou • Utilisez SSH ou Telnet pour vous connecter à l'adresse IP de la partition logique du mainframe (LPAR). Ce modèle suppose qu'il `cliuser` s'agit de l'identifiant utilisateur utilisé pour se connecter à l'environnement `/u/cliuser/` USS et du répertoire personnel de l'utilisateur. Vous pouvez définir le répertoire personnel de l'utilisateur différemment dans votre environnement z/OS en fonction de vos exigences d'installation.	Administrateur mainframe z/OS

Tâche	Description	Compétences requises
	2. Suivez le guide d'installation d'IBM Open Enterprise Python for z/OS pour installer Python 3.8 ou version ultérieure s'il n'est pas déjà installé.	

Tâche	Description	Compétences requises

Définissez les variables d'environnement USS.	Ajoutez des variables d'environnement au profil. Vous pouvez les ajouter soit au `/u/cliuser/.profile` fichier d'un utilisateur individuel (`cliuser`), soit au `/etc/profile` fichier de tous les utilisateurs.
	
	Note
	Ce modèle suppose que Python a été installé dans le `/u/awscli/python` répertoire. Si votre répertoire d'installation est différent, mettez à jour le code en conséquence.
	
	`# Python configuration`
	`export BPXKAUTOCVT='ON'`
	`export CEERUNOPTS='FILETAG(AUTOCVT,AUTOTAG) POSIX(ON)'`
	`export TAGREDIR_ERR=txt`
	`export TAGREDIR_IN=txt`
	`export TAGREDIR_OUT=txt`
	
	`# AWS CLI configuration`
		Administrateur mainframe z/OS

Tâche	Description	Compétences requises
	`export PATH=/u/cliuser/python/bin:$PATH` `export PYTHONPATH=/u/cliuser/python:$PYTHONPATH`	
Testez l'installation de Python.	Exécutez la commande python : `python --version` Le résultat devrait confirmer que Python 3.8 ou version ultérieure est correctement installé.	Administrateur mainframe z/OS

Tâche	Description	Compétences requises

Vérifiez ou installez pip.	1. La commande pip est généralement installée automatiquement lorsque vous installez Python depuis le site Web d'IBM. Pour vérifier, exécutez la commande suivante :
	`pip —-version`
	Si pip est installé, cette commande doit afficher la version installée.
	2. Si la commande pip est introuvable, installez pip en exécutant la commande suivante :
	`python -m ensurepip --upgrade`
	Pour plus d'options d'installation, consultez la documentation pip.
		Administrateur mainframe z/OS

Tâche	Description	Compétences requises

Installez AWS CLI la version 1.	1. Pour installer le AWS CLI, exécutez la commande suivante :
	`python -m pip install awscli`
	La sortie doit ressembler à ce qui suit.
	`Successfully installed PyYAML-6.0.1 awscli-1.32.23 botocore-1.34.23 colorama-0.4.4 docutils-0.16 jmespath-1.0.1 pyasn1-0.5.1 python-dateutil-2.8.2 rsa-4.7.2 s3transfer-0.10.0 urllib3-2.0.7`
	2. Modifiez l'autorisation de l'exécutable aws en exécutant la commande suivante. Assurez-vous de mettre à jour le répertoire des espaces réservés `<python_installation_dir>` avec votre chemin d'installation Python.
	`chmod 744 <python_installation_dir>/bin/aws`
		Administrateur mainframe z/OS

Tâche	Description	Compétences requises

	3. Exécutez la commande suivante pour tester l' AWS CLI installation :
	`aws --version`
	La sortie doit afficher les versions de AWS CLI Python et de botocore, comme indiqué ci-dessous.
	`aws-cli/1.32.3`
	` Python/3.9.5`
	` OS/390/27.00`
	` botocore/1.34.3`	

Configuration de AWS CLI l'accès depuis z/OS

Tâche	Description	Compétences requises
Configurez les clés AWS d'accès, la région par défaut et la sortie.	La AWS CLI documentation décrit les différentes options de configuration de AWS l'accès. Vous pouvez choisir une configuration en fonction des normes de votre organisation. Cet exemple utilise la configuration des informations d'identification à court terme. 1. Configurez le AWS CLI avec la commande suivante :	Administrateur AWS, administrateur Mainframe z/OS, développeur Mainframe z/OS

Tâche	Description	Compétences requises

	`aws configure`
	2. Fournissez les détails des éléments suivants lorsque vous y êtes invité. Les valeurs de l'ID de clé d'accès et de la clé d'accès secrète proviennent des clés que vous avez obtenues lorsque vous avez défini les AWS informations d'identification dans les étapes des conditions préalables.
	`AWS Access Key ID [None]: ASIAIOSFODNN7EXAMPLE`
	`AWS Secret Access Key [None]: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
	`Default region name [None]: us-east-1`
	`Default output format [None]:`
	`aws configure set aws_session_token IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZ2luX2IQoJb3JpZVERYLONGSTRINGEXAMPLE`
	Cette configuration, y compris les clés d'accès, est stockée dans le `/u/`	

Tâche	Description	Compétences requises
	`cliuser/.aws` dossier. Pour des raisons de sécurité, limitez ce dossier afin de n'autoriser l'accès qu'aux utilisateurs ou aux programmes qui utilisent le AWS CLI.	

Tâche	Description	Compétences requises
Testez le AWS CLI.	1. Exécutez la commande suivante à l'invite de commande pour tester le AWS CLI avec une commande simple : `aws s3 ls` La sortie doit répertorier tous les compartiments S3 pour la configuration Compte AWS sans aucune erreur. 2. Suivez les instructions des deux épisodes suivants pour transférer des données d'USS vers Amazon S3. Vous pouvez choisir l'une des deux options suivantes : • Option 1 (épisode suivant) : transférez de manière interactive un fichier de valeurs séparées par des virgules (CSV) EBCDIC vers Amazon S3 et interrogez le fichier depuis Amazon Athena. • Option 2 : transférer un ensemble de données de longueur fixe EBCDIC vers Amazon S3 sous	Administrateur mainframe z/OS, développeur Mainframe z/OS

Tâche	Description	Compétences requises
	forme de traitement par lots.	

Option 1 – Transférer des données d'USS vers Amazon S3 de manière interactive à partir d'une session USS

Tâche	Description	Compétences requises
Téléchargez et transférez l'exemple de fichier CSV.	1. Téléchargez `sales-records.csv` depuis la section Pièces jointes. Ce fichier fournit un exemple de fichier CSV contenant des enregistrements de ventes. 2. Transférez le fichier vers z/OS USS. 3. Vérifiez que le `/u/cliuser/sales-records.csv` fichier est lisible au format EBCDIC dans USS à l'aide de l'éditeur de texte de votre choix.	Développeur d'applications, développeur Mainframe z/OS
Créez un compartiment S3 et téléchargez le fichier CSV.	1. Créez un compartiment S3 pour stocker le fichier CSV. `aws s3 mb s3://<s3_bucket_name>` où `<s3_bucket_name>` est le nom unique d'un compartiment ; par exemple :	Développeur d'applications, développeur Mainframe z/OS

Tâche	Description	Compétences requises

	`aws s3 mb s3://DOC-EXAMPLE-BUCKET1`
	2. Téléchargez le fichier CSV depuis z/OS USS vers le compartiment S3 :
	`aws s3 cp <csv_file_path> s3://<s3_bucket_name>`
	Par exemple :
	`aws s3 cp /u/cliuser/sales-records.csv s3://DOC-EXAMPLE-BUCKET1`
	3. Répertoriez le contenu du compartiment S3 et vérifiez qu'il inclut le fichier téléchargé :
	`aws s3 ls s3://<s3_bucket_name>`
	Par exemple :
	`aws s3 ls s3://DOC-EXAMPLE-BUCKET1`	

Tâche	Description	Compétences requises
Affichez le compartiment S3 et le fichier chargé.	1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la. 2. Naviguez pour voir le nouveau compartiment S3 et l'objet chargé. Pour plus d'informations sur le téléchargement d'objets, consultez Getting started with Amazon S3 dans la documentation Amazon S3.	AWS général

Tâche	Description	Compétences requises

Exécutez une requête SQL sur une table Amazon Athena.	1. Ouvrez la console Amazon Athena.
	2. Créez une nouvelle table (par exemple`DOC-EXAMPLE-BUCKET`) en utilisant les données CSV d'Amazon S3. Pour plus d'informations, consultez la section Interroger l'inventaire Amazon S3 avec Amazon Athena dans la documentation Amazon S3.
	3. Exécutez la `SELECT` requête sur la table pour afficher les données.
	`SELECT * FROM <table_name>;`
	Par exemple :
	`SELECT * FROM DOC-EXAMPLE-BUCKET;`
	La sortie de la requête SQL affichera le contenu de votre fichier CSV.
		AWS général, développeur d'applications

Option 2 – Transférer des données d'USS vers Amazon S3 à l'aide du JCL par lots

Tâche	Description	Compétences requises
Téléchargez le fichier d'exemple.	1. Téléchargez `sales-records-fixed.txt` depuis la section Pièces jointes. Il s'agit d'un exemple de fichier contenant des enregistrements de ventes. Renommez le fichier texte, par exemple en `USER.DATA.FIXED` . 2. Transférez le fichier vers z/OS sous la forme d'un ensemble de données à blocage fixe (FB), d'une longueur d'enregistrement (LRECL) et d'une longueur d'enregistrement (PS). 3. Utilisez l'utilitaire de liste d'ensembles de données pour vérifier que l'`USER.DATA.FIXED` ensemble de données est lisible au format EBCDIC sous l'option 3.4 de l'ISPF. Consultez la section Informations supplémentaires pour un exemple de sortie.	Développeur Mainframe z/OS
Créez un JCL par lots.	Codez le JCL du lot comme suit pour créer le compartim	Développeur Mainframe z/OS

Tâche	Description	Compétences requises

	ent S3 de destination, télécharger l'ensemble de données et répertorier le contenu du compartiment. Assurez-vous de remplacer le nom du répertoire, le nom du fichier et le nom du compartim ent par vos propres valeurs.
	
	`//AWSCLICP JOB`
	`ACTINFO1,'IBMUSER'`
	`,CLASS=A,MSGCLASS=`
	`H,MSGLEVEL=(1,1),`
	`// NOTIFY=&SYSUID,TIM`
	`E=1440`
	`//*--------------`
	`----------`
	`----------`
	`-------`
	`//* Sample job for AWS`
	`CLI`
	`//*--------------`
	`----------`
	`----------`
	`-------`
	`//USSCMD EXEC PGM=BPXBA`
	`TCH`
	`//STDERR DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`export PATH=/u/c`
	`liuser/python/bin:`
	`$PATH`
	`//STDPARM DD *`
	`SH`
	`export _BPXK_AUT`
	`OCVT=ON;`
	`aws s3 mb s3://DOC-`
	`EXAMPLE-BUCKET2;`	

Tâche	Description	Compétences requises
	`cp "//'USER.DATA.FIXED'" /tmp/tmpfile; aws s3 cp /tmp/tmpfile s3://DOC-EXAMPLE-BUCKET2/USER.DATA.FIXED; rm /tmp/tmpfile; aws s3 ls s3://DOC-EXAMPLE-BUCKET2; /*`	
Soumettez la tâche JCL par lots.	1. Soumettez le job JCL que vous avez codé à l'étape précédente. 2. Vérifiez l'état de la tâche dans le System Display and Search Facility (SDSF). En cas de succès, la tâche doit se terminer par le code de retour 0. 3. La sortie standard (STDOUT) du journal des tâches indique la création réussie du bucket, le téléchargement du jeu de données et la liste du contenu du bucket. Pour un exemple d'illustration d'écran, consultez la section Informations supplémentaires.	Développeur Mainframe z/OS

Tâche	Description	Compétences requises
Affichez le jeu de données chargé dans le compartiment S3.	1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la. 2. Naviguez pour voir le fichier téléchargé dans le compartiment de test. 3. Vous pouvez poursuivre le traitement du `USER.DATA.FIXED` fichier ou l'analyser à l'aide de services d'analyse tels qu'Amazon Redshift.	AWS général

Ressources connexes

- AWS CLI documentation de la version 1
- AWS Mainframe Modernization Référence des commandes d'interface de ligne de commande
- AWS Mainframe Modernization

Informations supplémentaires

USER.DATA.FIXED dans l'option ISPF 3.4 (utilitaire de liste de jeux de données)

SYSOUT du traitement par lots soumis

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Sauvegardez et archivez les données du mainframe sur Amazon S3 à l'aide de BMC AMI Cloud Data

Créée par Santosh Kumar Singh (AWS), Mikhael Liberman (logiciel mainframe Model9), Gilberto Biondo (AWS) et Maggie Li (AWS)

Récapitulatif

Ce modèle montre comment sauvegarder et archiver les données du mainframe directement dans Amazon Simple Storage Service (Amazon S3), puis rappeler et restaurer ces données sur le mainframe à l'aide de BMC AMI Cloud Data (anciennement connu sous le nom de Model9 Manager). Si vous recherchez un moyen de moderniser votre solution de sauvegarde et d'archivage dans le cadre d'un projet de modernisation du mainframe ou pour répondre aux exigences de conformité, ce modèle peut vous aider à atteindre ces objectifs.

Généralement, les entreprises qui exécutent des applications métier de base sur des ordinateurs centraux utilisent une librairie de bandes virtuelles (VTL) pour sauvegarder les données stockées, telles que les fichiers et les journaux. Cette méthode peut être coûteuse car elle consomme du MIPS facturable et les données stockées sur des bandes en dehors du mainframe sont inaccessibles. Pour éviter ces problèmes, vous pouvez utiliser BMC AMI Cloud Data pour transférer rapidement et à moindre coût les données opérationnelles et historiques du mainframe directement vers Amazon S3. Vous pouvez utiliser BMC AMI Cloud Data pour sauvegarder et archiver des données via TCP/IP AWS tout en tirant parti des moteurs IBM z Integrated Information Processor (ZiIP) pour réduire les coûts, le parallélisme et les temps de transfert.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- BMC AMI Cloud Data avec une clé de licence valide
- Connectivité TCP/IP entre le mainframe et AWS
- Un rôle AWS Identity and Access Management (IAM) pour l'accès en lecture/écriture à un compartiment S3
- Accès aux produits de sécurité du mainframe (RACF) en place pour exécuter les processus BMC AMI Cloud

- Un agent BMC AMI Cloud z/OS (Java version 8 64 bits SR5 FP16 ou ultérieure) disposant de ports réseau disponibles, de règles de pare-feu autorisant l'accès aux compartiments S3 et d'un système de fichiers z/FS dédié
- Exigences satisfaites pour le serveur de gestion BMC AMI Cloud

Limites

- BMC AMI Cloud Data stocke ses données opérationnelles dans une base de données PostgreSQL qui s'exécute en tant que conteneur Docker sur la même instance Amazon Elastic Compute Cloud (EC2Amazon) que le serveur de gestion. Amazon Relational Database Service (Amazon RDS) n'est actuellement pas pris en charge en tant que backend pour BMC AMI Cloud Data. Pour plus d'informations sur les dernières mises à jour du produit, consultez la section Quoi de neuf ? dans la documentation BMC.
- Ce modèle sauvegarde et archive uniquement les données du mainframe z/OS. BMC AMI Cloud Data sauvegarde et archive uniquement les fichiers du mainframe.
- Ce modèle ne convertit pas les données dans des formats ouverts standard tels que JSON ou CSV. Utilisez un service de transformation supplémentaire tel que BMC AMI Cloud Analytics (anciennement connu sous le nom de Model9 Gravity) pour convertir les données en formats ouverts standard. Les applications natives du cloud et les outils d'analyse de données peuvent accéder aux données une fois qu'elles ont été écrites dans le cloud.

Versions du produit

- BMC AMI Cloud Data version 2.x

Architecture

Pile technologique source

- Mainframe exécutant z/OS
- Fichiers mainframe tels que les ensembles de données et les fichiers z/OS UNIX System Services (USS)
- Disque central, tel qu'un périphérique de stockage à accès direct (DASD)
- Bande mainframe (librairie de bandes virtuelle ou physique)

Pile technologique cible

- Amazon S3
- EC2 Instance Amazon dans un cloud privé virtuel (VPC)
- AWS Direct Connect
- Amazon Elastic File System (Amazon EFS)

Architecture cible

Le schéma suivant montre une architecture de référence dans laquelle les agents logiciels BMC AMI Cloud Data installés sur un mainframe pilotent les anciens processus de sauvegarde et d'archivage des données qui stockent les données dans Amazon S3.

Le schéma suivant illustre le flux de travail suivant :

1. Les agents logiciels BMC AMI Cloud Data s'exécutent sur des partitions logiques du mainframe ()LPARs. Les agents logiciels lisent et écrivent les données du mainframe à partir d'un DASD ou d'une bande directement sur Amazon S3 via TCP/IP.
2. AWS Direct Connect établit une connexion physique isolée entre le réseau local et AWS. Pour une sécurité renforcée, utilisez un site-to-site VPN en plus AWS Direct Connect pour chiffrer les données en transit.
3. Le compartiment S3 stocke les fichiers du mainframe sous forme de données de stockage d'objets, et les agents BMC AMI Cloud Data communiquent directement avec les compartiments S3. Les certificats sont utilisés pour le chiffrement HTTPS de toutes les communications entre l'agent et Amazon S3. Le chiffrement des données Amazon S3 est utilisé pour chiffrer et protéger les données au repos.
4. Les serveurs de gestion BMC AMI Cloud Data s'exécutent comme des conteneurs Docker sur EC2 les instances. Les instances communiquent avec les agents qui s'exécutent sur le mainframe LPARs et les buckets S3.
5. Amazon EFS est monté sur des EC2 instances actives et passives afin de partager le stockage NFS (Network File System). Cela permet de s'assurer que les métadonnées associées à une politique créée sur le serveur de gestion ne sont pas perdues en cas de basculement. En cas de basculement du serveur actif, le serveur passif est accessible sans perte de données. En cas de défaillance du serveur passif, le serveur actif est accessible sans perte de données.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le AWS Cloud.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer pratiquement n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.
- AWS Direct Connectrelie votre réseau interne à un AWS Direct Connect emplacement via un câble à fibre optique Ethernet standard. Grâce à cette connexion, vous pouvez créer des interfaces virtuelles directement vers les AWS services publics tout en contournant les fournisseurs de services Internet sur votre chemin réseau.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.

Outils BMC

- Le serveur de gestion BMC AMI Cloud est une application graphique qui s'exécute en tant que conteneur Docker sur une Amazon Machine Image (AMI) Amazon Linux pour Amazon. EC2 Le serveur de gestion fournit les fonctionnalités nécessaires pour gérer les activités de BMC AMI Cloud, telles que le reporting, la création et la gestion de politiques, l'exécution d'archives et l'exécution de sauvegardes, de rappels et de restaurations.
- L'agent BMC AMI Cloud s'exécute sur un LPAR mainframe sur site qui lit et écrit des fichiers directement dans le stockage d'objets à l'aide du protocole TCP/IP. Une tâche démarrée s'exécute sur un LPAR du mainframe et est chargée de lire et d'écrire les données de sauvegarde et d'archivage vers et depuis Amazon S3.

- L'interface de ligne de commande BMC AMI Cloud Mainframe (M9CLI) vous fournit un ensemble de commandes pour exécuter des actions BMC AMI Cloud directement depuis TSO/E ou par lots, sans dépendre du serveur de gestion.

Épopées

Création d'un compartiment S3 et d'une politique IAM

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment S3 pour stocker les fichiers et les volumes que vous souhaitez sauvegarder et archiver depuis votre environnement mainframe.	AWS général
Créez une politique IAM.	Tous les serveurs et agents de gestion BMC AMI Cloud doivent accéder au compartiment S3 que vous avez créé à l'étape précédente. Pour accorder l'accès requis, créez la politique IAM suivante : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "Listfolder", "Action": [ "s3:ListBucket",`	AWS général

Tâche	Description	Compétences requises

	<pre>"s3:GetBucketLocation",
	"s3:ListBucketVersions"
	],
	"Effect": "Allow",
	"Resource": [
	"arn:aws:s3:::<BucketName>"
	]
	},
	{
	"Sid": "Objectaccess",
	"Effect": "Allow",
	"Action": [
	"s3:PutObject",
	"s3:GetObjectAcl",
	"s3:GetObject",
	"s3:DeleteObjectVersion",
	"s3:DeleteObject",
	"s3:PutObjectAcl",
	"s3:GetObjectVersion"
	],
	"Resource": [</pre>	

Tâche	Description	Compétences requises

	<pre>"arn:aws:s3:::<Bucket Name>/*"
	            ]
	        }
	    ]
	}</pre>	

Obtenez la licence du logiciel BMC AMI Cloud et téléchargez le logiciel

Tâche	Description	Compétences requises
Obtenez une licence logicielle BMC AMI Cloud.	Pour obtenir une clé de licence logicielle, contactez l'équipe BMC AMI Cloud. La sortie de la `D M=CPU` commande z/OS est requise pour générer une licence.	Gagnez du plomb
Téléchargez le logiciel BMC AMI Cloud et la clé de licence.	Procurez-vous les fichiers d'installation et la clé de licence en suivant les instructions de la documentation BMC.	Administrateur de l'infrastructure mainframe

Installez l'agent logiciel BMC AMI Cloud sur le mainframe

Tâche	Description	Compétences requises
Installez l'agent logiciel BMC AMI Cloud.	1. Avant de commencer le processus d'installation, vérifiez que la configuration logicielle et matérielle minimale requise pour l'agent est respectée.	Administrateur de l'infrastructure mainframe

Tâche	Description	Compétences requises
	2. Pour installer l'agent, suivez les instructions de la documentation BMC. 3. Une fois que l'agent a commencé à s'exécuter sur le LPAR du mainframe, vérifiez la présence du `ZM91000I MODEL9 BACKUP AGENT INITIALIZED` message dans le spool. Vérifiez que la connectivité est correctement établie entre l'agent et le compartiment S3 en recherchant le `Object store connectivity has been established successfully` message dans le STDOUT de l'agent.	

Configuration d'un serveur de gestion BMC AMI Cloud sur une instance EC2

Tâche	Description	Compétences requises
Créez des instances Amazon EC2 Linux 2.	Lancez deux instances Amazon EC2 Linux 2 dans différentes zones de disponibilité en suivant les instructions de l'étape 1 : Lancer une instance dans la EC2 documentation Amazon.	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	L'instance doit répondre aux exigences matérielles et logicielles recommandées suivantes : • Processeur : 4 cœurs minimum • RAM : 8 Go minimum • Disque dur : 40 Go • EC2 Instance recommandée : C5.xLarge • Système d'exploitation — Linux • Logiciel — Docker, unzip, VI/Vim • Bande passante réseau : 1 Go minimum Pour plus d'informations, consultez la documentation BMC.	

Tâche	Description	Compétences requises
Créez un système de fichiers Amazon EFS.	Créez un système de fichiers Amazon EFS en suivant les instructions de l'étape 1 : Création de votre système de fichiers Amazon EFS dans la documentation Amazon EFS. Lors de la création du système de fichiers, procédez comme suit : • Choisissez la classe de stockage Standard. • Choisissez le même VPC que celui que vous avez utilisé pour lancer vos EC2 instances.	Administrateur cloud, architecte cloud

Tâche	Description	Compétences requises

Installez Docker et configurez le serveur de gestion.	Connectez-vous à vos EC2 instances :
	
	Connectez-vous à vos EC2 instances en suivant les instructions de Connect to your Linux instance dans la EC2 documentation Amazon.
	
	Configurez vos EC2 instances :
	
	Pour chaque EC2 instance, procédez comme suit :
	
	1. Pour installer Docker, exécutez la commande suivante :
	
	`sudo yum install docker`
	
	2. Pour démarrer Docker, exécutez la commande suivante :
	
	`sudo service docker start`
	
	3. Pour valider l'état de Docker, exécutez la commande suivante :
	
	`sudo service docker status`
	
	4. Dans le `/etc/selinux` dossier,
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

	remplacez le `config` fichier par`SELINUX=permissive` .
	5. Téléchargez les `VerificationScripts.zip` fichiers `model9-v2.x.y_build_build-id-server.zip` et (que vous avez téléchargés précédemment) dans un dossier temporaire de l'une des EC2 instances (par exemple, dans le `/var/tmp` dossier de votre instance).
	6. Pour accéder au `tmp` dossier, exécutez la commande suivante :
	`cd/var/tmp`
	7. Pour décompresser le script de vérification, exécutez la commande suivante :
	`unzip VerificationScripts.zip`
	8. Pour modifier le répertoire, exécutez la commande suivante :
	`cd /var/tmp/sysutils/PrereqsScripts`	

Tâche	Description	Compétences requises
	9. Pour exécuter le script de vérification, exécutez la commande suivante : `./M9VerifyPrereqs.sh` 10. Une fois que le script de vérification vous invite à saisir la saisie, entrez l'URL et le numéro de port Amazon S3. Entrez ensuite l'IP/DNS z/OS et le numéro de port. **Note** Le script exécute une vérification pour confirmer que l' EC2 instance peut se connecter au compartiment S3 et à l'agent qui s'exécutent sur le mainframe. Si une connexion est établie, un message de réussite s'affiche .	

Tâche	Description	Compétences requises

Installez le logiciel du serveur de gestion.	1. Créez un dossier et un sous-dossier dans le répertoire racine (par exemple,`/data/model9`) dans l' EC2 instance que vous souhaitez rendre le serveur actif.
	2. Pour installer le `amazon-efs-utils` package et monter le système de fichiers Amazon EFS créé précédemment, exécutez les commandes suivantes :
	`sudo yum install -y amazon-efs-utils`
	`sudo mount -t efs -o tls <File System ID>:/ /data/model9`
	3. Pour mettre à jour le `/etc/fstab` fichier de l' EC2 instance avec une entrée pour le système de fichiers Amazon EFS (afin qu'Amazon EFS soit automatiquement EC2 remonté au redémarrage d'Amazon), exécutez la commande suivante :
	`<Amazon-EFS-file-system-id>:/ /data/model9 efs defaults,_netdev 0 0`
		Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises

	4. Pour définir le chemin d'accès aux fichiers d'installation de BMC AMI Cloud et l'emplacement d'installation cible, exécutez les commandes suivantes pour exporter les variables :
	`export MODEL9_HOME=/data/model9`
	`export M9INSTALL=/var/tmp`
	Note
	Nous vous recommandons d'ajouter ces commandes EXPORT à votre `.bashrc` script.
	5. Pour modifier le répertoire, exécutez la `cd $MODEL9_HOME` commande, puis créez un autre sous-répertoire en exécutant la `mkdir diag` commande.
	6. Pour décompresser le fichier d'installation, exécutez la commande suivante :
	`unzip $M9INSTALL/model9-<v2.x.y>_`	

Tâche	Description	Compétences requises

	`build_<build-id>-server.zip`
	
	Note
	Remplacez `x.y` (la version) et `build-id` par vos valeurs.
	
	7. Pour déployer l'application, exécutez les commandes suivantes :
	
	`docker load -i $MODEL9_HOME/model9-<v2.x.y>_build_<build-id>.docker`
	`docker load -i $MODEL9_HOME/postgres-12.10-x86.docker.gz`
	
	Note
	Remplacez `v2.x.y` (la version) et `build-id` par vos valeurs.
	
	8. Dans le `$MODEL9_HOME/conf` dossier, mettez à jour le `model9-local.yml` fichier.	

Tâche	Description	Compétences requises

	Note
	Certains paramètres ont des valeurs par défaut, tandis que d'autres peuvent être mis à jour si nécessaire. Pour plus d'informations, consultez les instructions contenues dans le `model9-local.yml` fichier.
	9. Créez un fichier appelé **`$MODEL9_HOME/conf`**, puis ajoutez-y les paramètres suivants :
	`TZ=America/New_York`
	`EXTRA_JVM_ARGS=-Xmx2048m`
	10. Pour créer un pont réseau Docker, exécutez la commande suivante :
	`docker network create -d bridge model9network`
	11. Pour démarrer le conteneur de base de données PostgreSQL pour BMC	

Tâche	Description	Compétences requises

	AMI Cloud, exécutez la commande suivante :
	
	`docker run -p 127.0.0.1:5432:5432 \ -v $MODEL9_HOME/db/data:/var/lib/postgresql/data:z \ --name model9db --restart unless-stopped \ --network model9network \ -e POSTGRES_PASSWORD=model9 -e POSTGRES_DB=model9 -d postgres:12.10`
	
	12. Une fois le conteneur PostgreSQL lancé, exécutez la commande suivante pour démarrer le serveur d'applications :
	
	`docker run -d -p 0.0.0.0:443:443 -p 0.0.0.0:80:80 \ --sysctl net.ipv4.tcp_keepalive_time=600 \ --sysctl net.ipv4.tcp_keepalive_intvl=30 \ --sysctl net.ipv4.tcp_keepalive_probes=10 \ -v $MODEL9_HOME:/model9:z -h $(hostname)`	

Tâche	Description	Compétences requises

	<pre>--restart unless-stopped \
	--env-file $MODEL9_HOME/conf/model9.env \
	--network model9network \
	--name model9-v2.x.y model9:<v2.x.y>.<build-id></pre>
	Note
	Remplacez `v2.x.y` (la version) et `build-id` par vos valeurs.
	13. Pour vérifier l'état de santé des deux conteneurs, exécutez la commande suivante :
	<pre>docker ps -a</pre>
	14. Pour installer un serveur de gestion sur les EC2 instances passives, répétez les étapes 1 à 4, 7 et 10 à 13.
	Note
	Pour résoudre les problèmes, accédez aux journaux enregistrés dans le `/data/`	

Tâche	Description	Compétences requises
	`model9/logs/` dossier. Pour plus d'informations, consultez la documentation BMC.	

Ajoutez un agent et définissez une politique de sauvegarde ou d'archivage sur le serveur de gestion BMC AMI Cloud

Tâche	Description	Compétences requises
Ajoutez un nouvel agent.	Avant d'ajouter un nouvel agent, vérifiez les points suivants : • Un agent BMC AMI Cloud s'exécute sur le LPAR du mainframe et a été complètement initialisé. Identifiez l'agent en recherchant le message d'`ZM91000I MODEL9 BACKUP AGENT INITIALIZED` initialisation dans le spool. • Un conteneur Docker pour le serveur de gestion est entièrement initialisé et en cours d'exécution. Vous devez créer un agent sur le serveur de gestion avant de définir des politiques de	Administrateur ou développeur de stockage mainframe

Tâche	Description	Compétences requises
	sauvegarde et d'archivage. Pour créer l'agent, procédez comme suit : 1. Utilisez un navigateur Web pour accéder au serveur de gestion déployé sur votre EC2 machine Amazon, puis connectez-vous à l'aide des informations d'identification de votre mainframe. 2. Choisissez l'onglet AGENTS, puis sélectionnez AJOUTER UN NOUVEL AGENT. 3. Dans Nom, entrez le nom de l'agent. 4. Dans Nom d'hôte/adresse IP, entrez le nom d'hôte ou l'adresse IP de votre ordinateur central. 5. Pour Port, entrez votre numéro de port. 6. Choisissez TESTER LA CONNEXION. Vous pouvez voir un message de réussite si la connectivité est correctement établie. 7. Choisissez CREATE. Une fois l'agent créé, vous verrez l'état de connexion par rapport à l'agent de stockage d'objets et à l'agent mainframe	

Tâche	Description	Compétences requises
	dans une nouvelle fenêtre qui apparaît dans le tableau.	
Créez une politique de sauvegarde ou d'archivage.	1. Choisissez POLITIQUES. 2. Choisissez CREATE POLICY. 3. Sur la page CRÉER UNE NOUVELLE POLITIQUE, entrez les spécifications de votre politique. **Note** Pour plus d'informations sur les spécifications disponibles, consultez la section Création d'une nouvelle politique dans la documentation BMC. 4. Choisissez Finish (Terminer). 5. La nouvelle politique est désormais répertoriée sous forme de tableau. Pour voir ce tableau, cliquez sur l'onglet POLITIQUES.	Administrateur ou développeur de stockage mainframe

Exécutez la politique de sauvegarde ou d'archivage depuis le serveur de gestion

Tâche	Description	Compétences requises
Exécutez la politique de sauvegarde ou d'archivage.	Exécutez la politique de sauvegarde ou d'archiva ge des données que vous avez créée précédemment à partir du serveur de gestion, manuellement ou automatiq uement (selon un calendrie r). Pour exécuter la politique manuellement, procédez comme suit : 1. Choisissez l'onglet POLITIQUES dans le menu de navigation. 2. Sur le côté droit du tableau correspondant à la politique que vous souhaitez exécuter, choisissez le menu à trois points. 3. Choisissez Exécuter maintenant. 4. Dans la fenêtre de confirmation contextue lle, choisissez YES, RUN POLICY NOW. 5. Une fois la politique exécutée, vérifiez le statut d'exécution dans la section relative à l'activité de la stratégie. 6. Pour la politique exécutée, choisissez le menu à trois	Administrateur ou développeur de stockage mainframe

Tâche	Description	Compétences requises
	points, puis choisissez Afficher le journal d'exécution pour afficher les journaux. 7. Pour vérifier que la sauvegarde a été créée, vérifiez le compartiment S3.	

Tâche	Description	Compétences requises
Restaurez la politique de sauvegarde ou d'archivage.	1. Dans le menu de navigation, choisissez l'onglet POLITIQUES. 2. Choisissez la politique sur laquelle exécuter votre processus de restauration. Cela répertoriera toutes les activités de sauvegarde ou d'archivage exécutées dans le passé pour cette politique spécifique. 3. Pour sélectionner les sauvegardes que vous souhaitez restaurer, choisissez la colonne Date-heure. Le nom du `file/Volume/Storage` groupe indique les détails d'exécution de la politique. 4. Sur le côté droit du tableau, choisissez le menu à trois points, puis sélectionnez RESTAURER. 5. Dans la fenêtre contextuelle, entrez le nom, le volume et le groupe de stockage de votre cible, puis choisissez RESTORE. 6. Entrez les informations d'identification de votre ordinateur central, puis sélectionnez à nouveau RESTAURER.	Administrateur ou développeur de stockage mainframe

Tâche	Description	Compétences requises
	7. Pour vérifier que la restauration a réussi, consultez les journaux ou le mainframe.	

Exécuter la politique de sauvegarde ou d'archivage depuis le mainframe

Tâche	Description	Compétences requises
Exécutez la politique de sauvegarde ou d'archivage à l'aide de M9CLI.	Utilisez la M9CLI pour effectuer des processus de sauvegarde et de restauration à partir de TSO/E, REXX ou via TSO/E, JCLs sans définir de règles sur le serveur de gestion BMC AMI Cloud. En utilisant TSO/E : Si vous utilisez TSO/E, assurez-vous qu'il `M9CLI REXX` est concaténé à. `TSO` Pour sauvegarder un ensemble de données via TSO/E, utilisez la commande. `TSO M9CLI BACKDSN <DSNAME>` **Note** Pour plus d'informations sur les commandes M9CLI, consultez la référence	Administrateur ou développeur de stockage mainframe

Tâche	Description	Compétences requises

	de la CLI dans la documentation BMC.
	
	En utilisant JCLs :
	
	Pour exécuter la politique de sauvegarde et d'archivage à l'aide de JCLs, exécutez la `M9CLI` commande.
	
	À l'aide d'opérations par lots :
	
	L'exemple suivant montre comment archiver un ensemble de données en exécutant la `M9CLI` commande par lots :
	
	`//JOBNAME JOB …`
	`//M9CLI EXEC PGM=IKJEF T01`
	`//STEPLIB DD DISP=SHR, DSN=<MODEL9 LOADLIB>`
	`//SYSEXEC DD DISP=SHR, DSN=<MODEL9 EXEC LIB>`
	`//SYSTSPRT DD SYSOUT=*`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSTSIN DD TSO M9CLI`
	` ARCHIVE`
	` M9CLI ARCHIVE <DSNNAME`
	` OR DSN PATTERN>`
	`/`	

Tâche	Description	Compétences requises
Exécutez la politique de sauvegarde ou d'archivage dans le batch JCL.	BMC AMI Cloud fournit un exemple de routine JCL appelé M9SAPIJ. Vous pouvez personnaliser M9SAPIJ pour exécuter une politique spécifique créée sur le serveur de gestion à l'aide d'une JCL. Cette tâche peut également faire partie d'un planificateur de lots permettant d'exécuter automatiquement des processus de sauvegarde et de restauration. Le traitement par lots attend les valeurs obligatoires suivantes : • Adresse IP/nom d'hôte du serveur de gestion • Numéro de port • ID ou nom de stratégie (créé sur le serveur de gestion) **Note** Vous pouvez également modifier d'autres valeurs en suivant les instructions de l'exemple de tâche.	Administrateur ou développeur de stockage mainframe

Ressources connexes

- Modernisation du mainframe avec AWS (documentation AWS)
- Comment la sauvegarde dans le cloud pour les mainframes réduit les coûts avec Model9 et AWS (blog du réseau de partenaires AWS)
- Comment activer l'analyse des données du mainframe sur AWS à l'aide de Model9 (blog du réseau de partenaires AWS)
- Recommandations relatives à la résilience d'AWS Direct Connect (documentation AWS)
- Documentation de BMC AMI Cloud (site Web de BMC)

Créez des programmes COBOL DB2 en utilisant et AWS Mainframe ModernizationAWS CodeBuild

Créée par Luis Gustavo Dantas (AWS) et Eduardo Zimelewicz (AWS)

Récapitulatif

Ce modèle explique comment créer un AWS CodeBuild projet simple pour précompiler et lier des programmes COBOL Db2 à l'aide des outils de replateforme. AWS Mainframe Modernization Cela permet le déploiement et l'exécution de ces programmes dans l'environnement d'exécution AWS Mainframe Modernization Replatform.

COBOL, langage de programmation orienté métier, alimente de nombreuses applications critiques en raison de sa fiabilité et de sa lisibilité. IBM Db2, un système de gestion de base de données relationnelle, gère efficacement de grands volumes de données et s'intègre aux programmes COBOL via SQL. Ensemble, COBOL et Db2 constituent l'épine dorsale des opérations critiques dans des secteurs tels que la finance et le gouvernement, malgré l'émergence de nouvelles technologies.

La migration des composants COBOL et DB2 de l'environnement mainframe vers d'autres plateformes pose des défis tels que la compatibilité des plateformes, la complexité de l'intégration, la migration des données et l'optimisation des performances. Le déplacement de ces composants critiques nécessite une planification minutieuse, une expertise technique et des ressources pour garantir une migration fluide tout en préservant la fiabilité et les fonctionnalités.

Le AWS Mainframe Modernization service fournit des outils et des ressources pour reconfigurer les applications et les bases de données du mainframe afin qu'elles s'exécutent sur une AWS infrastructure, telle que les instances Amazon Elastic Compute Cloud EC2 (Amazon). Cela implique de déplacer les charges de travail du mainframe vers le cloud sans modifications majeures du code.

Le processus de précompilation et de liaison Db2 est essentiel pour optimiser les performances et la fiabilité des applications de base de données. La précompilation transforme les instructions SQL intégrées en code exécutable, ce qui réduit la charge d'exécution et améliore l'efficacité. Le processus de liaison lie le code précompilé aux structures de base de données, facilitant ainsi les chemins d'accès et l'optimisation des requêtes. Ce processus garantit l'intégrité des données, améliore la réactivité des applications et protège contre les failles de sécurité. Les applications correctement précompilées et liées minimisent la consommation de ressources, améliorent l'évolutivité et atténuent les risques d'attaques par injection de code SQL.

Conditions préalables et limitations

Prérequis

- Un accès Compte AWS à la console au niveau administratif.
- Un système de base de données IBM Db2, tel qu'IBM Db2 pour z/OS ou Db2 pour Linux, Unix et Windows (LUW).
- Le logiciel client IBM Data Server, disponible en téléchargement sur le site Web d'IBM. Pour plus d'informations, consultez les types de client et de pilote de serveur de données IBM Data Server.
- Un programme COBOL DB2 à compiler et à lier. Ce modèle fournit également un exemple de programme de base que vous pouvez utiliser.
- Un cloud privé virtuel (VPC) associé à un AWS réseau privé. Pour plus d'informations sur la création d'un VPC, consultez la documentation Amazon Virtual Private Cloud (Amazon VPC).
- Un référentiel de contrôle de source tel que GitHub ou GitLab.

Limites

- Pour les AWS CodeBuild quotas, voir Quotas pour AWS CodeBuild.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Pile technologique source

La pile source inclut :

- Programmes COBOL qui utilisent une base de données DB2 pour stocker des données
- Compilateur IBM COBOL et précompilateur DB2 pour z/OS
- Autres éléments de la configuration du mainframe, tels que le système de fichiers, le gestionnaire de transactions et le spool

Pile technologique cible

L'approche de ce modèle fonctionne pour deux options : déplacer les données de Db2 pour z/OS vers Db2 pour LUW, ou rester sur Db2 pour z/OS. L'architecture cible inclut :

- Programmes COBOL qui utilisent une base de données DB2 pour stocker des données
- AWS Mainframe Modernization Outils de compilation de replateformes
- AWS CodeBuild comme infrastructure pour créer l'application
- Autres AWS Cloud ressources telles qu'Amazon Linux

Architecture cible

Le diagramme illustre les éléments suivants :

1. L'utilisateur télécharge son code dans un référentiel de contrôle de source tel que GitHub ou GitLab.
2. AWS CodePipeline remarque le changement et récupère le code depuis le dépôt.
3. CodePipeline démarre AWS CodeBuild et envoie le code.
4. CodeBuild suit les instructions du `buildspec.yml` modèle (fournies dans la section Informations supplémentaires) pour :
   a. Obtenez le client IBM Data Server à partir d'un bucket Amazon Simple Storage Service (Amazon S3).
   b. Installez et configurez le client IBM Data Server.
   c. Récupérez les informations d'identification Db2 depuis. AWS Secrets Manager
   d. Connectez-vous au serveur DB2.
   e. Précompilez, compilez et liez le programme COBOL.
   f. Enregistrez les produits finis dans un compartiment S3 AWS CodeDeploy pour les utiliser.
5. CodePipeline démarre CodeDeploy.
6. CodeDeploy coordonne ses agents, qui sont déjà installés dans les environnements d'exécution. Les agents récupèrent l'application depuis Amazon S3 et l'installent conformément aux instructions fournies dans`appspec.yml`.

Pour simplifier les choses et se concentrer sur le build, les instructions de ce modèle couvrent les étapes 1 à 4 mais n'incluent pas le déploiement du programme COBOL Db2.

Automatisation et évolutivité

Pour des raisons de simplicité, ce modèle décrit comment provisionner les ressources manuellement. Cependant, de nombreuses options d'automatisation sont disponibles, telles que AWS CloudFormation, AWS Cloud Development Kit (AWS CDK), et HashiCorp Terraform, qui automatisent ces tâches. Pour plus d'informations, consultez la AWS CDKdocumentation AWS CloudFormationet.

Outils

Services AWS

- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeDeployautomatise les déploiements sur Amazon EC2 ou sur des instances, des AWS Lambda fonctions ou des services Amazon Elastic Container Service (Amazon ECS) sur site.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS Mainframe Modernizationfournit des outils et des ressources pour vous aider à planifier et à mettre en œuvre la migration et la modernisation des mainframes vers des environnements d'exécution AWS gérés.

Autres outils

- Image Amazon ECR pour les outils de AWS Mainframe Modernization replateforme. Pour compiler une application COBOL, vous devez commencer CodeBuild par utiliser une image Amazon Elastic Container Registry (Amazon ECR) contenant les outils de replateforme : AWS Mainframe Modernization

  `673918848628.dkr.ecr.<your-region>.amazonaws.com/m2-enterprise-build-tools:9.0.7.R1`

  Pour plus d'informations sur l'image ECR disponible, consultez le didacticiel dans le guide de l'AWS Mainframe Modernization utilisateur.
- Le logiciel client IBM Data Server est essentiel pour précompiler et lier les programmes COBOL Db2 dans. CodeBuild Il agit comme un pont entre le compilateur COBOL et Db2.

Bonnes pratiques

- Tous les programmes COBOL ne s'appuient pas sur Db2 comme couche de persistance des données. Assurez-vous que les directives de compilation pour accéder à Db2 sont appliquées uniquement aux programmes COBOL spécifiquement conçus pour interagir avec Db2. Implémentez une logique pour faire la distinction entre les programmes COBOL DB2 et les programmes COBOL qui n'utilisent pas Db2.
- Nous vous recommandons d'éviter de compiler des programmes qui n'ont pas été modifiés. Implémentez un processus pour identifier les programmes qui nécessitent une compilation.

Épopées

Créez l'infrastructure cloud

Tâche	Description	Compétences requises
Créez un compartiment S3 pour héberger le client IBM Data Server et les artefacts du pipeline.	Vous devez configurer un compartiment S3 pour (a) télécharger le client IBM Data Server, (b) stocker votre code depuis le référentiel et (c) stocker les résultats du processus de génération. 1. Connectez-vous à la AWS Management Consoleconsole Amazon S3 et ouvrez-la. 2. Choisissez un compartiment S3 existant ou créez-en un nouveau. Notez le nom de ressource Amazon (ARN) du compartiment pour une utilisation future.	AWS général

Tâche	Description	Compétences requises
	Pour savoir comment créer un compartiment S3, consultez la documentation Amazon S3.	

Tâche	Description	Compétences requises
Téléchargez le client IBM Data Server dans le compartiment S3.	1. Sur la console Amazon S3, choisissez le compartiment pour l'ouvrir. 2. Choisissez Créer un dossier, spécifiez son nom en tant que client, puis choisissez Créer un dossier. 3. Ouvrez le dossier client, choisissez Upload, Add files. 4. Choisissez le fichier client IBM Data Server que vous avez précédemm ent téléchargé depuis le site Web d'IBM vers votre système de fichiers local. Le nom du fichier doit être similaire à `v11.5.8_l inuxx64_client.tar .gz` ou `v11.5.9_l inuxx64_client.tar .gz` . 5. Choisissez Ouvrir, Télécharger et attendez que le téléchargement soit terminé. 6. Dans l'onglet Fichiers et dossiers, choisissez le client du serveur de données et notez son URI S3.	AWS général

Tâche	Description	Compétences requises
Créez un AWS Secrets Manager secret pour vos informations d'identification DB2.	Pour créer un secret afin de stocker vos DB2 informations d'identification en toute sécurité : 1. Sur la console Secrets Manager, choisissez Enregistrer un nouveau secret. 2. Dans le volet Choisir un type de secret, sélectionnez Autre type de secret et Texte en clair. 3. Dans la zone de texte en clair, saisissez vos informations d'identification Db2 en utilisant la structure JSON suivante. `{ "username": "<your-db2-user-name>", "password": "<your-db2-password>", "db2node": "db2dev", "db2host": "<your-db2-hostname-or-IP>", "db2port": <your-db2-port>, "db2name": "<your-db2-location>",`	AWS général

Tâche	Description	Compétences requises

	<pre>"qualifier": "<your-db2-qualifier>"
	}</pre>
	4. Choisissez Next et donnez au secret un nom tel que `dev-db2-cred` .
	5. Choisissez Next, Next et Store.
	
	Pour plus d'informations sur la création de secrets, consultez la documentation de Secrets Manager.	

Tâche	Description	Compétences requises
Vérifiez que Db2 est accessible depuis le sous-réseau VPC.	AWS CodeBuild nécessite une connexion au serveur DB2 afin que le client du serveur de données puisse effectuer des opérations de précompilation et de liaison. Assurez-vous qu'il CodeBuild peut atteindre le serveur DB2 via une connexion sécurisée. 1. Ouvrez la console VPC Amazon. 2. Dans le volet de navigation, choisissez Subnets et notez le IDs et IPv4 CIDRsdes sous-réseaux privés sur lesquels CodeBuild fonctionnera le système. 3. Mettez à jour les paramètres actuels de contrôle d'accès réseau pour votre système DB2 en introduisant une règle entrante. Cette règle doit permettre un accès TCP personnalisé au port DB2 exclusivement à partir du sous-réseau associé CIDRs à votre projet. CodeBuild	Administrateur réseau, AWS général

Création des artefacts de l'application

Tâche	Description	Compétences requises
Créez l'actif COBOL Db2.	1. Si vous souhaitez utiliser un exemple COBOL Db2 simple, enregistrez le code source suivant sous le nom de. `CDB2SMP.cbl` Vous pouvez également remplacer cet exemple par un programme que vous possédez déjà. `IDENTIFICATION DIVISION. PROGRAM-ID. CDB2SMP. DATA DIVISION. WORKING-STORAGE SECTION. 01 WS-NAME PIC X(100). PROCEDURE DIVISION. EXEC SQL SELECT NAME INTO :WS-NAME FROM SYSIBM.SYSTABLES END-EXEC GOBACK.` 2. Validez les modifications et transférez le fichier vers votre dépôt.	Développeur d’applications
Créez le fichier `buildspec.yml` .	1. Générez le `buildspec.yml` fichier en vous	AWS DevOps

Tâche	Description	Compétences requises
	basant sur l'exemple fourni dans la section Informations supplémentaires. 2. Validez les modifications et transférez le fichier vers votre dépôt.	
Connectez votre référentiel à CodePipeline.	1. Ouvrez la AWS console Outils de développement. 2. Dans le volet de navigation, choisissez Paramètres, Connexions. 3. Suivez les instructions de la documentation de la console Developer Tools pour le fournisseur de source de votre choix. Vous aurez besoin de l'Amazon Resource Name (ARN) pour la connexion lorsque vous créerez la politique AWS Identity and Access Management (IAM) pour CodePipeline une étape ultérieure.	AWS DevOps

Configurer des autorisations

Tâche	Description	Compétences requises
Créez une politique IAM pour CodeBuild.	Le CodeBuild projet nécessite l'accès à certaines ressources,	AWS général

Tâche	Description	Compétences requises
	notamment Secrets Manager et Amazon S3. Pour configurer les autorisations nécessaires : 1. Ouvrez la console IAM. 2. Dans le volet de navigation, choisissez Policies, Create Policy, puis sélectionnez le CodeBuild service. 3. Passez du format Visual au format JSON, puis copiez la CodeBuild politique fournie dans la section Informations supplémentaires dans le champ de l'éditeur de stratégie. 4. Nommez et enregistrez cette politique pour référence future à l'étape suivante. Pour plus d'informations sur la création de politiques IAM, consultez la documentation IAM.	

Tâche	Description	Compétences requises
Créez un rôle IAM pour CodeBuild.	Pour que les politiques de sécurité soient disponibles pour CodeBuild, vous devez configurer un rôle IAM. Pour créer ce rôle : 1. Sur la console IAM, dans le volet de navigation, choisissez Roles, Create Role. 3. Pour le type d'entité fiable, conservez le Service AWSparamètre par défaut. 4. Dans le champ Cas d'utilisation, sélectionnez le CodeBuild service, puis cliquez sur Suivant. 4. Dans la liste des stratégies IAM disponibles, recherchez la stratégie pour laquelle vous avez créé CodeBuild, puis choisissez Next pour l'associer au rôle. 5. Spécifiez un nom pour le rôle, puis choisissez Create role pour l'enregistrer pour référence future dans CodeBuild. Pour plus d'informations sur la création d'un rôle IAM pour	AWS général

Tâche	Description	Compétences requises
	un Service AWS, consultez la documentation IAM.	
Créez une politique IAM pour CodePipeline.	Le AWS CodePipeline pipeline nécessite l'accès à certaines ressources, notamment votre référentiel de code et Amazon S3. Répétez les étapes indiquées précédemment pour CodeBuild créer une politique IAM pour CodePipeline (à l'étape 2, choisissez CodePipelineau lieu de CodeBuild).	AWS DevOps

Tâche	Description	Compétences requises

Créez un rôle IAM pour CodePipeline.	Pour que les politiques de sécurité soient disponibles pour CodePipeline, vous devez configurer un rôle IAM.
	
	Pour créer ce rôle :
	
	1. Sur la console IAM, choisissez Roles, Create Role.
	2. Pour Trusted entity type (Type d'entité de confiance), choisissez Custom trust policy (Politique de confiance personnalisée).
	
	Une politique comportant un `Principal` élément vide sera affichée.
	3. Sur la `Principal` ligne, entre les accolades, ajoutez :
	
	`"Service": "codepipeline.amazonaws.com"`
	
	La politique de confiance ressemblera à ceci :
	
	`{ "Version": "2012-10-17", "Statement": [ { "Sid": "Statement1",`
		AWS DevOps

Tâche	Description	Compétences requises
	<pre>"Effect": "Allow", "Principal": { "Service": "codepipeline.amazonaws.com" }, "Action": "sts:AssumeRole" }] }</pre> 4. Choisissez Suivant. 5. Dans la liste des stratégies IAM disponibles, recherchez la stratégie pour laquelle vous avez créé CodePipeline, puis choisissez Next pour l'associer au rôle. 6. Spécifiez un nom pour le rôle, puis choisissez Create role pour l'enregistrer pour référence future dans CodePipeline.	

Compilez et liez le programme COBOL Db2

Tâche	Description	Compétences requises
Créez un CodePipeline pipeline et un CodeBuild projet.	Pour créer un CodePipeline pipeline et le CodeBuild projet qui compile et lie le programme COBOL Db2 : 1. Ouvrez la CodePipeline console, puis choisisse	AWS DevOps

Tâche	Description	Compétences requises
	z Create Pipeline, Build custom pipeline. 2. Spécifiez le nom du pipeline. 3. Pour Rôle de service, choisissez Rôle de service existant et choisissez Spécifiez l'ARN pour le rôle IAM pour CodePipeline lequel vous avez créé. 4. Développez les paramètre s avancés, choisissez Emplacement personnal isé, choisissez le compartim ent S3 que vous avez créé précédemment, puis cliquez sur Suivant. 5. Pour le fournisseur de source, sélectionnez votre fournisseur de source tiers et fournissez les informati ons pertinentes pour le fournisseur :. a. Pour Connexion , sélectionnez la connexion créée pour le fournisseur source. b. Pour Nom du référenti el, sélectionnez votre référentiel. c. Pour Branche par défaut, sélectionnez la branche qui stocke votre	

Tâche	Description	Compétences requises
	programme COBOL et`buildspec.yml` . d. Choisissez Suivant. 6. Pour Fournisseur de build, sélectionnez Autres fournisseurs de build, AWS CodeBuild. 7. Pour Nom du projet, choisissez Créer un projet. La console affiche une CodeBuild fenêtre dans laquelle vous pouvez créer un projet de construction. Dans cette fenêtre : a. Entrez un nom pour le projet. b. Pour Image d'environnement, choisissez Image personnalisée. c. Pour le type d'environnement, choisissez Linux Container. d. Pour le compte ECR, choisissez Autre compte ECR. e. Pour l'URI du référentiel Amazon ECR, entrez :`673918848628.dkr.ecr.<your-region>.amazonaws.com/`	

Tâche	Description	Compétences requises
	`m2-enterprise-build-too ls:8.0.9.R1` .	
	f. Pour Rôle de service, choisissez Rôle de service existant et sélectionnez le rôle pour lequel vous avez créé CodeBuild.	
	g. Développez la section Configuration supplémen taire, puis choisissez le VPC, les sous-réseaux privés et le groupe de sécurité pour ce projet.	
	h. Dans la section Buildspec, choisisse z Utiliser un fichier buildspec.	
	i. À la fin de la fenêtre, choisissez Continuer versCodePipeline. La CodeBuild fenêtre se ferme pour que vous puissiez revenir à la CodePipeline console.	
	8. De retour dans la CodePipeline console, choisissez Next.	
	9. Dans le volet Ajouter une étape de déploieme nt, choisissez Ignorer l'étape de déploiement et confirmez.	

Tâche	Description	Compétences requises
	10. Vérifiez les paramètres du pipeline, puis choisissez Create pipeline.	
Vérifiez la sortie.	Vérifiez le succès de la compilation en consultant les journaux de CodePipeline compilation.	AWS DevOps

Tâche	Description	Compétences requises

Vérifiez les résultats dans DB2.	Vérifiez la version du package dans le tableau SYSPLAN.
	
	`select CAST(NAME AS VARCHAR(10)) as name, VALIDATE, LAST_BIND_TIME, LASTUSED, CAST(PKGVERSION AS VARCHAR(10)) as PKGVERSION from SYSIBM.SYSPLAN where NAME = 'CDB2SMP' order by LAST_BIND_TIME desc`
	
	La version doit correspondre à l'ID de CodeBuild build, qui se trouve CDB2SMP dans notre exemple :
	
	`NAME VALIDATE LAST_BIND_TIME LASTUSED PKGVERSION ---------- -------- ---------- -------- CDB2SMP B 2024-05-18-11.53.11.503738 01/01/0001 19`	

Résolution des problèmes

Problème	Solution
Parfois, la AWS console change de région lorsque vous passez d'un service à l'autre.	Assurez-vous de vérifier la valeur sélectionnée Région AWS chaque fois que vous passez d'un service à l'autre. Le Région AWS sélecteur se trouve dans le coin supérieur droit de la fenêtre de console.
Il peut être difficile d'identifier les problèmes de connectivité Db2 à partir de CodeBuild.	Pour résoudre les problèmes de connectiv ité, ajoutez la commande de DB2 connexion suivante au `buildspec.yml` fichier. Cet ajout vous permet de déboguer et de résoudre les problèmes de connectivité. `db2 connect to $DB_NAME user $DB2USER using $DB2PASS`
Parfois, le volet des rôles de la console IAM n'affiche pas immédiatement la politique IAM que vous avez créée.	En cas de retard, actualisez l'écran pour afficher les dernières informations.

Ressources connexes

Documentation IBM

- Types de clients et de pilotes IBM Data Server
- Télécharger les types de clients et de pilotes IBM Data Server

AWS documentation

- Guide de l'utilisateur Amazon S3
- AWS CodeBuild Guide de l'utilisateur
- AWS Mainframe Modernization Guide de l'utilisateur

- AWS Secrets Manager Guide de l'utilisateur
- AWS CodePipeline Guide de l'utilisateur
- AWS CodeDeploy Guide de l'utilisateur

Informations supplémentaires

CodeBuild stratégie

Remplacez les espaces réservés <RegionID><AccountID>,, <SubnetARN><BucketARN>, et <DB2CredSecretARN> par vos valeurs.

```
{"Version": "2012-10-17",
    "Statement": [
        {"Action": "ecr:GetAuthorizationToken", "Effect": "Allow", "Resource": "*" },
        {"Action": ["ecr:GetDownloadUrlForLayer", "ecr:BatchGetImage",
                    "ecr:BatchCheckLayerAvailability"],
         "Effect": "Allow",
         "Resource": "arn:aws:ecr:*:673918848628:repository/m2-enterprise-build-
tools"},
        {"Action": "s3:PutObject", "Effect": "Allow", "Resource": "arn:aws:s3:::aws-m2-
repo-*/*"},
        {"Action": ["logs:PutLogEvents", "logs:CreateLogStream",
 "logs:CreateLogGroup"],
         "Effect": "Allow", "Resource": "arn:aws:logs:<RegionId>:<AccountId>:*"},
        {"Action": ["ec2:DescribeVpcs", "ec2:DescribeSubnets",
                    "ec2:DescribeSecurityGroups", "ec2:DescribeNetworkInterfaces",
                    "ec2:DescribeDhcpOptions", "ec2:DeleteNetworkInterface",
                    "ec2:CreateNetworkInterface"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": "ec2:CreateNetworkInterfacePermission",
         "Effect": "Allow", "Resource": ["<SubnetARN>"]},
        {"Action": "s3:*", "Effect": "Allow", "Resource": ["<BucketARN>/
*","<BucketARN>"]},
        {"Action": "secretsmanager:GetSecretValue",
         "Effect": "Allow", "Resource": "<DB2CredSecretARN>"}
    ]
}
```

CodePipeline stratégie

Remplacez les espaces réservés <BucketARN> <ConnectionARN> par vos valeurs.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {"Action": ["s3:List*", "s3:GetObjectVersion", "s3:GetObject",
 "s3:GetBucketVersioning" ],
        "Effect": "Allow",
        "Resource": ["<BucketARN>/*", "<BucketARN>"]},
        {"Action": ["codebuild:StartBuild", "codebuild:BatchGetBuilds"],
         "Effect": "Allow", "Resource": "*"},
        {"Action": ["codestar-connections:UseConnection"],
         "Effect": "Allow", "Resource": "<ConnectionARN>"}
        ]
}
```

`buildspec.yml`

Remplacez l'`<your-bucket-name>`espace réservé par le nom réel de votre compartiment S3.

```
version: 0.2
phases:
  pre_build:
    commands:
      - /var/microfocuslicensing/bin/mfcesd -no > /var/microfocuslicensing/logs/
mfcesd_startup.log 2>&1 &
      - |
        mkdir $CODEBUILD_SRC_DIR/db2client
        aws s3 cp s3://<your-bucket-name>/v11.5.8_linuxx64_client.tar.gz
 $CODEBUILD_SRC_DIR/db2client/ >> /dev/null 2>&1
        tar -xf $CODEBUILD_SRC_DIR/db2client/v11.5.8_linuxx64_client.tar.gz -C
 $CODEBUILD_SRC_DIR/db2client/
        cd $CODEBUILD_SRC_DIR/db2client/
        ./client/db2_install -f sysreq -y -b /opt/ibm/db2/V11.5 >> /dev/null 2>&1

        useradd db2cli
        /opt/ibm/db2/V11.5/instance/db2icrt -s client -u db2cli db2cli
        DB2CRED=$(aws secretsmanager get-secret-value --secret-id dev-db2-cred | jq -r
 '.SecretString | fromjson')
        read -r DB2USER DB2PASS DB_NODE DB_HOST DB_PORT DB_NAME DB_QUAL <<<$(echo
 $DB2CRED | jq -r
 '.username, .password, .db2node, .db2host, .db2port, .db2name, .qualifier')
        . /home/db2cli/sqllib/db2profile
        db2 catalog tcpip node $DB_NODE remote $DB_HOST server $DB_PORT
        db2 catalog db $DB_NAME as $DB_NAME at node $DB_NODE authentication server
```

```
  build:
    commands:
      - |
        revision=$CODEBUILD_SRC_DIR/loadlib
        mkdir -p $revision; cd $revision
        . /opt/microfocus/EnterpriseDeveloper/bin/cobsetenv
        cob -zU $CODEBUILD_SRC_DIR/CDB2SMP.cbl -C "DB2(DB==${DB_NAME} PASS==${DB2USER}.
${DB2PASS} VERSION==${CODEBUILD_BUILD_NUMBER} COLLECTION==DB2AWSDB"
artifacts:
  files:
    - "**/*"
  base-directory: $revision
```

Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager

Créée par Kevin Yung (AWS), Peter Woods, Abraham Rondon (Micro Focus) et Krithika Palani Selvam (AWS)

Récapitulatif

Ce modèle introduit une architecture évolutive pour les applications mainframe utilisant Micro Focus Enterprise Server dans Scale-Out Performance and Availability Cluster (PAC) et un groupe Amazon Elastic Compute Cloud (Amazon) EC2 Auto Scaling sur Amazon Web Services ().AWS La solution est entièrement automatisée grâce aux hooks AWS Systems Manager de cycle de vie Amazon EC2 Auto Scaling. En utilisant ce modèle, vous pouvez configurer les applications en ligne et par lots de votre mainframe afin d'obtenir une résilience élevée grâce à une mise à l'échelle interne et externe automatique en fonction de vos demandes de capacité.

> **Note**
>
> Ce modèle a été testé avec Micro Focus Enterprise Server version 6.0. Pour la version 8, consultez Configurer Micro Focus Runtime (sur Amazon EC2).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Logiciel et licence Micro Focus Enterprise Server. Pour plus de détails, contactez le service commercial de Micro Focus.
- Compréhension du concept de reconstruction et de fourniture d'une application mainframe à exécuter dans Micro Focus Enterprise Server. Pour une présentation détaillée, consultez la fiche technique du serveur Micro Focus Enterprise.
- Compréhension des concepts du cluster de performance et de disponibilité évolutif de Micro Focus Enterprise Server. Pour plus d'informations, consultez la documentation de Micro Focus Enterprise Server.

- Compréhension du concept global d'application mainframe DevOps avec intégration continue (CI). Pour un modèle de guidage AWS prescriptif développé par Micro Focus AWS et Micro Focus, voir Modernisation du mainframe : DevOps on AWS with Micro Focus.

> **Note**
>
> Ce modèle a été testé avec Micro Focus Enterprise Server version 6. Pour la version 8, consultez Configurer Micro Focus Runtime (sur Amazon EC2).

Limites

- Pour obtenir la liste des plateformes prises en charge par Micro Focus Enterprise Server, consultez la fiche technique du serveur Micro Focus Enterprise.
- Les scripts et les tests utilisés dans ce modèle sont basés sur Amazon EC2 Windows Server 2019 ; les autres versions de Windows Server et systèmes d'exploitation n'ont pas été testés pour ce modèle.
- Le modèle est basé sur Micro Focus Enterprise Server 6.0 pour Windows ; les versions antérieures ou ultérieures n'ont pas été testées lors du développement de ce modèle.

Versions du produit

- Serveur Micro Focus Enterprise 6.0
- Windows Server 2019

Architecture

Dans un environnement mainframe classique, vous devez fournir du matériel pour héberger vos applications et vos données d'entreprise. Pour répondre aux pics de demandes saisonnières, mensuelles, trimestrielles, voire inédits ou inattendus, les utilisateurs de mainframe doivent évoluer en achetant des capacités de stockage et de calcul supplémentaires. L'augmentation du nombre de ressources de stockage et de capacité de calcul améliore les performances globales, mais la mise à l'échelle n'est pas linéaire.

Ce n'est pas le cas lorsque vous commencez à adopter un modèle de consommation à la demande sur AWS en utilisant les serveurs Amazon EC2 Auto Scaling et Micro Focus Enterprise. Les

sections suivantes expliquent en détail comment créer une architecture d'application mainframe entièrement automatisée et évolutive à l'aide du cluster PAC (Micro Focus Enterprise Server Scale-Out Performance and Availability Cluster) avec un groupe Amazon EC2 Auto Scaling.

Architecture de mise à l'échelle automatique de Micro Focus Enterprise Server

Tout d'abord, il est important de comprendre les concepts de base de Micro Focus Enterprise Server. Cet environnement fournit un environnement de déploiement x86 compatible avec le mainframe pour les applications qui s'exécutaient traditionnellement sur le mainframe IBM. Il propose des exécutions en ligne et par lots ainsi qu'un environnement de transaction prenant en charge les éléments suivants :

- IBM COBOL
- IBM PL/I
- Tâches par lots IBM JCL
- Transactions IBM CICS et IMS TM
- Services Web
- Utilitaires de traitement par lots courants, notamment SORT

Micro Focus Enterprise Server permet aux applications mainframe de s'exécuter avec un minimum de modifications. Les charges de travail du mainframe existantes peuvent être déplacées vers des plateformes x86 et modernisées afin de tirer parti des extensions natives du cloud AWS pour une expansion rapide vers de nouveaux marchés ou zones géographiques.

Le modèle AWS Prescriptive Guidance Modernisation du mainframe : on DevOps AWS with Micro Focus a introduit l'architecture permettant d'accélérer le développement et le test d'applications mainframe sur AWS à l'aide de Micro Focus Enterprise Developer et Enterprise Test Server avec AWS et AWS. CodePipeline CodeBuild Ce modèle met l'accent sur le déploiement d'applications mainframe dans l'environnement de production AWS afin de garantir une disponibilité et une résilience élevées.

Dans un environnement de production mainframe, vous avez peut-être configuré IBM Parallel Sysplex dans le mainframe pour obtenir des performances et une disponibilité élevées. Pour créer une architecture évolutive similaire à Sysplex, Micro Focus a introduit le cluster de performance et de disponibilité (PAC) dans Enterprise Server. PACs prendre en charge le déploiement d'applications mainframe sur plusieurs régions de serveurs d'entreprise gérées sous forme d'image unique et

redimensionnées dans des instances Amazon EC2 . PACs prennent également en charge les performances prévisibles des applications et le débit du système à la demande.

Dans un PAC, plusieurs instances d'Enterprise Server fonctionnent ensemble en tant qu'entité logique unique. La défaillance d'une instance de serveur d'entreprise n'interrompt donc pas la continuité des activités, car la capacité est partagée avec d'autres régions, tandis que les nouvelles instances sont automatiquement démarrées à l'aide de fonctionnalités standard telles qu'un groupe Amazon EC2 Auto Scaling. Cela élimine les points de défaillance uniques, améliorant ainsi la résilience face aux problèmes matériels, réseau et applicatifs. Les instances de serveur d'entreprise évolutives peuvent être exploitées et gérées à l'aide de l'administration Web commune d'Enterprise Server (ESCWA) APIs, ce qui simplifie la maintenance opérationnelle et la facilité de maintenance des serveurs d'entreprise.

> **Note**
>
> Micro Focus recommande que le cluster de performance et de disponibilité (PAC) soit composé d'au moins trois régions de serveurs d'entreprise afin que la disponibilité ne soit pas compromise en cas de défaillance ou de maintenance d'une région de serveurs d'entreprise.

La configuration PAC nécessite un service de gestion de base de données relationnelle (RDBMS) pris en charge pour gérer la base de données régionale, une base de données entre régions et les bases de données facultatives. Une base de données de stockage de données doit être utilisée pour gérer les fichiers VSAM (Virtual Storage Access Method) à l'aide du support du gestionnaire de fichiers de base de données Micro Focus afin d'améliorer la disponibilité et l'évolutivité. Les produits suivants RDBMSs sont pris en charge :

- Microsoft SQL Server 2009 R2 et versions ultérieures
- PostgreSQL 10.x, y compris l'édition compatible avec Amazon Aurora PostgreSQL
- DB2 10.4 et versions ultérieures

Pour plus de détails sur les exigences RDBMS et PAC prises en charge, voir Micro Focus Enterprise Server - Conditions préalables et Micro Focus Enterprise Server - Configuration PAC recommandée.

Le schéma suivant montre une configuration d'architecture AWS typique pour un Micro Focus PAC.

	Composant	Description
1	Groupe de mise à l'échelle automatique des instances d'Enterprise Server	Configurez un groupe de dimensionnement automatique déployé avec des instances de serveur d'entreprise dans un PAC. Le nombre d'instances peut être augmenté ou introduit par des CloudWatch alarmes Amazon à l'aide de CloudWatch métriques.
2	Groupe de mise à l'échelle automatique des instances de la CESAO d'Enterprise Server	Configurez un groupe de dimensionnement automatique déployé avec Enterprise Server Common Web Administration (ESCWA). La CESAO assure la gestion des clusters. APIs Les serveurs de la CESAO agissent comme un plan de contrôle pour ajouter ou supprimer des serveurs d'entreprise et pour démarrer ou arrêter des régions de serveurs d'entreprise dans le PAC lors des événements de dimensionnement automatique de l'instance de serveur d'entreprise. Comme l'instance de la CESAO n'est utilisée que pour la gestion du PAC, son schéma de trafic est prévisible et sa mise à l'échelle automatique requise en

		termes de capacité peut être définie sur 1.
3	Instance Amazon Aurora dans une configuration multi-AZ	Configurez un système de gestion de base de données relationnelle (RDBMS) pour héberger les fichiers de données utilisateur et système à partager entre les instances d'Enterprise Server.
4	Instance et réplique Amazon ElastiCache (Redis OSS)	Configurez une instance principale ElastiCache (Redis OSS) et au moins une réplique pour héberger les données utilisateur et faire office de référentiel évolutif (SOR) pour les instances d'Enterprise Server. Vous pouvez configure r un ou plusieurs référenti els évolutifs pour stocker des types spécifiques de données utilisateur. Enterprise Server utilise une base de données Redis NoSQL comme SOR, une exigence pour maintenir l'intégrité du PAC.
5	Network Load Balancer	Configurez un équilibreur de charge, en fournissant un nom d'hôte pour que les applications se connectent aux services fournis par les instances d'Enterprise Server (par exemple, accès à l'applica tion via un émulateur 3270).

Ces composants constituent la configuration minimale requise pour un cluster PAC Micro Focus Enterprise Server. La section suivante traite de l'automatisation de la gestion des clusters.

Utilisation d'AWS Systems Manager Automation pour le dimensionnement

Une fois le cluster PAC déployé sur AWS, le PAC est géré via l'Enterprise Server Common Web Administration (ESCWA). APIs

Pour automatiser les tâches de gestion du cluster lors d'événements de dimensionnement automatique, vous pouvez utiliser les runbooks Systems Manager Automation et Amazon EC2 Auto Scaling with Amazon EventBridge. L'architecture de ces automatisations est illustrée dans le schéma suivant.

	Composant	Description
1	Crochet de cycle de vie évolutif automatique	Configurez des hooks de cycle de vie de dimension nement automatique et envoyez des notifications à Amazon EventBridge lorsque de nouvelles instances sont lancées et que des instances existantes sont résiliées dans le groupe de dimensionnement automatique.
2	Amazon EventBridge	Configurez une EventBridge règle Amazon pour acheminer les événements de dimension nement automatique vers les cibles du runbook de Systems Manager Automation.
3	Runbooks d'automatisation	Configurez les runbooks Systems Manager Automation pour exécuter PowerShell des scripts Windows et appelez

		la CESAO APIs pour gérer le PAC. Pour des exemples, consultez la section Informations supplémentaires.
4	Instance ESCWA d'Enterprise Server dans un groupe de dimensionnement automatique	Configurez une instance Enterprise Server ESCWA dans un groupe de dimensionnement automatique. L'instance de la CESAO permet APIs de gérer le PAC.

Outils

- Micro Focus Enterprise Server — Micro Focus Enterprise Server fournit l'environnement d'exécution pour les applications créées avec n'importe quelle variante de l'environnement de développement intégré (IDE) d'Enterprise Developer.
- Amazon EC2 Auto Scaling — Amazon EC2 Auto Scaling vous aide à vous assurer que vous disposez du nombre correct d' EC2 instances Amazon disponibles pour gérer la charge de votre application. Vous créez des ensembles d' EC2 instances, appelés groupes Auto Scaling, et vous spécifiez le nombre minimum et maximum d'instances.
- Amazon ElastiCache (Redis OSS) — Amazon ElastiCache est un service Web permettant de configurer, de gérer et de dimensionner un stockage de données en mémoire distribué ou un environnement de cache dans le cloud. Il fournit une solution de cache performante, évolutive et économique.
- Amazon RDS — Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud AWS. Il fournit une capacité redimensionnable et rentable pour une base de données relationnelle et gère les tâches d'administration de base de données courantes.
- AWS Systems Manager — AWS Systems Manager est un service AWS que vous pouvez utiliser pour visualiser et contrôler votre infrastructure sur AWS. À l'aide de la console Systems Manager, vous pouvez consulter les données opérationnelles de plusieurs services AWS et automatiser les tâches opérationnelles sur l'ensemble de vos ressources AWS. Systems Manager vous aide à maintenir la sécurité et la conformité en analysant vos Instances gérées et en signalant toute infraction à la politique (ou en prenant des mesures correctives pour y remédier).

Épopées

Création d'une instance Amazon Aurora

Tâche	Description	Compétences requises
Créez un CloudFormation modèle AWS pour une instance Amazon Aurora.	Utilisez l'extrait de code d'exemple AWS pour créer un CloudFormation modèle qui créera une instance Amazon Aurora PostgreSQL Edition compatible.	Architecte du cloud
Déployez une CloudForm ation pile pour créer l'instance Amazon Aurora.	Utilisez le CloudFormation modèle pour créer une instance compatible Aurora PostgreSQL sur laquelle la réplication multi-AZ est activée pour les charges de travail de production.	Architecte du cloud
Configurez les paramètres de connexion à la base de données pour Enterprise Server.	Suivez les instructions de la documentation Micro Focus pour préparer les chaînes de connexion et la configura tion de la base de données pour Micro Focus Enterprise Server.	Ingénieur de données, DevOps ingénieur

Création d'un ElastiCache cluster Amazon pour l'instance Redis

Tâche	Description	Compétences requises
Créez un CloudFormation modèle pour le ElastiCache cluster Amazon pour l'instance Redis.	Utilisez l'extrait de code d'exemple AWS pour créer un CloudFormation modèle qui	Architecte du cloud

Tâche	Description	Compétences requises
	créera un ElastiCache cluster Amazon pour l'instance Redis.	
Déployez la CloudFormation pile pour créer un ElastiCache cluster Amazon pour l'instance Redis.	Créez le ElastiCache cluster Amazon pour l'instance Redis sur laquelle la réplication multi-AZ est activée pour les charges de travail de productio n.	Architecte du cloud
Configurez les paramètres de connexion PSOR d'Enterprise Server.	Suivez les instructions de la documentation Micro Focus pour préparer la configuration de connexion au référentiel PAC Scale-Out (PSOR) pour le PAC Micro Focus Enterprise Server.	DevOps ingénieur

Création d'un groupe de dimensionnement automatique Micro Focus Enterprise Server (CESAO)

Tâche	Description	Compétences requises
Créez une AMI Micro Focus Enterprise Server.	Créez une instance Amazon EC2 Windows Server et installez le binaire Micro Focus Enterprise Server dans l' EC2 instance. Créez une Amazon Machine Image (AMI) de l' EC2 instance. Pour plus d'informations, consultez la documentation d'installation d'Enterprise Server.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un CloudFormation modèle pour Enterprise Server ESCWA.	Utilisez l'exemple d'extrait de code AWS pour créer un modèle permettant de créer une pile personnalisée d'Enterprise Server ESCWA dans un groupe de dimension nement automatique.	Architecte du cloud
Déployez la CloudFormation pile pour créer un groupe de EC2 dimensionnement Amazon pour Enterprise Server ESCWA.	Utilisez le CloudFormation modèle pour déployer le groupe de dimensionnement automatique avec l'AMI Micro Focus Enterprise Server ESCWA créée dans l'article précédent.	Architecte du cloud

Création d'un manuel d'automatisation d'AWS Systems Manager

Tâche	Description	Compétences requises
Créez un CloudFormation modèle pour un runbook de Systems Manager Automation.	Utilisez les exemples d'extrait s de code présentés dans la section Informations supplémentaires pour créer un CloudFormation modèle qui créera un runbook Systems Manager Automation afin d'automatiser la création de PAC, le scalage d'Enterpr ise Server et le scaling out d'Enterprise Server.	Architecte du cloud
Déployez la CloudFormation pile qui contient le runbook Systems Manager Automation.	Utilisez le CloudFormation modèle pour déployer une pile contenant le runbook	Architecte du cloud

Tâche	Description	Compétences requises
	d'automatisation pour la création de PAC, le scalage intégré du serveur Enterprise et le dimensionnement externe du serveur Enterprise.	

Création d'un groupe de dimensionnement automatique pour Micro Focus Enterprise Server

Tâche	Description	Compétences requises
Créez un CloudFormation modèle pour configurer un groupe de dimensionnement automatique pour Micro Focus Enterprise Server.	Utilisez l'extrait de code d'exemple AWS pour créer un CloudFormation modèle qui créera un groupe de dimensionnement automatiq ue. Ce modèle réutilisera la même AMI que celle créée pour l'instance ESCWA de Micro Focus Enterprise Server. Utilisez ensuite un exemple d'extrait de code AWS pour créer l'événement de cycle de vie de dimensionnement automatique et configurez Amazon EventBridge pour filtrer les événements de scale-out et de scale-in dans le même modèle. CloudForm ation	Architecte du cloud
Déployez la CloudForm ation pile pour le groupe de dimensionnement automatique	Déployez la CloudFormation pile contenant le groupe de dimensionnement automatique	Architecte du cloud

Tâche	Description	Compétences requises
pour les serveurs Micro Focus Enterprise.	pour les serveurs Micro Focus Enterprise.	

Ressources connexes

- Cluster de performance et de disponibilité des serveurs Micro Focus Enterprise (PAC)
- Crochets relatifs au cycle de vie d'Amazon EC2 Auto Scaling
- Exécution d'automatisations avec des déclencheurs à l'aide de EventBridge

Informations supplémentaires

Les scénarios suivants doivent être automatisés pour étendre ou dédimensionner les clusters PAC.

Automatisation pour démarrer ou recréer un PAC

Au démarrage d'un cluster PAC, Enterprise Server nécessite l'appel de la CESAO pour APIs créer une configuration PAC. Cela démarre et ajoute des régions Enterprise Server dans le PAC. Pour créer ou recréer un PAC, procédez comme suit :

1. Configurez un référentiel PAC Scale-Out (PSOR) dans la CESAO avec un nom donné.

```
POST /server/v1/config/groups/sors
```

2. Créez un PAC avec un nom donné et joignez-y le PSOR.

```
POST /server/v1/config/groups/pacs
```

3. Configurez la base de données régionale et la base de données interrégionale si c'est la première fois que vous configurez un PAC.

> **Note**
>
> Cette étape utilise des requêtes SQL et l'outil de ligne de commande dbhfhadmin de Micro Focus Enterprise Suite pour créer la base de données et importer les données initiales.

4. Installez la définition PAC dans les régions Enterprise Server.

```
POST /server/v1/config/mfds
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

5. Démarrez les régions Enterprise Server dans le PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

Les étapes précédentes peuvent être mises en œuvre à l'aide d'un PowerShell script Windows.

Les étapes suivantes expliquent comment créer une automatisation pour créer un PAC en réutilisant le PowerShell script Windows.

1. Créez un modèle de EC2 lancement Amazon qui télécharge ou crée le PowerShell script Windows dans le cadre du processus de démarrage. Par exemple, vous pouvez utiliser les données EC2 utilisateur pour télécharger le script depuis un bucket Amazon Simple Storage Service (Amazon S3).
2. Créez un runbook AWS Systems Manager Automation pour appeler le PowerShell script Windows.
3. Associez le runbook à l'instance de la CESAO à l'aide de la balise d'instance.
4. Créez un groupe de dimensionnement automatique de la CESAO à l'aide du modèle de lancement.

Vous pouvez utiliser l'exemple d' CloudFormation extrait AWS suivant pour créer le runbook Automation.

Exemple d' CloudFormation extrait pour un runbook Systems Manager Automation utilisé pour la création de PAC

```
PACInitDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to create Enterprise Server PAC
       mainSteps:
       - action: aws:runPowerShellScript
         name: CreatePAC
         inputs:
```

```
            onFailure: Abort
            timeoutSeconds: "1200"
            runCommand:
            - |
              C:\Scripts\PAC-Init.ps1
  PacInitAutomation:
     Type: AWS::SSM::Document
     Properties:
       DocumentType: Automation
       Content:
         description: Prepare Micro Focus PAC Cluster via ESCWA Server
         schemaVersion: '0.3'
         assumeRole: !GetAtt SsmAssumeRole.Arn
         mainSteps:
           - name: RunPACInitDocument
             action: aws:runCommand
             timeoutSeconds: 300
             onFailure: Abort
             inputs:
               DocumentName: !Ref PACInitDocument
               Targets:
                 - Key: tag:Enterprise Server - ESCWA
                   Values:
                     - "true"
   PacInitDocumentAssociation:
     Type: AWS::SSM::Association
     Properties:
       DocumentVersion: "$LATEST"
       Name: !Ref PACInitDocument
       Targets:
         - Key: tag:Enterprise Server - ESCWA
           Values:
             - "true"
```

Pour plus d'informations, voir Micro Focus Enterprise Server - Configuration d'un PAC.

Automatisation pour une mise à l'échelle avec une nouvelle instance de serveur d'entreprise

Lorsqu'une instance de serveur d'entreprise est étendue, sa région de serveur d'entreprise doit être ajoutée au PAC. Les étapes suivantes expliquent comment invoquer la CESAO APIs et ajouter la région Enterprise Server dans le PAC.

1. Installez la définition PAC dans les régions Enterprise Server.

```
POST '/server/v1/config/mfds'
POST /native/v1/config/groups/pacs/${pac_uid}/install
```

2. Démarrez à chaud la région dans le PAC.

```
POST /native/v1/regions/${host_ip}/${port}/${region_name}/start
```

3. Ajoutez l'instance Enterprise Server à l'équilibreur de charge en associant le groupe de dimensionnement automatique à l'équilibreur de charge.

Les étapes précédentes peuvent être mises en œuvre à l'aide d'un PowerShell script Windows. Pour plus d'informations, voir Micro Focus Enterprise Server - Configuration d'un PAC.

Les étapes suivantes peuvent être utilisées pour créer une automatisation pilotée par les événements afin d'ajouter une instance Enterprise Server récemment lancée dans un PAC en réutilisant le PowerShell script Windows.

1. Créez un modèle de EC2 lancement Amazon pour une instance de serveur d'entreprise qui provisionne une région de serveur d'entreprise lors de son démarrage. Par exemple, vous pouvez utiliser la commande mfds de Micro Focus Enterprise Server pour importer une configuration de région. Pour plus de détails et pour connaître les options disponibles pour cette commande, consultez le manuel Enterprise Server Reference.
2. Créez un groupe de dimensionnement automatique Enterprise Server qui utilise le modèle de lancement créé à l'étape précédente.
3. Créez un runbook Systems Manager Automation pour appeler le PowerShell script Windows.
4. Associez le runbook à l'instance de la CESAO à l'aide de la balise d'instance.
5. Créez une EventBridge règle Amazon pour filtrer l'événement EC2 Instance Launch Successful pour le groupe de dimensionnement automatique Enterprise Server, et créez la cible pour utiliser le runbook Automation.

Vous pouvez utiliser l'exemple d' CloudFormation extrait suivant pour créer le runbook Automation et la règle. EventBridge

Exemple d' CloudFormation extrait de code pour Systems Manager utilisé pour étendre les instances d'Enterprise Server

```
  ScaleOutDocument:
```

```
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Command
      Content:
        schemaVersion: '2.2'
        description: Operation Runbook to Adding MFDS Server into an existing PAC
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        mainSteps:
        - action: aws:runPowerShellScript
          name: Add_MFDS
          inputs:
            onFailure: Abort
            timeoutSeconds: "300"
            runCommand:
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-Out.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleOutAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
```

```
        description: Scale Out 1 New Server in Micro Focus PAC Cluster via ESCWA
Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleOutCommand
            action: aws:runCommand
            timeoutSeconds: 300
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleOutDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                InstanceId: "{{InstanceId}}"
                MfdsPort: "{{MfdsPort}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
```

Automatisation pour le dimensionnement dans une instance de serveur d'entreprise

Comme dans le cas du scaling out, lorsqu'une instance de serveur d'entreprise est mise à l'échelle, l'action de EC2 fin du cycle de vie de l'instance d'événement est lancée et les appels de processus et d'API suivants sont nécessaires pour supprimer une instance de Micro Focus Enterprise Server du PAC.

1. Arrêtez la région dans l'instance d'Enterprise Server en cours de terminaison.

```
POST "/native/v1/regions/${host_ip}/${port}/${region_name}/stop"
```

2. Supprimez l'instance de serveur d'entreprise du PAC.

```
DELETE "/server/v1/config/mfds/${uid}"
```

3. Envoyez un signal pour continuer à mettre fin à l'instance de serveur d'entreprise.

Les étapes précédentes peuvent être implémentées dans un PowerShell script Windows. Pour plus de détails sur ce processus, consultez le document Micro Focus Enterprise Server - Administration d'un PAC.

Les étapes suivantes expliquent comment créer une automatisation pilotée par les événements pour mettre fin à une instance de serveur d'entreprise à partir d'un PAC en réutilisant le script Windows. PowerShell

1. Créez un runbook Systems Manager Automation pour appeler le PowerShell script Windows.
2. Associez le runbook à l'instance de la CESAO à l'aide de la balise d'instance.
3. Créez un hook automatique pour le cycle de vie d'un groupe de dimensionnement pour la résiliation de l' EC2 instance.
4. Créez une EventBridge règle Amazon pour filtrer l'événement EC2 Instance-Terminate Lifecycle Action pour le groupe de dimensionnement automatique Enterprise Server, et créez la cible pour utiliser le runbook Automation.

Vous pouvez utiliser l'exemple de CloudFormation modèle suivant pour créer un runbook, un hook de cycle de vie et une EventBridge règle de Systems Manager Automation.

Exemple d' CloudFormation extrait de code d'exécution de Systems Manager Automation utilisé pour le dimensionnement dans une instance de serveur d'entreprise

```
ScaleInDocument:
   Type: AWS::SSM::Document
   Properties:
     DocumentType: Command
     Content:
       schemaVersion: '2.2'
       description: Operation Runbook to Remove MFDS Server from PAC
       parameters:
         MfdsPort:
           type: String
         InstanceIpAddress:
           type: String
           default: "Not-Available"
         InstanceId:
           type: String
           default: "Not-Available"
       mainSteps:
       - action: aws:runPowerShellScript
         name: Remove_MFDS
         inputs:
           onFailure: Abort
           runCommand:
```

```
            - |
              $ip = "{{InstanceIpAddress}}"
              if ( ${ip} -eq "Not-Available" ) {
                $ip = aws ec2 describe-instances --instance-id {{InstanceId}} --output
text --query "Reservations[0].Instances[0].PrivateIpAddress"
              }
              C:\Scripts\Scale-In.ps1 -host_ip ${ip} -port {{MfdsPort}}

  PacScaleInAutomation:
    Type: AWS::SSM::Document
    Properties:
      DocumentType: Automation
      Content:
        parameters:
          MfdsPort:
            type: String
          InstanceIpAddress:
            type: String
            default: "Not-Available"
          InstanceId:
            type: String
            default: "Not-Available"
        description: Scale In 1 New Server in Micro Focus PAC Cluster via ESCWA Server
        schemaVersion: '0.3'
        assumeRole: !GetAtt SsmAssumeRole.Arn
        mainSteps:
          - name: RunScaleInCommand
            action: aws:runCommand
            timeoutSeconds: "600"
            onFailure: Abort
            inputs:
              DocumentName: !Ref ScaleInDocument
              Parameters:
                InstanceIpAddress: "{{InstanceIpAddress}}"
                MfdsPort: "{{MfdsPort}}"
                InstanceId: "{{InstanceId}}"
              Targets:
                - Key: tag:Enterprise Server - ESCWA
                  Values:
                    - "true"
          - name: TerminateTheInstance
            action: aws:executeAwsApi
            inputs:
              Service: autoscaling
```

```
                Api: CompleteLifecycleAction
                AutoScalingGroupName: !Ref AutoScalingGroup
                InstanceId: "{{ InstanceId }}"
                LifecycleActionResult: CONTINUE
                LifecycleHookName: !Ref ScaleInLifeCycleHook
```

Automatisation pour un déclencheur de dimensionnement EC2 automatique Amazon

Le processus de configuration d'une politique de dimensionnement pour les instances d'Enterprise Server nécessite de comprendre le comportement de l'application. Dans la plupart des cas, vous pouvez configurer des politiques de dimensionnement pour le suivi des cibles. Par exemple, vous pouvez utiliser l'utilisation moyenne du processeur comme CloudWatch métrique Amazon pour définir la politique de dimensionnement automatique. Pour plus d'informations, consultez les politiques de dimensionnement du suivi de Target pour Amazon EC2 Auto Scaling. Pour les applications présentant des modèles de trafic réguliers, envisagez d'utiliser une politique de dimensionnement prédictive. Pour plus d'informations, consultez Predictive Scaling pour Amazon EC2 Auto Scaling.

Créez un visualiseur de fichiers mainframe avancé dans le cloud AWS

Créée par Boopathy GOPALSAMY (AWS) et Jeremiah O'Connor (AWS)

Récapitulatif

Ce modèle fournit des exemples de code et des étapes pour vous aider à créer un outil avancé pour parcourir et examiner les fichiers au format fixe de votre mainframe à l'aide des services sans serveur AWS. Le modèle fournit un exemple de la façon de convertir un fichier d'entrée du mainframe en un document Amazon OpenSearch Service à des fins de navigation et de recherche. L'outil de visualisation de fichiers peut vous aider à réaliser les objectifs suivants :

- Conservez la même structure et la même mise en page des fichiers du mainframe pour garantir la cohérence dans votre environnement de migration cible AWS (par exemple, vous pouvez conserver la même mise en page pour les fichiers dans une application par lots qui transmet des fichiers à des tiers externes)
- Accélérez le développement et les tests lors de la migration de votre mainframe
- Support des activités de maintenance après la migration

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cloud privé virtuel (VPC) doté d'un sous-réseau accessible par votre ancienne plateforme
-

> **Note**
>
> Un fichier d'entrée et le cahier COBOL (Common Business Oriented Language) correspondant (: pour des exemples de fichier d'entrée et de cahier COBOL, voir le référentiel. gfs-mainframe-solutions GitHub Pour plus d'informations sur les copybooks COBOL, consultez le guide de programmation Enterprise COBOL for z/OS 6.3 sur le site Web d'IBM.)

Limites

- L'analyse des cahiers est limitée à un maximum de deux niveaux imbriqués (SURVENUS)

Architecture

Pile technologique source

- Fichiers d'entrée au format FB (Fixed Blocked)
- Mise en page du cahier COBOL

Pile technologique cible

- Amazon Athena
- Amazon OpenSearch Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Lambda
- AWS Step Functions

Architecture cible

Le schéma suivant montre le processus d'analyse et de conversion d'un fichier d'entrée du mainframe en document de OpenSearch service à des fins de navigation et de recherche.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur ou une application administrateur envoie les fichiers d'entrée vers un compartiment S3 et les copybooks COBOL vers un autre compartiment S3.
2.
> **Note**
>
> Le compartiment S3 contenant les fichiers d'entrée invoque une fonction Lambda qui lance un flux de travail Step Functions sans serveur. : L'utilisation d'un déclencheur d'événement S3 et d'une fonction Lambda pour piloter le flux de travail Step Functions dans ce modèle est facultative. Les exemples de GitHub code de ce modèle n'incluent pas l'utilisation de ces services, mais vous pouvez utiliser ces services en fonction de vos besoins.

3. Le flux de travail Step Functions coordonne tous les processus par lots à partir des fonctions Lambda suivantes :

- La `s3copybookparser.py` fonction analyse la mise en page du cahier et extrait les attributs des champs, les types de données et les décalages (nécessaires au traitement des données d'entrée).
- La `s3toathena.py` fonction crée une mise en page de table Athena. Athena analyse les données d'entrée traitées par la `s3toathena.py` fonction et les convertit dans un fichier CSV.
- La `s3toelasticsearch.py` fonction ingère le fichier de résultats depuis le compartiment S3 et le transmet au OpenSearch service.

4. Les utilisateurs accèdent à OpenSearch Dashboards with OpenSearch Service pour récupérer les données sous différents formats de tables et de colonnes, puis exécuter des requêtes sur les données indexées.

Outils

Services AWS

- Amazon Athena est un service de requêtes interactif qui vous permet d'analyser les données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du SQL standard.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez. Dans ce modèle, vous utilisez Lambda pour implémenter la logique de base, telle que l'analyse de fichiers, la conversion de données et le chargement de données dans OpenSearch Service pour un accès interactif aux fichiers.
- Amazon OpenSearch Service est un service géré qui vous permet de déployer, d'exploiter et de dimensionner des clusters de OpenSearch services dans le cloud AWS. Dans ce modèle, vous utilisez le OpenSearch service pour indexer les fichiers convertis et fournir des fonctionnalités de recherche interactives aux utilisateurs.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner les fonctions Lambda et d'autres services AWS pour créer des applications critiques pour l'entreprise. Dans ce modèle, vous utilisez Step Functions pour orchestrer les fonctions Lambda.

Autres outils

- GitHubest un service d'hébergement de code qui fournit des outils de collaboration et de contrôle de version.
- Python est un langage de programmation de haut niveau.

Code

Le code de ce modèle est disponible dans le GitHub gfs-mainframe-patternsréférentiel.

Épopées

Préparer l'environnement cible

Tâche	Description	Compétences requises
Créez le compartiment S3.	Créez un compartiment S3 pour stocker les copybooks , les fichiers d'entrée et les fichiers de sortie. Nous recommandons la structure de dossiers suivante pour votre compartiment S3 : • `copybook/` • `input/` • `output/` • `query/` • `results/`	AWS général
Créez la fonction s3copyboo kparser.	1. Créez une fonction Lambda appelée `s3copyboo kparser` et télécharg	AWS général

Tâche	Description	Compétences requises
	ez le code source (`s3copybookparser.py` et `copybook.py`) depuis le GitHubréférentiel. 2. Attachez la politique IAM `S3ReadOnly` à la fonction Lambda.	
Créez la fonction s3toathena.	1. Créez une fonction Lambda appelée `s3toathena` et téléchargez le code source (`s3toathena.py`) depuis le GitHubréférentiel. Configurez le délai d'expiration Lambda sur > 60 secondes. 2. Pour fournir un accès aux ressources requises, associez les politiques IAM `AmazonAthenaFullAccess` et `S3FullAccess` à la fonction Lambda.	AWS général

Tâche	Description	Compétences requises
Créez la fonction s3toelasticsearch.	1. **Important** [Ajoutez une dépendance Python à votre environnement Lambda]. : Pour utiliser la `s3toelasticsearch` fonction, vous devez ajouter la dépendance Python car la fonction Lambda utilise les dépendances du client Python Elasticsearch (et). `Elasticsearch==7.9.0 requests_aws4auth` 2. Créez une fonction Lambda appelée `s3toelasticsearch` et téléchargez le code source (`s3toelasticsearch.py`) depuis le GitHubréférentiel. 3. Importez la dépendance Python sous forme de couche Lambda. 4. Attachez les politiques IAM `S3ReadOnly` et	AWS général

Tâche	Description	Compétences requises
	`AmazonOpenSearchServiceReadOnlyAccess` à la fonction Lambda.	

Tâche	Description	Compétences requises
Créez le cluster OpenSearch de services.	Création du cluster 1. Créez un cluster OpenSearch de services. Lorsque vous créez le cluster, procédez comme suit : • **Note** Créez un utilisateur principal et un mot de passe pour le cluster que vous pouvez utiliser pour vous connecter aux OpenSearch tableaux de bord. : Cette étape n'est pas obligatoire si vous utilisez l'authentification via Amazon Cognito. • Optez pour un contrôle d'accès précis. Cela vous donne des moyens supplémentaires de contrôler l'accès à vos données dans le OpenSearch Service. 2. Copiez l'URL du domaine et transmettez-la en tant que	AWS général

Tâche	Description	Compétences requises
	variable d'environnement « HOST » à la fonction Lambda. `s3toelasticsearch` Accorder l'accès au rôle IAM Pour fournir un accès détaillé au rôle IAM (`arn:aws:iam::**:role/service-role/s3toelasticsearch-role-**`) de la fonction Lambda, procédez comme suit : 1. Connectez-vous à OpenSearch Dashboards en tant qu'utilisateur principal. 2. Choisissez l'onglet Sécurité, puis sélectionnez Roles, all_access, Map user, Backend roles. 3. Ajoutez le nom de ressource Amazon (ARN) du rôle IAM de la fonction Lambda, puis choisissez Enregistrer. Pour plus d'informations, consultez la section Mappage des rôles aux utilisateurs dans la documentation du OpenSearch service.	

Tâche	Description	Compétences requises
Créez des Step Functions pour l'orchestration.	1. Créez une machine à états Step Functions avec le flux standard. La définition est incluse dans le GitHub référentiel. 2. Dans le script JSON, remplacez la fonction Lambda par la fonction ARNs ARNs from the Lambda de votre environnement.	AWS général

Déployer et exécuter

Tâche	Description	Compétences requises
Téléchargez les fichiers d'entrée et les cahiers dans le compartiment S3.	Téléchargez des exemples de fichiers depuis le dossier d'échantillons du GitHub référentiel et chargez-les dans le compartiment S3 que vous avez créé précédemment. 1. `Mockedcopy.cpy` Téléchargez-le et `acctix.cpy` placez-le `<S3_Bucket>/copybook` dans le dossier. 2. Téléchargez les fichiers d'entrée `Modedupdate.txt` et les `acctindex.cpy` exemples de fichiers	AWS général

Tâche	Description	Compétences requises
	d'entrée `<S3_Bucket>/input` dans le dossier.	

Tâche	Description	Compétences requises

Invoquez les Step Functions.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Step Functions.
	2. Dans le volet de navigation, sélectionnez State machines.
	3. Choisissez votre machine à états, puis choisissez Démarrer l'exécution.
	4. Dans la zone de saisie, entrez le chemin du copybook/fichier suivant en tant que variable JSON vers le compartiment S3, puis choisissez Démarrer l'exécution.
	
	`{ "s3_copybook_bucket_name": "<BUCKET NAME>", "s3_copybook_bucket_key": "<COPYBOOK PATH>", "s3_source_bucket_name": "<BUCKET NAME", "s3_source_bucket_key": "INPUT FILE PATH" }`
	
	Par exemple :
	
	`{`
		AWS général

Tâche	Description	Compétences requises

	<pre>"s3_copybook_bucket_name": "fileaidtest",
	"s3_copybook_bucket_key": "copybook/acctix.cpy",
	"s3_source_bucket_name": "fileaidtest",
	"s3_source_bucket_key": "input/acctindex"
	}</pre>	

Validez l'exécution du flux de travail dans Step Functions.	Dans la console Step Functions, passez en revue l'exécution du flux de travail dans l'inspecteur Graph. Les états d'exécution sont codés par couleur pour représenter l'état d'exécution. Par exemple, le bleu indique En cours, le vert indique la réussite et le rouge indique l'échec. Vous pouvez également consulter le tableau dans la section Historique des événements d'exécution pour obtenir des informations plus détaillées sur les événements d'exécution. Pour un exemple d'exécution d'un flux de travail graphique, voir le graphe Step Functions dans la section Informations supplémentaires de ce modèle.	AWS général

Tâche	Description	Compétences requises
Validez les journaux de livraison sur Amazon CloudWatch.	1. Connectez-vous à AWS Management Console et ouvrez la console CloudWatch . 2. Dans le volet de navigation, développez Logs, puis choisissez Log groups. 3. Dans le champ de recherche, recherchez le groupe de journaux de la `s3toelasticsearch` fonction. Pour un exemple de journaux de livraison réussis, consultez les journaux de CloudWatch livraison dans la section Informations supplémentaires de ce modèle.	AWS général

Tâche	Description	Compétences requises
Validez le fichier formaté dans les OpenSearch tableaux de bord et effectuez des opérations sur les fichiers.	1. Connectez-vous à l'AWS Management Console. Sous Analytics, sélection nez Amazon OpenSearch Service. 2. Dans le volet de navigation, sélectionnez Domains. 3. Dans le champ de recherche, entrez l'URL de votre domaine dans OpenSearch Dashboards. 4. Choisissez votre tableau de bord, puis connectez-vous en tant qu'utilisateur principal. 5. Parcourez les données indexées sous forme de tableau. 6. Comparez le fichier d'entrée au fichier de sortie formaté (document indexé) dans OpenSearch les tableaux de bord. La vue du tableau de bord montre les en-têtes de colonne ajoutés pour vos fichiers formatés. Vérifiez que les données source de vos fichiers d'entrée non formatés correspondent aux données cibles dans la vue du tableau de bord. 7. Effectuez des actions telles que des recherches (par	AWS général

Tâche	Description	Compétences requises
	exemple, en utilisant des noms de champs, des valeurs ou des expressions), des filtres et des opérations DQL (Dashboard Query Language) sur le fichier indexé.	

Ressources connexes

Références

- Exemple de cahier COBOL (documentation IBM)
- Aide aux fichiers BMC Compuware (documentation BMC)

Didacticiels

- Tutoriel : Utilisation d'un déclencheur Amazon S3 pour appeler une fonction Lambda (documentation AWS Lambda)
- Comment créer un flux de travail sans serveur avec AWS Step Functions et AWS Lambda (documentation AWS)
- Utilisation OpenSearch de tableaux de bord avec Amazon OpenSearch Service (documentation AWS)

Informations supplémentaires

Graphe Step Functions

L'exemple suivant montre un graphe Step Functions. Le graphique montre l'état d'exécution des fonctions Lambda utilisées dans ce modèle.

CloudWatch journaux de livraison

L'exemple suivant montre les journaux de livraison réussis pour l'exécution de l'`s3toelasticsearch`exécution.

2008-10T 15:53:33 .033-05:00	Nombre de documents de traitement : 100	
	2008-10T 15:53:33 .171-05:00	[INFO] 02:08-10T 20:53:33 .171 Z a1b2c3d4-5678-90ab-cdef- Post:443/ _BULK [statut : 200 requête:0 ,100 s] EXAMPLE11111 https://search-essearch-3h4uqclifeqaj2vg4mphe7ffle.us-east-2.es.amazonaws.com
	2008-10T 15:53:33 .172-05:00	Rédaction en masse réussie : 100 documents

Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age

Créée par Richard Milner-Watts (AWS)

Récapitulatif

Ce modèle fournit un exemple d'environnement de conteneur pour exécuter des charges de travail mainframe qui ont été modernisées à l'aide de l'outil Blu Age. Blu Age convertit les charges de travail des ordinateurs centraux existants en code Java moderne. Ce modèle enveloppe l'application Java afin que vous puissiez l'exécuter à l'aide de services d'orchestration de conteneurs tels qu'Amazon Elastic Container Service (Amazon ECS) ou Amazon Elastic Kubernetes Service (Amazon EKS).

Pour plus d'informations sur la modernisation de vos charges de travail à l'aide de Blu Age et des services AWS, consultez les publications AWS Prescriptive Guidance suivantes :

- Exécution de charges de travail de mainframe Blu Age modernisées sur une infrastructure AWS sans serveur
- Déployez un environnement pour les applications Blu Age conteneurisées à l'aide de Terraform

Pour obtenir de l'aide sur l'utilisation de Blu Age afin de moderniser les charges de travail de votre mainframe, contactez l'équipe Blu Age en sélectionnant Contacter nos experts sur le site Web de Blu Age. Pour obtenir de l'aide concernant la migration de vos charges de travail modernisées vers AWS, leur intégration aux services AWS et leur mise en production, contactez votre responsable de compte AWS ou remplissez le formulaire AWS Professional Services.

Conditions préalables et limitations

Prérequis

- Une application Java modernisée créée par Blu Age. À des fins de test, ce modèle fournit un exemple d'application Java que vous pouvez utiliser comme preuve de concept.
- Un environnement Docker que vous pouvez utiliser pour créer le conteneur.

Limites

Selon la plate-forme d'orchestration de conteneurs que vous utilisez, les ressources pouvant être mises à la disposition du conteneur (telles que le processeur, la RAM et le stockage) peuvent être

limitées. Par exemple, si vous utilisez Amazon ECS avec AWS Fargate, consultez la documentation Amazon ECS pour connaître les limites et les considérations.

Architecture

Pile technologique source

- Âge bleu
- Java

Pile technologique cible

- Docker

Architecture cible

Le schéma suivant montre l'architecture de l'application Blu Age dans un conteneur Docker.

1. Le point d'entrée du conteneur est le script wrapper. Ce script bash est chargé de préparer l'environnement d'exécution de l'application Blu Age et de traiter les sorties.
2. Les variables d'environnement du conteneur sont utilisées pour configurer les variables du script wrapper, telles que les noms de bucket Amazon Simple Storage Service (Amazon S3) et les informations d'identification de base de données. Les variables d'environnement sont fournies soit par AWS Secrets Manager, soit par Parameter Store, une fonctionnalité d'AWS Systems Manager. Si vous utilisez Amazon ECS comme service d'orchestration de conteneurs, vous pouvez également coder en dur les variables d'environnement dans la définition de tâche Amazon ECS.
3. Le script wrapper est chargé d'extraire tous les fichiers d'entrée du compartiment S3 vers le conteneur avant d'exécuter l'application Blu Age. L'interface de ligne de commande AWS (AWS CLI) est installée dans le conteneur. Cela fournit un mécanisme permettant d'accéder aux objets stockés dans Amazon S3 via le point de terminaison VPC (Virtual Private Cloud) de la passerelle.
4. Le fichier Java Archive (JAR) de l'application Blu Age peut avoir besoin de communiquer avec d'autres sources de données, telles qu'Amazon Aurora.
5. Une fois terminé, le script wrapper fournit les fichiers de sortie obtenus dans un compartiment S3 pour un traitement ultérieur (par exemple, par Amazon CloudWatch Logging Services). Le modèle

prend également en charge l'envoi de fichiers journaux compressés à Amazon S3, si vous utilisez une alternative à la CloudWatch journalisation standard.

Outils

Services AWS

- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.

Outils

- Docker est une plate-forme logicielle permettant de créer, de tester et de déployer des applications. Docker regroupe les logiciels dans des unités standardisées appelées conteneurs, qui contiennent tout ce dont le logiciel a besoin pour fonctionner, notamment les bibliothèques, les outils système, le code et le runtime. Vous pouvez utiliser Docker pour déployer et faire évoluer des applications dans n'importe quel environnement.
- Bash est une interface en langage de commande (shell) pour le système d'exploitation GNU.
- Java est le langage de programmation et l'environnement de développement utilisés dans ce modèle.
- Blu Age est un outil de modernisation du mainframe AWS qui convertit les charges de travail du mainframe existant, y compris le code d'application, les dépendances et l'infrastructure, en charges de travail modernes pour le cloud.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel de conteneurs d'échantillons GitHub Blu Age.

Bonnes pratiques

- Externalisez les variables pour modifier le comportement de votre application en utilisant des variables d'environnement. Ces variables permettent à la solution d'orchestration de conteneurs de modifier l'environnement d'exécution sans reconstruire le conteneur. Ce modèle inclut des exemples de variables d'environnement qui peuvent être utiles pour les applications Blu Age.

- Validez toutes les dépendances des applications avant d'exécuter votre application Blu Age. Par exemple, vérifiez que la base de données est disponible et que les informations d'identification sont valides. Écrivez des tests dans le script wrapper pour vérifier les dépendances, et échouez prématurément si elles ne sont pas satisfaites.
- Utilisez la journalisation détaillée dans le script wrapper. L'interaction directe avec un conteneur en cours d'exécution peut s'avérer difficile, en fonction de la plate-forme d'orchestration et de la durée du travail. Assurez-vous que le résultat utile est écrit pour aider `STDOUT` à diagnostiquer les problèmes éventuels. Par exemple, la sortie peut inclure le contenu du répertoire de travail de l'application avant et après l'exécution de l'application.

Épopées

Obtenir un fichier JAR d'application Blu Age

Tâche	Description	Compétences requises
Option 1 - Travaillez avec Blu Age pour obtenir le fichier JAR de votre application.	Le contenant de ce modèle nécessite une application Blu Age. Vous pouvez également utiliser l'exemple d'application Java fourni avec ce modèle pour un prototype. Travaillez avec l'équipe Blu Age pour obtenir un fichier JAR pour votre application qui pourra être intégré au conteneur. Si le fichier JAR n'est pas disponible, reportez-vous à la tâche suivante pour utiliser l'exemple d'application à la place.	Architecte du cloud
Option 2 : créez ou utilisez le fichier JAR d'application d'exemple fourni.	Ce modèle fournit un exemple de fichier JAR prédéfini. Ce fichier affiche les variables d'environnement de l'applica	Développeur d’applications

Tâche	Description	Compétences requises
	tion STDOUT avant de dormir pendant 30 secondes et de quitter l'application. Ce fichier est nommé `bluAgeSample.jar` et se trouve dans le dossier docker du GitHub dépôt. Si vous souhaitez modifier le code et créer votre propre version du fichier JAR, utilisez le code source situé à l'adresse. /java_ sample/src/ sample _java_app.java dans le dépôt. GitHub Vous pouvez utiliser le script de compilati on à l'adresse. /java_sam ple/build.sh pour compiler le code source Java et créer un nouveau fichier JAR.	

Construisez le conteneur Blu Age

Tâche	Description	Compétences requises
Clonez le GitHub dépôt.	Clonez le référentiel d'exemple s de code à l'aide de la commande : `git clone https://g ithub.com/aws-samp les/aws-blu-age-sa mple-container`	AWS DevOps

Tâche	Description	Compétences requises
Utilisez Docker pour créer le conteneur.	Utilisez Docker pour créer le conteneur avant de le transférer vers un registre Docker tel qu'Amazon ECR : 1. Depuis le terminal de votre choix, accédez au `docker` dossier de votre GitHub dépôt local. 2. Utilisez cette commande pour créer le conteneur : `docker build -t <tag> .` où `<tag>` est le nom du conteneur que vous souhaitez utiliser.	AWS DevOps
Testez le conteneur Blu Age.	(Facultatif) Si nécessaire, testez le conteneur localement à l'aide de la commande : `docker run -it <tag> / bin/bash`	AWS DevOps

Tâche	Description	Compétences requises
Authentifiez-vous auprès de votre référentiel Docker.	Si vous prévoyez d'utiliser Amazon ECR, suivez les instructions de la documentation Amazon ECR pour installer et configurer l'AWS CLI et authentifier la CLI Docker dans votre registre par défaut. Nous vous recommandons d'utiliser la get-login-password commande pour l'authentification. **Note** La console Amazon ECR fournit une version préremplie de cette commande si vous utilisez le bouton Afficher les commandes push. Pour plus d'informations, consultez la documentation Amazon ECR. `aws ecr get-login-password --region <region> | docker login --username AWS --password-stdin <account>.dkr.ecr.`	AWS DevOps

Tâche	Description	Compétences requises
	`<region>.amazonaws.com` Si vous ne prévoyez pas d'utiliser Amazon ECR, suivez les instructions fournies pour votre système de registre de conteneurs.	
Créez un référentiel de conteneurs.	Créez un référentiel dans Amazon ECR. Pour obtenir des instructions, consultez le modèle Déployer un environnement pour les applications Blu Age conteneurisées à l'aide de Terraform. Si vous utilisez un autre système de registre de conteneurs, suivez les instructions fournies pour ce système.	AWS DevOps

Tâche	Description	Compétences requises

Marquez et transférez votre conteneur vers le référentiel cible.	Si vous utilisez Amazon ECR :
	1. Marquez l'image Docker locale avec le registre et le référentiel Amazon ECR, afin de pouvoir la transférer vers votre référentiel distant :
	`docker tag <tag>:latest <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>`
	2. Transférez l'image vers le dépôt distant :
	`docker push <account>.dkr.ecr.<region>.amazonaws.com/<repository>:<versionNumber>`
	Pour plus d'informations, consultez la section Envoyer une image Docker dans le guide de l'utilisateur Amazon ECR.
		AWS DevOps

Ressources connexes

Ressources AWS

- Référentiel d'exemples de conteneurs AWS Blu Age

- Exécution de charges de travail de mainframe Blu Age modernisées sur une infrastructure AWS sans serveur
- Déployez un environnement pour les applications Blu Age conteneurisées à l'aide de Terraform
- Utilisation d'Amazon ECR avec l'AWS CLI (Amazon ECR User Guide)
- Authentification du registre privé (Guide de l'utilisateur Amazon ECR)
- Documentation Amazon ECS
- Documentation Amazon EKS

Ressources supplémentaires

- Site web de Blu Age
- Site web Docker

Convertissez et décompressez les données EBCDIC en ASCII sur AWS à l'aide de Python

Créée par Luis Gustavo Dantas (AWS)

Récapitulatif

Les mainframes hébergeant généralement des données commerciales critiques, la modernisation des données est l'une des tâches les plus importantes lors de la migration des données vers le cloud Amazon Web Services (AWS) ou un autre environnement ASCII (American Standard Code for Information Interchange). Sur les ordinateurs centraux, les données sont généralement codées au format EBCDIC (Extended Binary Coded Decimal Interchange Code). L'exportation d'une base de données, d'une méthode d'accès au stockage virtuel (VSAM) ou de fichiers plats produit généralement des fichiers EBCDIC binaires compressés, dont la migration est plus complexe. La solution de migration de base de données la plus couramment utilisée est la capture des données modifiées (CDC), qui, dans la plupart des cas, convertit automatiquement le codage des données. Cependant, les mécanismes CDC peuvent ne pas être disponibles pour ces bases de données, VSAM ou fichiers plats. Pour ces fichiers, une autre approche est nécessaire pour moderniser les données.

Ce modèle décrit comment moderniser les données EBCDIC en les convertissant au format ASCII. Après la conversion, vous pouvez charger les données dans des bases de données distribuées ou demander aux applications du cloud de les traiter directement. Le modèle utilise le script de conversion et les fichiers d'exemple du mainframe-data-utilities GitHub référentiel.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un fichier d'entrée EBCDIC et le cahier COBOL (Common Business Oriented Language) correspondant. Un exemple de fichier EBCDIC et de cahier COBOL sont inclus dans le référentiel. mainframe-data-utilities GitHub Pour plus d'informations sur les copybooks COBOL, consultez le guide de programmation Enterprise COBOL for z/OS 6.4 sur le site Web d'IBM.

Limites

- Les mises en page de fichiers définies dans les programmes COBOL ne sont pas prises en charge. Ils doivent être mis à disposition séparément.

Versions du produit

- Python version 3.8 ou ultérieure

Architecture

Pile technologique source

- Données EBCDIC sur un ordinateur central
- Cahier COBOL

Pile technologique cible

- Instance Amazon Elastic Compute Cloud (Amazon EC2) dans un cloud privé virtuel (VPC)
- Amazon Elastic Block Store (Amazon EBS)
- Python et ses packages requis, JavaScript Object Notation (JSON), sys et datetime
- Fichier plat ASCII prêt à être lu par une application moderne ou chargé dans une table de base de données relationnelle

Architecture cible

Le schéma d'architecture montre le processus de conversion d'un fichier EBCDIC en fichier ASCII sur une instance : EC2

1. À l'aide du script parse_copybook_to_json.py, vous convertissez le cahier COBOL en fichier JSON.
2. À l'aide du fichier JSON et du script extract_ebcdic_to_ascii.py, vous convertissez les données EBCDIC en fichier ASCII.

Automatisation et mise à l'échelle

Une fois que les ressources nécessaires pour les premières conversions de fichiers manuelles sont en place, vous pouvez automatiser la conversion de fichiers. Ce modèle n'inclut pas d'instructions

pour l'automatisation. Il existe plusieurs méthodes pour automatiser la conversion. Voici un aperçu de l'une des approches possibles :

1. Encapsulez l'interface de ligne de commande AWS (AWS CLI) et les commandes de script Python dans un script shell.
2. Créez une fonction AWS Lambda qui soumet de manière asynchrone le job de script shell à une instance. EC2 Pour plus d'informations, consultez la section Planification de tâches SSH à l'aide d'AWS Lambda.
3. Créez un déclencheur Amazon Simple Storage Service (Amazon S3) qui invoque la fonction Lambda chaque fois qu'un ancien fichier est chargé. Pour plus d'informations, consultez Utilisation d'un déclencheur Amazon S3 pour appeler une fonction Lambda.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les faire rapidement évoluer vers le haut ou vers le bas.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.

Autres outils

- GitHubest un service d'hébergement de code qui fournit des outils de collaboration et de contrôle de version.
- Python est un langage de programmation de haut niveau.

Référentiel de code

Le code de ce modèle est disponible dans le mainframe-data-utilities GitHub référentiel.

Épopées

Préparer l' EC2 instance

Tâche	Description	Compétences requises
Lancez une EC2 instance.	L' EC2 instance doit disposer d'un accès Internet sortant. Cela permet à l'instance d'accéder au code source Python disponible sur GitHub. Pour créer l'instance, procédez comme suit : 1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2. 2. Lancez une instance EC2 Linux. Utilisez une adresse IP publique et autorisez l'accès entrant via le port 22. Assurez-vous que la taille de stockage de l'instance est au moins deux fois supérieure à celle du fichier de données EBCDIC. Pour obtenir des instructions, consultez la EC2 documentation Amazon.	AWS général
Installez Git.	1. À l'aide d'un client Secure Shell (SSH), connectez-vous à l' EC2 instance que vous venez de lancer. Pour plus d'informations,	AWS, Linux en général

Tâche	Description	Compétences requises

	consultez Connect to your Linux instance.
	2. Dans la EC2 console Amazon, exécutez la commande suivante. Cela installe Git sur l' EC2 instance.
	`sudo yum install git`
	3. Exécutez la commande suivante et vérifiez que Git a été correctement installé.
	`git --version`	

Tâche	Description	Compétences requises

Installez Python.	1. Dans la EC2 console Amazon, exécutez la commande suivante. Cela installe Python sur l' EC2 instance.
	`sudo yum install python3`
	2. Dans la EC2 console Amazon, exécutez la commande suivante. Cela installe Pip3 sur l'instance. EC2
	`sudo yum install python3-pip`
	3. Dans la EC2 console Amazon, exécutez la commande suivante. Ceci installe le SDK AWS pour Python (Boto3) sur l'instance. EC2
	`sudo pip3 install boto3`
	4. Dans la EC2 console Amazon, exécutez la commande suivante, où se `<us-east-1>` trouve le code de votre région AWS. Pour obtenir la liste complète des codes de région, consultez la section
		AWS, Linux en général

Tâche	Description	Compétences requises
	Régions disponibles dans la EC2 documentation Amazon. `export AWS_DEFAULT_REGION=<us-east-1>`	
Clonez le GitHub dépôt.	1. Dans la EC2 console Amazon, exécutez la commande suivante. Cela clone le mainframe-data-utilitiesréférentiel depuis GitHub et ouvre l'emplacement de copie par défaut, le home dossier. `git clone https://github.com/aws-samples/mainframe-data-utilities.git` 2. Dans le home dossier, vérifiez que le `mainframe-data-utilities` dossier est présent.	AWS général, GitHub

Créez le fichier ASCII à partir des données EBCDIC

Tâche	Description	Compétences requises
Analysez le cahier COBOL dans le fichier de mise en page JSON.	Dans le `mainframe-data-utilities` dossier, exécutez le script parse_copybook_to_json.py. Ce module d'automatisation lit la mise	AWS, Linux en général

Tâche	Description	Compétences requises

	en page du fichier à partir d'un cahier COBOL et crée un fichier JSON. Le fichier JSON contient les informations nécessaires pour interpréter et extraire les données du fichier source. Cela crée les métadonnées JSON à partir du cahier COBOL.
	
	La commande suivante convertit le cahier COBOL en fichier JSON.
	
	`python3 parse_copybook_to_json.py \ -copybook LegacyReference/COBPACK2.cpy \ -output sample-data/cobpack2-list.json \ -dict sample-data/cobpack2-dict.json \ -ebcdic sample-data/COBPACK.OUTFILE.txt \ -ascii sample-data/COBPACK.ASCII.txt \ -print 10000`
	
	Le script affiche les arguments reçus.
	
	`---------- ---------- ---------- ---------- Copybook file..... .....| LegacyReference/COBPACK2.cpy`	

Tâche	Description	Compétences requises

	<pre>Parsed copybook (JSON List).| sample-data/cobpack2-list.json
	JSON Dict (documentation)...| sample-data/cobpack2-dict.json
	ASCII file.....| sample-data/COBPACK.ASCII.txt
	EBCDIC file.....| sample-data/COBPACK.OUTFILE.txt
	Print each.....| 10000
	---------- 	
	---------- 	
	---------- 	
	----------</pre> Pour plus d'informations sur les arguments, consultez le fichier README du GitHub référentiel.	

Tâche	Description	Compétences requises
Inspectez le fichier de mise en page JSON.	1. Accédez au chemin de sortie défini dans le script parse_copybook_to_json.py. 2. Vérifiez l'heure de création du fichier sample-data/cobpack2-list.json pour confirmer que vous avez sélectionné le fichier de mise en page JSON approprié. 3. Examinez le fichier JSON et vérifiez que son contenu est similaire au suivant. `"input": "extract-ebcdic-to-ascii/COBPACK.OUTFILE.txt", "output": "extract-ebcdic-to-ascii/COBPACK.ASCII.txt", "max": 0, "skip": 0, "print": 10000, "lrecl": 150, "rem-low-values": true, "separator": "|", "transf": [ { "type": "ch", "bytes": 19, "name": "OUTFILE-TEXT" }`	AWS, JSON en général

Tâche	Description	Compétences requises
	Les attributs les plus importants du fichier de mise en page JSON sont les suivants : • `input`— Contient le chemin du fichier EBCDIC à convertir • `output`— Définit le chemin où le fichier ASCII sera généré • `lrecl`— Spécifie la taille en octets de la longueur logique de l'enregistrement • `transf`— Liste tous les champs et leur taille en octets Pour plus d'informations sur le fichier de mise en page JSON, consultez le fichier README dans le GitHub référentiel.	

Tâche	Description	Compétences requises

Créez le fichier ASCII.	Exécutez le script extract_ebcdic_to_ascii.py, qui est inclus dans le GitHub référentiel cloné. Ce script lit le fichier EBCDIC et écrit un fichier ASCII converti et lisible.
	`python3 extract_ebcdic_to_ascii.py -local-json sample-data/cobpack2-list.json`
	Lorsque le script traite les données EBCDIC, il imprime un message pour chaque lot de 10 000 enregistrements. Consultez l'exemple suivant.
	`---------- 2023-05-15 21:21:46.322253 | Local Json file | -local-json | sample-data/cobpack2-list.json 2023-05-15 21:21:47.034556 | Records processed | 10000 2023-05-15 21:21:47.736434 | Records processed | 20000 2023-05-15 21:21:48.441696 | Records processed | 30000`
		AWS général

Tâche	Description	Compétences requises

	<pre>2023-05-15 21:21:49.
	173781 | Records
	 processed | 40000
	2023-05-15 21:21:49.
	874779 | Records
	 processed | 50000
	2023-05-15 21:21:50.
	705873 | Records
	 processed | 60000
	2023-05-15 21:21:51.
	609335 | Records
	 processed | 70000
	2023-05-15 21:21:52.
	292989 | Records
	 processed | 80000
	2023-05-15 21:21:52.
	938366 | Records
	 processed | 89280
	2023-05-15 21:21:52.
	938448 Seconds 6.616232</pre>
	Pour plus d'informations sur la modification de la fréquence d'impression, consultez le fichier README du GitHub référentiel.	

Tâche	Description	Compétences requises
Examinez le fichier ASCII.	1. Vérifiez l'heure de création du fichier extract-ebcdic-to-ascii/cobpack.ascii.txt pour vérifier qu'il a été créé récemment. 2. Dans la EC2 console Amazon, entrez la commande suivante. Cela ouvre le premier enregistrement du fichier ASCII. `head sample-data/COBPACK.ASCII.txt -n 1| xxd` 3. Examinez le contenu du premier enregistrement. Les fichiers EBCDIC étant généralement binaires, ils ne contiennent pas de caractères spéciaux CRLF (Carriage Return and Line Feed). Le script extract_ebcdic_to_ascii.py ajoute un caractère de tube en tant que séparateur de colonne, défini dans les paramètres du script. Si vous avez utilisé l'exemple de fichier EBCDIC fourni, voici le premier enregistrement du fichier ASCII.	AWS, Linux en général

Tâche	Description	Compétences requises
	00000000: 2d30 3030 3030 3030 3030 3130 3030 3030 -000000000100000 00000010: 3030 307c 3030 3030 3030 3030 3031 3030 000|00000 0000100 00000020: 3030 3030 3030 7c2d 3030 3030 3030 3030 000000|-0 0000000 00000030: 3031 3030 3030 3030 3030 7c30 7c30 7c31 0100000000| 0|0|1 00000040: 3030 3030 3030 3030 7c2d 3130 3030 3030 00000000| -100000 00000050: 3030 307c 3130 3030 3030 3030 307c 2d31 000|10000 0000|-1 00000060: 3030 3030 3030 3030 7c30 3030 3030 7c30 00000000| 00000|0 00000070: 3030 3030 7c31 3030 3030 3030 3030 7c2d 0000|1000 00000|- 00000080: 3130 3030 3030 3030 307c 3030 3030 3030 100000000| 000000 00000090: 3030 3030 3130 3030 3030 3030 307c 2d30 000010000 0000|-0 000000a0: 3030 3030 3030 3030 3031 3030	

Tâche	Description	Compétences requises
	3030 3030 000000000 1000000 000000b0: 3030 7c41 7c41 7c0a 00|A|A|.	

Tâche	Description	Compétences requises
Évaluez le fichier EBCDIC.	Dans la EC2 console Amazon, entrez la commande suivante. Cela ouvre le premier enregistrement du fichier EBCDIC. `head sample-data/COBPACK.OUTFILE.txt -c 150 | xxd` Si vous avez utilisé l'exemple de fichier EBCDIC, voici le résultat. `00000000: 60f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 f0f0 `........ ....` `00000010: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 f0f0 ....` `00000020: f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f0f0 f1f0 ....` `00000030: f0f0 f0f0 f0f0 d000 0000 0005 f5e1 00fa ....` `00000040: 0a1f 0000 0000 0005 f5e1 00ff ffff fffa ....` `00000050: 0a1f 0000 000f 0000 0c10 0000 000f 1000 ....`	Informations générales sur AWS, Linux, EBCDIC

Tâche	Description	Compétences requises
	00000060: 0000 0d00 0000 0000 1000 0000 0f00 0000 .... 00000070: 0000 1000 0000 0dc1 c100 0000 0000 0000 .... 00000080: 0000 0000 0000 0000 0000 0000 0000 0000 .... 00000090: 0000 0000 0000 ...... Pour évaluer l'équivalence entre les fichiers source et cible, une connaissance approfondie de l'EBCDIC est requise. Par exemple, le premier caractère de l'exemple de fichier EBCDIC est un tiret (). - Dans la notation hexadécimale du fichier EBCDIC, ce caractère est représenté par60, et dans la notation hexadécimale du fichier ASCII, ce caractère est représenté par. 2D Pour un tableau EBCDIC-to-ASCII de conversion, voir EBCDIC en ASCII sur le site Web d'IBM.	

Ressources connexes

Références

- Le jeu de caractères EBCDIC (documentation IBM)
- EBCDIC vers ASCII (documentation IBM)
- COBOL (documentation IBM)
- Concepts de base du JCL (documentation IBM)
- Connectez-vous à votre instance Linux (EC2 documentation Amazon)

Didacticiels

- Planification de tâches SSH à l'aide d'AWS Lambda (article de blog AWS)
- Utilisation d'un déclencheur Amazon S3 pour appeler une fonction Lambda (documentation AWS Lambda)

Convertissez des fichiers mainframe du format EBCDIC au format ASCII délimité par des caractères dans Amazon S3 à l'aide d'AWS Lambda

Créée par Luis Gustavo Dantas (AWS)

Récapitulatif

Ce modèle explique comment lancer une fonction AWS Lambda qui convertit automatiquement les fichiers EBCDIC (Extended Binary Coded Decimal Interchange Code) du mainframe en fichiers ASCII (American Standard Code for Information Interchange) délimités par des caractères. La fonction Lambda s'exécute une fois les fichiers ASCII chargés dans un bucket Amazon Simple Storage Service (Amazon S3). Après la conversion des fichiers, vous pouvez lire les fichiers ASCII sur des charges de travail basées sur x86 ou charger les fichiers dans des bases de données modernes.

L'approche de conversion de fichiers illustrée dans ce modèle peut vous aider à surmonter les défis liés à l'utilisation de fichiers EBCDIC dans des environnements modernes. Les fichiers codés en EBCDIC contiennent souvent des données représentées dans un format binaire ou décimal compressé, et les champs sont de longueur fixe. Ces caractéristiques créent des obstacles car les charges de travail modernes basées sur le x86 ou les environnements distribués fonctionnent généralement avec des données codées en ASCII et ne peuvent pas traiter les fichiers EBCDIC.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Compartiment S3
- Un utilisateur d'AWS Identity and Access Management (IAM) disposant d'autorisations administratives
- AWS CloudShell
- Python 3.8.0 ou version ultérieure
- Un fichier plat codé en EBCDIC et sa structure de données correspondante dans un cahier COBOL (Common Business Oriented Language)

> **Note**
>
> Ce modèle utilise un exemple de fichier EBCDIC (Client.EBCDIC.txt) et le cahier COBOL correspondant (Cobks05.cpy). Les deux fichiers sont disponibles dans le GitHub mainframe-data-utilitiesréférentiel.

Limites

- Les cahiers COBOL contiennent généralement plusieurs définitions de mise en page. Le mainframe-data-utilitiesprojet peut analyser ce type de cahier mais ne peut pas déduire quelle mise en page prendre en compte lors de la conversion des données. Cela est dû au fait que les cahiers ne tiennent pas compte de cette logique (qui reste dans les programmes COBOL à la place). Par conséquent, vous devez configurer manuellement les règles de sélection des mises en page après avoir analysé le cahier.
- Ce modèle est soumis à des quotas Lambda.

Architecture

Pile technologique source

- IBM z/OS, IBM i et autres systèmes EBCDIC
- Fichiers séquentiels avec données codées en EBCDIC (tels que les déchargements IBM Db2)
- Cahier COBOL

Pile technologique cible

- Amazon S3
- Notification d'événement Amazon S3
- IAM
- fonction Lambda
- Python 3.8 ou version ultérieure
- Utilitaires de données du mainframe
- métadonnées JSON
- Fichiers ASCII délimités par des caractères

Architecture cible

Le schéma suivant montre une architecture permettant de convertir les fichiers EBCDIC du mainframe en fichiers ASCII.

Le schéma suivant illustre le flux de travail suivant :

1. L'utilisateur exécute le script d'analyse du cahier pour convertir le cahier COBOL en fichier JSON.
2. L'utilisateur télécharge les métadonnées JSON dans un compartiment S3. Cela rend les métadonnées lisibles par la fonction Lambda de conversion de données.
3. L'utilisateur ou un processus automatisé télécharge le fichier EBCDIC dans le compartiment S3.
4. L'événement de notification S3 déclenche la fonction Lambda de conversion de données.
5. AWS vérifie les autorisations de lecture/écriture du compartiment S3 pour la fonction Lambda.
6. Lambda lit le fichier depuis le compartiment S3 et convertit localement le fichier EBCDIC en ASCII.
7. Lambda enregistre l'état du processus sur Amazon. CloudWatch
8. Lambda réécrit le fichier ASCII sur Amazon S3.

> **Note**
>
> Le script d'analyse du copybook ne s'exécute qu'une seule fois, après avoir converti les métadonnées au format JSON, puis chargé ces données dans un compartiment S3. Après la conversion initiale, tout fichier EBCDIC utilisant le même fichier JSON que celui chargé dans le compartiment S3 utilisera les mêmes métadonnées.

Outils

Outils AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

- AWS CloudShell est un shell basé sur un navigateur que vous pouvez utiliser pour gérer les services AWS à l'aide de l'AWS Command Line Interface (AWS CLI) et d'une gamme d'outils de développement préinstallés.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Lambda exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Autres outils

- GitHubest un service d'hébergement de code qui fournit des outils de collaboration et de contrôle de version.
- Python est un langage de programmation de haut niveau.

Code

Le code de ce modèle est disponible dans le GitHub mainframe-data-utilitiesréférentiel.

Bonnes pratiques

Tenez compte des meilleures pratiques suivantes :

- Définissez les autorisations requises au niveau Amazon Resource Name (ARN).
- Accordez toujours des autorisations de moindre privilège pour les politiques IAM. Pour plus d'informations, consultez la section Bonnes pratiques en matière de sécurité dans IAM dans la documentation IAM.

Épopées

Création de variables d'environnement et d'un dossier de travail

Tâche	Description	Compétences requises
Créez les variables d'environ nement.	Copiez les variables d'environ nement suivantes dans	AWS général

Tâche	Description	Compétences requises

	un éditeur de texte, puis remplacez les <placehol der>valeurs de l'exemple suivant par les valeurs de vos ressources :
	
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
	
	Note
	Vous créerez des références à votre compartiment S3, à votre compte AWS et à votre région AWS ultérieurement.
	
	Pour définir des variables d'environnement, ouvrez la CloudShell console, puis copiez et collez vos variables d'environnement mises à jour sur la ligne de commande.
	
	Note
	Vous devez répéter cette étape chaque	

Tâche	Description	Compétences requises
	fois que la CloudShell session redémarre.	
Créez un dossier de travail.	Pour simplifier ultérieurement le processus de nettoyage des ressources, créez un dossier de travail en CloudShel l exécutant la commande suivante : `mkdir workdir; cd workdir` **Note** Vous devez remplacer le répertoire par le répertoire de travail (`workdir`) chaque fois que vous perdez une connexion à votre CloudShell session.	AWS général

Définition d'un rôle et d'une politique IAM

Tâche	Description	Compétences requises
Créez une politique de confiance pour la fonction Lambda.	Le convertisseur EBCDIC fonctionne selon une fonction Lambda. La fonction doit avoir un rôle IAM. Avant de créer le rôle IAM, vous devez définir un document de politique	AWS général

Tâche	Description	Compétences requises

	de confiance qui permet aux ressources d'assumer cette politique.
	
	À partir du dossier de CloudShell travail, créez un document de politique en exécutant la commande suivante :
	
	`E2ATrustPol=$(cat <<EOF`
	`{`
	`  "Version": "2012-10-17",`
	`  "Statement": [`
	`  {`
	`  "Effect": "Allow",`
	`  "Principal": {`
	`  "Service": "lambda.amazonaws.com"`
	`  },`
	`  "Action": "sts:AssumeRole"`
	`  }`
	`  ]`
	`}`
	`EOF`
	`)`
	`printf "$E2ATrustPol" > E2ATrustPol.json`	

Tâche	Description	Compétences requises
Créez le rôle IAM pour la conversion Lambda.	Pour créer un rôle IAM, exécutez la commande AWS CLI suivante depuis le dossier de CloudShell travail : `aws iam create-role --role-name E2AConvLambdaRole --assume-role-policy-document file://E2ATrustPol.json`	AWS général

Tâche	Description	Compétences requises

Créez le document de politique IAM pour la fonction Lambda.	La fonction Lambda doit disposer d'un accès en lecture-écriture au compartiment S3 et d'autorisations d'écriture pour Amazon Logs. CloudWatch
	
	Pour créer une politique IAM, exécutez la commande suivante depuis le dossier de CloudShell travail :
	
	`E2APolicy=$(cat <<EOF`
	`{`
	`"Version": "2012-10-17",`
	`"Statement": [`
	`{`
	`"Sid": "Logs",`
	`"Effect": "Allow",`
	`"Action": [`
	`"logs:PutLogEvents",`
	`"logs:CreateLogStream",`
	`"logs:CreateLogGroup"`
	`],`
	`"Resource": [`
	`"arn:aws:logs:*:*:log-group:*",`
	`"arn:aws:logs:*:*:`
		AWS général

Tâche	Description	Compétences requises

	log-group:*:log-st
	ream:*"
	            ]
	        },
	        {
	            "Sid": "S3",
	            "Effect":
	 "Allow",
	            "Action": [
	
	 "s3:GetObject",
	
	 "s3:PutObject",
	
	 "s3:GetObjectVersion"
	            ],
	            "Resource":
	 [
	
	 "arn:aws:s3:::%s/*",
	
	 "arn:aws:s3:::%s"
	            ]
	        }
	    ]
	}
	EOF
	)
	printf "$E2APolicy"
	 "$bucket" "$bucket"
	 > E2AConvLambdaPolic
	y.json	

Tâche	Description	Compétences requises
Joignez le document de politique IAM au rôle IAM.	Pour associer la politique IAM au rôle IAM, exécutez la commande suivante depuis votre dossier de CloudShell travail : `aws iam put-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy --policy-document file://E2AConvLambdaPolicy.json`	AWS général

Créez la fonction Lambda pour la conversion EBCDIC

Tâche	Description	Compétences requises
Téléchargez le code source de conversion EBCDIC.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour télécharger le code mainframe-data-utilities source depuis GitHub : `git clone https://github.com/aws-samples/mainframe-data-utilities.git mdu`	AWS général
Créez le package ZIP.	À partir du dossier de CloudShell travail, exécutez la commande suivante pour créer le package ZIP qui crée la fonction Lambda pour la conversion EBCDIC :	AWS général

Tâche	Description	Compétences requises
	`cd mdu; zip ../mdu.zip *.py; cd ..`	
Créez la fonction Lambda.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour créer la fonction Lambda pour la conversion EBCDIC : `aws lambda create-function \ --function-name E2A \ --runtime python3.9 \ --zip-file fileb://mdu.zip \ --handler extract_ebcdic_to_ascii.lambda_handler \ --role arn:aws:iam::$account:role/E2AConvLambdaRole \ --timeout 10 \ --environment "Variables={layout=$bucket/layout/}"` **Note** La disposition des variables d'environnement indique à la fonction Lambda où se trouvent les métadonnées JSON.	AWS général

Tâche	Description	Compétences requises
Créez la politique basée sur les ressources pour la fonction Lambda.	Depuis le dossier de CloudShell travail, exécutez la commande suivante pour permettre à votre notification d'événement Amazon S3 de déclencher la fonction Lambda pour la conversion EBCDIC : `aws lambda add-permi ssion \ --function-name E2A \ --action lambda:In vokeFunction \ --principal s3.amazon aws.com \ --source-arn arn:aws:s 3:::$bucket \ --source-account $account \ --statement-id 1`	AWS général

Création de la notification d'événement Amazon S3

Tâche	Description	Compétences requises
Créez le document de configuration pour la notificat ion d'événement Amazon S3.	La notification d'événement Amazon S3 lance la fonction Lambda de conversion EBCDIC lorsque des fichiers sont placés dans le dossier d'entrée. À partir du dossier de CloudShell travail, exécutez la commande suivante pour créer le document JSON pour	AWS général

Tâche	Description	Compétences requises
	la notification d'événement Amazon S3 : `{ "LambdaFunctionConfigurations": [{ "Id": "E2A", "LambdaFunctionArn": "arn:aws:lambda:%s:%s:function:E2A", "Events": ["s3:ObjectCreated:Put"], "Filter": { "Key": { "FilterRules": [{ "Name": "prefix", "Value": "input/" }] } } }] } EOF) printf "$S3E2AEvent" "$region" "$account" > S3E2AEvent.json`	

Tâche	Description	Compétences requises
Créez la notification d'événement Amazon S3.	À partir du dossier de CloudShell travail, exécutez la commande suivante pour créer la notification d'événement Amazon S3 : `aws s3api put-bucket-notification-configuration --bucket $bucket --notification-configuration file://S3E2AEvent.json`	AWS général

Création et téléchargement des métadonnées JSON

Tâche	Description	Compétences requises
Analysez le cahier COBOL.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour analyser un exemple de cahier COBOL dans un fichier JSON (qui définit comment lire et découper correctement le fichier de données) : `python3 mdu/parse_copybook_to_json.py \ -copybook mdu/LegacyReference/COBKS05.cpy \ -output CLIENT.json \`	AWS général

Tâche	Description	Compétences requises

	`-output-s3key CLIENT.ASCII.txt \`
	`-output-s3bkt $bucket \`
	`-output-type s3 \`
	`-print 25`	

Tâche	Description	Compétences requises

Ajoutez la règle de transform ation.	L'exemple de fichier de données et le cahier COBOL correspondant sont des fichiers à mises en page multiples. Cela signifie que la conversion doit découper les données en fonction de certaines règles. Dans ce cas, les octets situés aux positions 3 et 4 de chaque ligne définissent la mise en page.
	
	Dans le dossier de CloudShell travail, modifiez le `CLIENT.js` on fichier et modifiez le contenu comme suit : `"transf-rule": [],`
	
	`"transf-rule": [`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0002",`
	`"transf": "transf1"`
	`},`
	`{`
	`"offset": 4,`
	`"size": 2,`
	`"hex": "0000",`
	`"transf": "transf2"`
	`}`
	`],`
		AWS général, IBM Mainframe , Cobol

Tâche	Description	Compétences requises
Téléchargez les métadonnées JSON dans le compartiment S3.	Depuis le dossier de CloudShell travail, exécutez la commande AWS CLI suivante pour télécharger les métadonnées JSON dans votre compartiment S3 : `aws s3 cp CLIENT.json s3://$bucket/layout/CLIENT.json`	AWS général

Convertissez le fichier EBCDIC

Tâche	Description	Compétences requises
Envoyez le fichier EBCDIC au compartiment S3.	À partir du dossier de CloudShell travail, exécutez la commande suivante pour envoyer le fichier EBCDIC vers le compartiment S3 : `aws s3 cp mdu/sample-data/CLIENT.EBCDIC.txt s3://$bucket/input/` **Note** Nous vous recommandons de définir des dossiers différents pour les fichiers d'entrée (EBCDIC) et de sortie (ASCII) afin	AWS général

Tâche	Description	Compétences requises
	d'éviter d'appeler à nouveau la fonction de conversion Lambda lorsque le fichier ASCII est chargé dans le compartiment S3.	

Tâche	Description	Compétences requises

Vérifiez la sortie.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour vérifier si le fichier ASCII est généré dans votre compartiment S3 :
	`awss3 ls s3://$bucket/`
	Note
	La conversion des données peut prendre plusieurs secondes. Nous vous recommandons de vérifier la présence du fichier ASCII à quelques reprises.
	Une fois le fichier ASCII disponible, exécutez la commande suivante pour télécharger le fichier depuis le compartiment S3 vers le dossier actuel :
	`aws s3 cp s3://$bucket/ CLIENT.ASCII.txt .`
	Vérifiez le contenu du fichier ASCII :
	`head CLIENT.ASCII.txt`
		AWS général

Nettoyez l'environnement

Tâche	Description	Compétences requises

(Facultatif) Préparez les variables et le dossier.	Si vous perdez la connexion avec CloudShell, reconnectez-vous, puis exécutez la commande suivante pour transformer le répertoire en dossier de travail :
	`cd workdir`
	Assurez-vous que les variables d'environnement sont définies :
	`bucket=<your_bucket_name>`
	`account=<your_account_number>`
	`region=<your_region_code>`
		AWS général

Supprimez la configuration de notification pour le compartiment.	Depuis le dossier de CloudShell travail, exécutez la commande suivante pour supprimer la configuration des notifications d'événements Amazon S3 :
	`aws s3api put-bucket-notification-configuration \`
	`--bucket=$bucket \`
	`--notification-configuration="{}"`
		AWS général

Tâche	Description	Compétences requises
Supprimez la fonction Lambda.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour supprimer la fonction Lambda du convertisseur EBCDIC : `awslambdadelete-function--function-nameE2A`	AWS général

Supprimez le rôle et la politique IAM.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour supprimer le rôle et la politique du convertisseur EBCDIC :
	`aws iam delete-role-policy --role-name E2AConvLambdaRole --policy-name E2AConvLambdaPolicy`
	
	`aws iam delete-role --role-name E2AConvLambdaRole`
		AWS général

Tâche	Description	Compétences requises

Supprimez les fichiers générés dans le compartiment S3.	Dans le dossier de CloudShell travail, exécutez la commande suivante pour supprimer les fichiers générés dans le compartiment S3 :
	`aws s3 rm s3://$bucket/layout --recursive`
	`aws s3 rm s3://$bucket/input --recursive`
	`aws s3 rm s3://$bucket/CLIENT.ASCII.txt`
		AWS général

Supprimez le dossier de travail.	À partir du dossier de CloudShell travail, exécutez la commande suivante pour supprimer `workdir` et son contenu : `cd ..; rm -Rf workdir`	AWS général

Ressources connexes

- Utilitaires de données pour ordinateurs centraux README () GitHub
- Le jeu de caractères EBCDIC (documentation IBM)
- EBCDIC vers ASCII (documentation IBM)
- COBOL (documentation IBM)
- Utilisation d'un déclencheur Amazon S3 pour appeler une fonction Lambda (documentation AWS Lambda)

Convertissez des fichiers de données du mainframe avec des mises en page d'enregistrement complexes à l'aide de Micro Focus

Créée par Peter West

Récapitulatif

Ce modèle vous montre comment convertir des fichiers de données d'ordinateur central contenant des données non textuelles et des mises en page d'enregistrement complexes du codage de caractères EBCDIC (Extended Binary Coded Decimal Interchange Code) vers le codage de caractères ASCII (American Standard Code for Information Interchange) à l'aide d'un fichier de structure Micro Focus. Pour terminer la conversion du fichier, vous devez effectuer les opérations suivantes :

1. Préparez un fichier source unique qui décrit tous les éléments de données et les mises en page des enregistrements de votre environnement mainframe.
2. Créez un fichier de structure contenant la mise en page des données à l'aide de l'éditeur de fichiers de données Micro Focus dans le cadre des outils de fichiers de données Micro Focus Classic ou des outils de fichiers de données. Le fichier de structure identifie les données non textuelles afin que vous puissiez convertir correctement les fichiers EBCDIC en ASCII de votre ordinateur central.
3. Testez le fichier de structure à l'aide des outils de fichiers de données classiques ou des outils de fichiers de données.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Micro Focus Enterprise Developer pour Windows, disponible via AWS Mainframe Modernization

Versions du produit

- Micro Focus Enterprise Server 7.0 et versions ultérieures

Outils

- Micro Focus Enterprise Developer fournit l'environnement d'exécution pour les applications créées avec n'importe quelle variante de l'environnement de développement intégré (IDE) d'Enterprise Developer.
- Les outils de fichiers de données Micro Focus Classic vous aident à convertir, parcourir, modifier et créer des fichiers de données. Les outils de fichiers de données classiques incluent le convertisseur de fichiers de données, l'éditeur de mise en page d'enregistrement et l'éditeur de fichiers de données.
- Les outils de fichiers de données Micro Focus vous aident à créer, modifier et déplacer des fichiers de données. Les outils de fichiers de données incluent l'éditeur de fichiers de données, les utilitaires de conversion de fichiers et l'utilitaire de ligne de commande de structure de fichiers de données.

Épopées

Préparez le fichier source

Tâche	Description	Compétences requises
Identifiez les composants source.	Identifiez toutes les mises en page d'enregistrement possibles pour le fichier, y compris les redéfinitions contenant des données non textuelles. Si vos mises en page contiennent des redéfinitions, vous devez les réduire à des mises en page uniques décrivant chaque permutation possible de la structure de données. Généralement, les mises en page des enregistrements d'un fichier de	Développeur d’applications

Tâche	Description	Compétences requises
	données peuvent être décrites par les archétypes suivants : • Mise en page d'enregis trement avec uniquement des données textuelles • Mise en page des enregistr ements avec des données autres que du texte • Mise en page d'enregis trement avec des données non textuelles subordonnées à une clause REDEFINES Pour plus d'informations sur la création de mises en page d'enregistrement aplaties pour les fichiers contenant des mises en page d'enregis trement complexes, voir Réhébergement d'applica tions EBCDIC dans des environnements ASCII pour les migrations de mainframe.	

Tâche	Description	Compétences requises

Identifiez les conditions de mise en page des enregistrements.	Pour les fichiers comportant plusieurs mises en page d'enregistrement ou les fichiers contenant des mises en page complexes avec une clause REDEFINES, identifiez les données et les conditions d'un enregistrement que vous pouvez utiliser pour définir la mise en page à utiliser lors de la conversion. Nous vous recommandons de discuter de cette tâche avec un expert en la matière (PME) qui comprend les programmes qui traitent ces fichiers.
	
	Par exemple, un fichier peut contenir deux types d'enregistrement contenant des données autres que du texte. Vous pouvez inspecter la source et éventuellement trouver un code similaire au suivant :
	
	`MOVE "M" TO PART-TYPE`
	`MOVE "MAIN ASSEMBLY" TO PART-NAME`
	`MOVE "S" TO PART-TYPE`
	`MOVE "SUB ASSEMBLY 1" TO PART-NAME`
	
	Le code vous aide à identifier les éléments suivants :
		Développeur d’applications

Tâche	Description	Compétences requises
	• Le champ « PART-TYPE » est utilisé pour déterminer le type d'enregistrement • La valeur « M » est utilisée pour le « M-PART-RE CORD » • La valeur « S » est utilisée pour le « S-PART-RE CORD » Vous pouvez documenter les valeurs utilisées par ce champ pour associer les mises en page d'enregistrement aux enregistrements de données corrects du fichier.	

Tâche	Description	Compétences requises
Créez le fichier source.	Si le fichier est décrit sur plusieurs fichiers sources ou si la mise en page d'enregistrement contient des données non textuelles subordonnées à une clause REDEFINES, créez un nouveau fichier source contenant les mises en page d'enregistrement. Le nouveau programme n'a pas besoin de décrire le fichier à l'aide des instructions SELECT et FD. Le programme peut simplement contenir les descriptions des enregistrements sous forme de niveaux 01 dans WorkingStorage. **Note** Vous pouvez créer un fichier source pour chaque fichier de données ou créer un fichier source principal qui décrit tous les fichiers de données.	Développeur d'applications

Tâche	Description	Compétences requises
Compilez le fichier source.	Compilez le fichier source pour créer le dictionnaire de données. Nous vous recommandons de compiler le fichier source en utilisant le jeu de caractères EBCDIC. Si la directive IBMCOMP ou les directives ODOSLIDE sont utilisées, vous devez également utiliser ces directives dans le fichier source. **Note** IBMCOMP affecte le stockage en octets des champs COMP et ODOSLIDE affecte le remplissage des structures OCCURRENTS VARIING. Si ces directives ne sont pas définies correctement, l'outil de conversion ne lira pas correctement l'enregistrement de données. Cela entraîne des données incorrectes dans le fichier converti.	Développeur d’applications

(Option A) Créez le fichier de structure à l'aide des outils de fichiers de données classiques

Tâche	Description	Compétences requises
Démarrez l'outil et chargez le dictionnaire.	1. Choisissez l'icône du menu Démarrer de Windows, recherchez et choisisse z Micro Focus Enterprise Developer, puis choisissez Classic Data File Tools. 2. Choisissez Fichier, puis Disposition d'enregis trement. 3. Dans la boîte de dialogue Sélectionnez un fichier à partir duquel créer les mises en page, dans Nom du fichier, sélection nez le fichier IDY (`.idy`) créé lors de la compilati on précédente du fichier source. Choisissez ensuite Ouvrir. 4. Pour vérifier que Classic Data File Tools utilise EBCDIC, dans la boîte de dialogue Outils de fichiers de données, sélection nez YES si le fichier IDY est défini sur EBCDIC et Datatools sur ANSI.	Développeur d’applications
Créez la mise en page d'enregistrement par défaut.	Utilisez le format d'enregis trement par défaut pour tous les enregistrements qui	Développeur d’applications

Tâche	Description	Compétences requises
	ne correspondent à aucun modèle conditionnel. 1. Dans la fenêtre de mise en page, développez la structure de données, puis localisez le niveau 01 utilisé pour la mise en page par défaut. 2. Cliquez avec le bouton droit sur l'élément 01, puis choisissez Nouvelle mise en page. 3. Dans la boîte de dialogue Nouvel assistant de mise en page d'enregistrement, choisissez Disposition par défaut, puis Suivant. 4. Choisissez Finish (Terminer). La mise en page par défaut apparaît dans le volet Dispositions et peut être identifiée par l'icône de dossier rouge.	

Tâche	Description	Compétences requises
Créez une mise en page d'enregistrement condition nelle.	Utilisez le format d'enregis trement conditionnel lorsqu'il existe plusieurs modèles d'enregistrement dans un fichier. 1. Dans le volet Dispositions, développez la structure de données, puis localisez le niveau 01 utilisé pour la mise en page condition nelle. 2. Cliquez avec le bouton droit sur l'élément 01, puis choisissez Nouvelle mise en page. 3. Dans la boîte de dialogue Nouvel assistant de mise en page d'enregistrement, choisissez Mise en page conditionnelle, puis cliquez sur Suivant. 4. Choisissez Finish (Terminer). La mise en page conditionnelle apparaît dans le volet Dispositions et peut être identifiée par l'icône de dossier jaune. 5. Développez la mise en page conditionnelle, cliquez avec le bouton droit sur le champ dans lequel vous devez placer une condition,	Développeur d’applications

Tâche	Description	Compétences requises
	puis sélectionnez Propriété s. 6. Dans la boîte de dialogue Propriétés du champ, entrez la condition. Vérifiez que le jeu de caractères est défini sur EBCDIC, puis cliquez sur OK. Une coche apparaît à côté du champ pour lequel une condition est définie. 7. Répétez les étapes 5 et 6 pour tous les autres champs nécessitant des conditions pour ce modèle. 8. Répétez les étapes 1 à 6 pour toutes les autres mises en page conditionnelles qui doivent être ajoutées. 9. Choisissez Fichier, puis Enregistrer sous, puis enregistrez le fichier de structure sur le disque.	

(Option B) Créez le fichier de structure à l'aide des outils de fichiers de données

Tâche	Description	Compétences requises
Démarrez l'outil et chargez le dictionnaire.	1. Choisissez l'icône du menu Démarrer de Windows, recherchez et choisisse z Micro Focus Enterprise	Développeur d’applications

Tâche	Description	Compétences requises
	Developer, puis choisissez Data File Tools. 2. Choisissez Fichier, Nouveau, Fichier de structure. 3. Dans la boîte de dialogue Ouvrir, dans Nom du fichier, sélectionnez le fichier IDY (`.idy`) créé lors de la compilation précédente du fichier source. Choisissez ensuite Ouvrir. 4. Pour vérifier que Data File Tools utilise EBCDIC, vérifiez que le menu déroulant de la section Fichier de débogage est défini sur EBCDIC.	

Tâche	Description	Compétences requises
Créez la mise en page d'enregistrement par défaut.	Utilisez le format d'enregistrement par défaut pour tous les enregistrements qui ne correspondent à aucun modèle conditionnel. 1. Dans la section Dispositions disponibles du volet gauche, développez la structure de données, puis localisez le niveau 01 utilisé pour la mise en page par défaut. 2. Cliquez avec le bouton droit sur l'élément 01, puis choisissez Créer une mise en page par défaut. La mise en page par défaut apparaît dans le volet Dispositions et peut être identifiée par l'icône bleue « D ».	Développeur d’applications

Tâche	Description	Compétences requises
Créez une mise en page d'enregistrement condition nelle.	Utilisez le format d'enregis trement conditionnel lorsqu'il existe plusieurs modèles d'enregistrement dans un fichier. 1. Dans la section Mises en page sélectionnées du volet droit, développez la structure de données, puis localisez le niveau 01 utilisé pour la mise en page conditionnelle. 2. Cliquez avec le bouton droit sur l'élément 01, puis choisissez Créer une mise en page conditionnelle. La mise en page condition nelle apparaît dans le volet Dispositions sur le côté droit et peut être identifiée par l'icône verte « C ». 3. Développez la mise en page conditionnelle, cliquez avec le bouton droit sur le champ dans lequel vous devez placer une condition, puis sélectionnez Propriété s. 4. Dans la boîte de dialogue Propriétés du champ, entrez la condition. Vérifiez que le jeu de caractères est défini sur EBCDIC, puis	Développeur d’applications

Tâche	Description	Compétences requises
	cliquez sur OK. Une icône rouge « IF » apparaît à côté du champ pour lequel une condition est définie. 5. Répétez les étapes 3 et 4 pour tous les autres champs nécessitant des conditions pour ce modèle. 6. Répétez les étapes 1 à 4 pour toutes les autres mises en page conditionnelles qui doivent être ajoutées. 7. Choisissez Fichier, puis Enregistrer sous, puis enregistrez le fichier de structure sur le disque.	

(Option A) Tester le fichier de structure à l'aide des outils de fichiers de données classiques

Tâche	Description	Compétences requises
Testez un fichier de données EBCDIC.	Vérifiez que vous pouvez utiliser votre fichier de structure pour afficher correctement un fichier de données de test EBCDIC. 1. Choisissez l'icône du menu Démarrer de Windows, recherchez et choisisse z Micro Focus Enterprise Developer, puis choisissez Classic Data Tools.	Développeur d’applications

Tâche	Description	Compétences requises
	2. Choisissez Fichier, puis Ouvrir. 3. Dans la boîte de dialogue Ouvrir, pour Nom du fichier, sélectionnez le jeu de données EBCDIC, puis sélectionnez Ouvrir. 4. Choisissez Fichier, Éditeur de fichiers de données, Charger les mises en page d'enregistrement. 5. Dans la boîte de dialogue Ouvrir, pour Nom du fichier, sélectionnez le fichier de structure, puis choisissez Ouvrir. 6. Pour confirmer que le mode de jeu de caractères est défini sur EBCDIC, vérifiez que le menu déroulant est défini sur EBCDIC. Vous pouvez voir les données d'enregistrement brutes dans le volet de gauche et les données formatées dans le volet de droite. 7. Choisissez différents enregistrements pour vous assurer que tous les formats sont rendus avec la bonne mise en page.	

(Option B) Tester le fichier de structure à l'aide des outils de fichiers de données

Tâche	Description	Compétences requises
Testez un fichier de données EBCDIC.	Vérifiez que vous pouvez utiliser votre fichier de structure pour afficher correctement un fichier de données de test EBCDIC. 1. Choisissez l'icône du menu Démarrer de Windows, recherchez et sélectionnez Micro Focus Enterprise Developer, puis choisissez Data File Tools. 2. Choisissez Fichier, Ouvrir, Fichier de données. 3. Dans la boîte de dialogue Fichier de données ouvert, sous l'onglet Local, pour Nom de fichier, choisissez Parcourir pour trouver l'emplacement du fichier de test EBCDIC. 4. Pour Fichier de structure (facultatif), choisissez Parcourir pour trouver l'emplacement du fichier de structure. 5. Dans la section Détails du fichier, entrez les détails du fichier et vérifiez que le codage est défini sur EBCDIC.	Développeur d’applications

Tâche	Description	Compétences requises
	6. Choisissez le mode Open Shared ou Open Exclusive en fonction de vos besoins. 7. Vérifiez que le menu déroulant de la section Apparence de la barre d'outils est défini sur EBCDIC. Vous verrez les données d'enregistrement brutes dans le volet de gauche et les données formatées dans le volet de droite. 8. Choisissez différents enregistrements pour vous assurer que tous les formats sont rendus avec la bonne mise en page.	

Conversion de fichiers de données de test

Tâche	Description	Compétences requises
Testez la conversion d'un fichier EBCDIC.	1. Choisissez l'icône du menu Démarrer de Windows, recherchez et sélection nez Micro Focus Enterprise Developer, puis choisissez Classic Data Tools. 2. Choisissez Outils, puis sélectionnez Convertir. 3. Dans la boîte de dialogue Conversion de fichiers de	Développeur d’applications

Tâche	Description	Compétences requises
	données, dans la section Fichier d'entrée, pour Nom de fichier, choisisse z Parcourir pour recherche r et sélectionner le fichier d'entrée EBCDIC. Vérifiez que le jeu de caractères est défini sur EBCDIC. 4. Dans la section Conversio n du jeu de caractères, cochez les cases Convertir le jeu de caractères et Les enregistrements contiennent des éléments de données autres que du texte. Choisissez Sélection ner la mise en page pour la conversion, puis choisisse z Parcourir pour rechercher et sélectionner le fichier de structure. 5. Dans la section Nouveau fichier, pour Nom de fichier, entrez le chemin et le nom du fichier de sortie ASCII que vous souhaitez créer. Par défaut, l'outil de conversion utilise le même format que le fichier d'entrée. Pour les tests, laissez les options définies sur leurs valeurs par défaut. 6. Choisissez Convertir.	

Tâche	Description	Compétences requises
	7. Suivez les étapes décrites dans la section (Option A) Tester le fichier de structure à l'aide des outils de fichiers de données classiques ou (Option B) Testez le fichier de structure à l'aide des outils de fichier de données, mais chargez le fichier de sortie ASCII au lieu du fichier EBCDIC. 8. Chargez les fichiers EBCDIC et ASCII dans l'éditeur de fichiers de données, puis comparez les fichiers côte à côte pour vérifier l'exactitude de la conversion.	

Ressources connexes

- Micro Focus (documentation Micro Focus)
- Mainframe et code existant (articles de blog AWS)
- Directives AWS Prescriptive Guidance (documentation AWS)
- Documentation AWS (documentation AWS)
- Référence générale AWS (documentation AWS)
- Glossaire AWS (documentation AWS)

Déployez un environnement pour les applications Blu Age conteneurisées à l'aide de Terraform

Créée par Richard Milner-Watts (AWS)

Récapitulatif

La migration des charges de travail d'un mainframe existant vers des architectures cloud modernes peut éliminer les coûts de maintenance d'un mainframe, coûts qui ne font qu'augmenter à mesure que l'environnement vieillit. Cependant, la migration de tâches depuis un ordinateur central peut poser des défis uniques. Les ressources internes ne sont peut-être pas familiarisées avec la logique du travail, et les hautes performances des ordinateurs centraux pour ces tâches spécialisées peuvent être difficiles à reproduire par rapport à une solution standard généralisée. CPUs La réécriture de ces tâches peut être une entreprise de grande envergure et nécessiter des efforts considérables.

Blu Age convertit les charges de travail du mainframe existant en code Java moderne, que vous pouvez ensuite exécuter en tant que conteneur.

Ce modèle fournit un exemple d'architecture sans serveur pour exécuter une application conteneurisée qui a été modernisée avec l'outil Blu Age. Les fichiers HashiCorp Terraform inclus créeront une architecture sécurisée pour l'orchestration des conteneurs Blu Age, prenant en charge à la fois les tâches par lots et les services en temps réel.

Pour plus d'informations sur la modernisation de vos charges de travail à l'aide de Blu Age et des services AWS, consultez les publications AWS Prescriptive Guidance suivantes :

- Exécution de charges de travail mainframe modernisées avec Blu Age sur une infrastructure sans serveur AWS
- Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age

Pour obtenir de l'aide sur l'utilisation de Blu Age afin de moderniser les charges de travail de votre mainframe, contactez l'équipe Blu Age en sélectionnant Contacter nos experts sur le site Web de Blu Age. Pour obtenir de l'aide concernant la migration de vos charges de travail modernisées vers AWS, leur intégration aux services AWS et leur mise en production, contactez votre responsable de compte AWS ou remplissez le formulaire AWS Professional Services.

Conditions préalables et limitations

Prérequis

- L'exemple d'application Blu Age conteneurisée fourni par le mainframe Containerize charge de travail qui a été modernisé selon le modèle Blu Age. L'exemple d'application fournit la logique permettant de gérer le traitement des entrées et des sorties pour l'application modernisée, et il peut s'intégrer à cette architecture.
- Terraform est requis pour déployer ces ressources.

Limites

- Amazon Elastic Container Service (Amazon ECS) impose des limites aux ressources de tâches qui peuvent être mises à la disposition du conteneur. Ces ressources incluent le processeur, la RAM et le stockage. Par exemple, lorsque vous utilisez Amazon ECS avec AWS Fargate, les limites des ressources des tâches s'appliquent.

Versions du produit

Cette solution a été testée avec les versions suivantes :

- Terraform 1.3.6
- Fournisseur Terraform AWS 4.46.0

Architecture

Pile technologique source

- Âge bleu
- Terraform

Pile technologique cible

- Amazon Aurora PostgreSQL-Compatible Edition
- AWS Backup
- Amazon Elastic Container Registry (Amazon ECR)
- Amazon ECS
- AWS Identity and Access Management Service (IAM)
- Serveur de gestion des clés AWS (AWS KMS)

- AWS Secrets Manager
- Amazon Simple Notification Service (Amazon SNS)
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager

Architecture cible

Le schéma suivant montre l'architecture de la solution.

1. La solution déploie les rôles IAM suivants :
   - Rôle de tâche Batch
   - Rôle d'exécution de tâches Batch
   - Rôle de tâche de service
   - Rôle d'exécution des tâches de service
   - Rôle Step Functions
   - Rôle AWS Backup
   - Rôle de surveillance améliorée RDS.

   Les rôles sont conformes aux principes d'accès les moins privilégiés.
2. Amazon ECR est utilisé pour stocker l'image du conteneur orchestrée par ce modèle.
3. AWS Systems Manager Parameter Store fournit des données de configuration relatives à chaque environnement à la définition de tâche Amazon ECS lors de l'exécution.
4. AWS Secrets Manager fournit des données de configuration sensibles concernant l'environnement à la définition des tâches Amazon ECS lors de l'exécution. Les données ont été chiffrées par AWS KMS.
5. Les modules Terraform créent des définitions de tâches Amazon ECS pour toutes les tâches en temps réel et par lots.
6. Amazon ECS exécute une tâche par lots en utilisant AWS Fargate comme moteur de calcul. Il s'agit d'une tâche de courte durée, initiée conformément aux exigences d'AWS Step Functions.
7. Amazon Aurora PostgreSQL compatible fournit une base de données pour prendre en charge l'application modernisée. Cela remplace les bases de données mainframe telles qu'IBM Db2 ou IBM IMS DB.

8. Amazon ECS gère un service de longue durée pour fournir une charge de travail en temps réel modernisée. Ces applications apatrides s'exécutent en permanence avec des conteneurs répartis dans les zones de disponibilité.
9. Un Network Load Balancer est utilisé pour autoriser l'accès à la charge de travail en temps réel. Le Network Load Balancer prend en charge les protocoles antérieurs, tels qu'IBM CICS. Vous pouvez également utiliser un Application Load Balancer avec des charges de travail basées sur le protocole HTTP.
10. Amazon S3 fournit un stockage d'objets pour les entrées et sorties des tâches. Le conteneur doit gérer les opérations de pull et de push dans Amazon S3 afin de préparer le répertoire de travail de l'application Blu Age.
11. Le service AWS Step Functions est utilisé pour orchestrer l'exécution des tâches Amazon ECS afin de traiter des charges de travail par lots.
12. Les rubriques SNS pour chaque charge de travail par lots sont utilisées pour intégrer l'application modernisée à d'autres systèmes, tels que le courrier électronique, ou pour lancer des actions supplémentaires, telles que la livraison d'objets de sortie depuis Amazon S3 vers FTP.

> **Note**
>
> Par défaut, la solution n'a pas accès à Internet. Ce modèle suppose que le cloud privé virtuel (VPC) sera connecté à d'autres réseaux à l'aide d'un service tel qu'AWS Transit Gateway. Ainsi, plusieurs points de terminaison VPC d'interface sont déployés pour accorder l'accès aux services AWS utilisés par la solution. Pour activer l'accès direct à Internet, vous pouvez utiliser le bouton du module Terraform pour remplacer les points de terminaison VPC par une passerelle Internet et les ressources associées.

Automatisation et évolutivité

L'utilisation de ressources sans serveur tout au long de ce modèle permet de garantir que, grâce à une mise à l'échelle progressive, l'échelle de cette conception est limitée. Cela réduit les problèmes liés au bruit des voisins, tels que la concurrence pour les ressources informatiques qui pourrait être rencontrée sur le mainframe d'origine. Les tâches Batch peuvent être planifiées pour s'exécuter simultanément selon les besoins.

Les conteneurs individuels sont limités par les tailles maximales prises en charge par Fargate. Pour plus d'informations, consultez la section relative au processeur et à la mémoire des tâches dans la documentation Amazon ECS.

Pour dimensionner horizontalement les charges de travail en temps réel, vous pouvez ajouter des conteneurs.

Outils

Services AWS

- Amazon Aurora PostgreSQL Compatible Edition est un moteur de base de données relationnelle entièrement géré et compatible ACID qui vous aide à configurer, exploiter et dimensionner les déploiements PostgreSQL.
- AWS Backup est un service entièrement géré qui vous aide à centraliser et à automatiser la protection des données sur site Services AWS, dans le cloud et sur site.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Step Functions est un service d'orchestration sans serveur qui vous permet de combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.
- AWS Systems Manager Parameter Store fournit un stockage hiérarchique sécurisé pour la gestion des données de configuration et la gestion des secrets.

Autres services

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud. Ce modèle utilise Terraform pour créer l'exemple d'architecture.

Référentiel de code

Le code source de ce modèle est disponible dans le référentiel GitHub Blu Age Sample ECS Infrastructure (Terraform).

Bonnes pratiques

- Pour les environnements de test, utilisez des fonctionnalités telles que la `forceDate` possibilité de configurer l'application modernisée afin de générer des résultats de test cohérents en s'exécutant toujours pendant une période connue.
- Ajustez chaque tâche individuellement pour consommer le maximum de ressources. Vous pouvez utiliser Amazon CloudWatch Container Insights pour obtenir des conseils sur les goulets d'étranglement potentiels.

Épopées

Préparer l'environnement pour le déploiement

Tâche	Description	Compétences requises
Clonez le code source de la solution.	Clonez le code de solution à partir du GitHub projet.	DevOps ingénieur
Démarrez l'environnement en déployant des ressources pour stocker l'état Terraform.	1. Ouvrez une fenêtre de terminal et vérifiez que Terraform est installé et que les AWS informati ons d'identification sont disponibles. 2. Accédez au dossier `bootstrap-terrafor m .`	DevOps ingénieur

Tâche	Description	Compétences requises
	3. Modifiez le fichier `main.tf` si vous souhaitez modifier les noms du compartiment S3 (`<accountId>-terraform-backend`) et de la table Amazon DynamoDB (`terraform-lock`). 4. Exécutez la commande `terraform apply` pour déployer les ressources. Notez les noms du bucket S3 et des tables DynamoDB.	

Déployer l'infrastructure de la solution

Tâche	Description	Compétences requises
Vérifiez et mettez à jour la configuration de Terraform.	Dans le répertoire racine, ouvrez le fichier, `main.tf`, examinez son contenu et pensez à effectuer les mises à jour suivantes : 1. Mettez à jour le Région AWS en recherchant et en remplaçant `eu-west-1` la chaîne par la région que vous souhaitez utiliser. 2. Mettez à jour le nom du bucket dans le bloc `Terraform Backend` si le nom par	DevOps ingénieur

Tâche	Description	Compétences requises
	défaut a été modifié dans l'épopée précédente. 3. Mettez à jour la `dynamodb_table` valeur si la valeur par défaut a été modifiée dans l'épopée précédente. 4. Mettez à jour la valeur de la `stack_prefix` variable avec la chaîne de votre choix. Cette chaîne sera ajoutée aux noms de toutes les ressources créées par ce modèle. 5. Mettez à jour la valeur de `vpc_cidr` This should be at least a `/24` address range. 6. Consultez la `Locals` section. Ceci est utilisé pour définir les tâches Blu Age qui seront déployées . La solution va itérer sur l'objet de la liste`bluage_batch_modules` , en créant les ressources associées (machine d'état Step Functions, définitio n des tâches et rubrique SNS) pour chaque élément de la liste. Dans certains cas, vous souhaiterez peut-être ajuster les variables pour différents environne ments. Par exemple, pour	

Tâche	Description	Compétences requises
	forcer l'exécution dans les environnements de test, vous pouvez modifier la valeur de la `force_execution_time` variable. 7. Pour activer l'accès à Internet, modifiez la valeur `direct_internet_access_required` de `false` à `true`. Cela permettra de déployer une passerelle Internet, ainsi que les passerelles NAT et les tables de routage qui activent l'accès public à Internet pour l'infrastructure. Par défaut, la solution déploiera les points de terminaison VPC d'interface dans un VPC sans accès direct à Internet. 8. Pour accorder l'accès à toutes les charges de travail client-serveur servies via Elastic Load Balancing, mettez à jour les valeurs `additional_nlb_ingress_cidrs` des réseaux CIDR qui devraient être autorisés.	

Tâche	Description	Compétences requises
Déployez le fichier Terraform.	Depuis votre terminal, exécutez la `terraform apply` commande pour déployer toutes les ressource s. Passez en revue les modifications générées par Terraform et entrez oui pour lancer la construction. Notez que le déploiement de cette infrastructure peut prendre plus de 15 minutes.	DevOps ingénieur

(Facultatif) Déployez une application conteneurisée Blu Age valide

Tâche	Description	Compétences requises
Transférez l'image du conteneur Blu Age vers Amazon ECR.	Insérez le conteneur dans le référentiel Amazon ECR que vous avez créé dans l'épopée précédente. Pour obtenir des instructions, consultez la documentation Amazon ECR. Notez l'URI de l'image du conteneur.	DevOps ingénieur
Mettez à jour le Terraform pour faire référence à l'image du conteneur Blu Age.	Mettez à jour le fichier `main.tf` pour faire référence à l'image du conteneur que vous avez chargée.	DevOps ingénieur
Redéployez le fichier Terraform.	Depuis votre terminal, exécutez `terraform apply` pour déployer toutes les	DevOps ingénieur

Tâche	Description	Compétences requises
	ressources. Passez en revue les mises à jour suggérées par Terraform, puis entrez oui pour poursuivre le déploiement.	

Ressources connexes

- Âge bleu
- Exécution de charges de travail mainframe modernisées avec Blu Age sur une infrastructure sans serveur AWS
- Conteneurisez les charges de travail du mainframe qui ont été modernisées par Blu Age

Générez des informations sur les données Db2 z/OS à l'aide d' AWS Mainframe Modernization Amazon Q dans QuickSight

Créée par Shubham Roy (AWS), Roshna Razack (AWS) et Santosh Kumar Singh (AWS)

Récapitulatif

Si votre entreprise héberge des données critiques dans un environnement mainframe IBM Db2, il est essentiel d'obtenir des informations à partir de ces données pour stimuler la croissance et l'innovation. En débloquant les données du mainframe, vous pouvez créer des informations commerciales plus rapides, sécurisées et évolutives afin d'accélérer la prise de décision, la croissance et l'innovation basées sur les données dans le cloud Amazon Web Services ()AWS.

Ce modèle présente une solution pour générer des informations commerciales et créer des récits partageables à partir des données du mainframe dans les tables IBM Db2 for z/OS. Les modifications des données du mainframe sont transmises à la AWS Mainframe Modernization rubrique Amazon Managed Streaming for Apache Kafka (Amazon MSK) à l'aide de la réplication de données avec Precisely. Grâce à l'ingestion en streaming d'Amazon Redshift, les données thématiques Amazon MSK sont stockées dans des tables d'entrepôt de données Amazon Redshift Serverless à des fins d'analyse sur Amazon. QuickSight

Une fois les données disponibles dans QuickSight, vous pouvez utiliser des instructions en langage naturel avec Amazon Q QuickSight pour créer des résumés des données, poser des questions et générer des récits de données. Vous n'avez pas besoin d'écrire de requêtes SQL ou de vous familiariser avec un outil de business intelligence (BI).

Contexte commercial

Ce modèle présente une solution pour les cas d'utilisation de l'analyse des données sur le mainframe et de l'analyse des données. À l'aide de ce modèle, vous créez un tableau de bord visuel pour les données de votre entreprise. Pour démontrer la solution, ce modèle fait appel à une entreprise de soins de santé qui fournit des plans médicaux, dentaires et ophtalmologiques à ses membres aux États-Unis. Dans cet exemple, les données démographiques des membres et les informations relatives au plan sont stockées dans les tables de données IBM Db2 for z/OS. Le tableau de bord visuel présente les éléments suivants :

- Répartition des membres par région
- Répartition des membres par sexe

- Répartition des membres par âge
- Répartition des membres par type de plan
- Membres qui n'ont pas terminé leur vaccination préventive

Pour des exemples de répartition des membres par région et de membres n'ayant pas terminé la vaccination préventive, consultez la section Informations supplémentaires.

Après avoir créé le tableau de bord, vous générez un récit de données qui explique les informations issues de l'analyse précédente. L'histoire des données fournit des recommandations pour augmenter le nombre de membres ayant effectué des vaccinations préventives.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS. Cette solution a été développée et testée sur Amazon Linux 2 sur Amazon Elastic Compute Cloud (Amazon EC2).
- Un cloud privé virtuel (VPC) doté d'un sous-réseau accessible par votre système mainframe.
- Une base de données mainframe contenant des données commerciales. Pour les exemples de données utilisés pour créer et tester cette solution, consultez la section Pièces jointes.
- La capture des données de modification (CDC) est activée sur les tables Db2 z/OS. Pour activer le CDC sur Db2 z/OS, consultez la documentation IBM.
- Precisely Connect CDC for z/OS installé sur le système z/OS hébergeant les bases de données sources. L'image Precisely Connect CDC for z/OS est fournie sous forme de fichier zip dans le fichier AWS Mainframe Modernization - Data Replication for IBM z/OS Amazon Machine Image (AMI). Pour installer Precisely Connect CDC pour z/OS sur le mainframe, consultez la documentation d'installation de Precisely.

Limites

- Les données Db2 de votre mainframe doivent être dans un type de données pris en charge par Precisely Connect CDC. Pour obtenir la liste des types de données pris en charge, consultez la documentation Precisely Connect CDC.
- Vos données chez Amazon MSK doivent être dans un type de données pris en charge par Amazon Redshift. Pour obtenir la liste des types de données pris en charge, consultez la documentation Amazon Redshift.

- Amazon Redshift a des comportements et des limites de taille différents selon les types de données. Pour plus d'informations, consultez la documentation Amazon Redshift.
- Les données entrantes en temps quasi réel QuickSight dépendent de l'intervalle d'actualisation défini pour la base de données Amazon Redshift.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Amazon Q in n' QuickSight est actuellement pas disponible dans toutes les régions compatibles QuickSight. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Versions du produit

- AWS Mainframe Modernization Réplication des données avec Precisely version 4.1.44
- Python version 3.6 ou ultérieure
- Apache Kafka version 3.5.1

Architecture

Architecture cible

Le schéma suivant montre une architecture permettant de générer des informations commerciales à partir des données du mainframe en utilisant la réplication de AWS Mainframe Modernization données avec Precisely et Amazon Q dans QuickSight.

Le schéma suivant illustre le flux de travail suivant :

1. L'agent Precisely Log Reader lit les données des journaux DB2 et les écrit dans un stockage transitoire sur un système de fichiers OMVS sur le mainframe.
2. L'agent Publisher lit les journaux Db2 bruts depuis le stockage transitoire.
3. Le démon du contrôleur local authentifie, autorise, surveille et gère les opérations.
4. L'agent Apply est déployé sur Amazon à EC2 l'aide de l'AMI préconfigurée. Il se connecte à l'agent Publisher via le démon du contrôleur à l'aide du protocole TCP/IP. L'agent Apply envoie les données vers Amazon MSK en faisant appel à plusieurs opérateurs pour un débit élevé.

5. Les travailleurs écrivent les données dans la rubrique Amazon MSK au format JSON. En tant que cible intermédiaire pour les messages répliqués, Amazon MSK fournit des fonctionnalités de basculement automatisées et hautement disponibles.
6. L'ingestion de streaming Amazon Redshift permet une ingestion de données à faible latence et à haut débit depuis Amazon MSK vers une base de données Amazon Redshift Serverless. Une procédure stockée dans Amazon Redshift effectue la réconciliation des données de modification du mainframe (insert/update/deletes) dans les tables Amazon Redshift. Ces tables Amazon Redshift servent de source d'analyse de données pour. QuickSight
7. Les utilisateurs accèdent aux données à des QuickSight fins d'analyse et d'analyse. Vous pouvez utiliser Amazon Q QuickSight pour interagir avec les données à l'aide d'instructions en langage naturel.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les étendre ou les intégrer rapidement.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- Amazon Managed Streaming for Apache Kafka (Amazon MSK) est un service entièrement géré qui vous permet de créer et d'exécuter des applications utilisant Apache Kafka pour traiter les données de streaming.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique. Ce modèle utilise les fonctionnalités de BI générative d'Amazon Q dans QuickSight.
- Amazon Redshift Serverless est une option sans serveur d'Amazon Redshift qui permet d'exécuter et de faire évoluer les analyses de manière plus efficace en quelques secondes, sans qu'il soit nécessaire de configurer et de gérer une infrastructure d'entrepôt de données.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.

Autres outils

- Precisely Connect CDC collecte et intègre les données des systèmes existants dans le cloud et les plateformes de données.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Mainframe_ DataInsights _change_data_reconciliation. Le code est une procédure stockée dans Amazon Redshift. Cette procédure stockée concilie les modifications des données du mainframe (insertions, mises à jour et suppressions) depuis Amazon MSK avec les tables Amazon Redshift. Ces tables Amazon Redshift servent de source d'analyse de données pour. QuickSight

Bonnes pratiques

- Suivez les meilleures pratiques lors de la configuration de votre cluster Amazon MSK.
- Suivez les meilleures pratiques d'analyse des données Amazon Redshift pour améliorer les performances.
- Lorsque vous créez les rôles AWS Identity and Access Management (IAM) pour la configuration de Precisely, suivez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.

Épopées

Configurez la réplication AWS Mainframe Modernization des données avec Precisely sur Amazon EC2

Tâche	Description	Compétences requises
Configurez un groupe de sécurité.	Pour vous connecter au démon du contrôleur et au cluster Amazon MSK, créez un groupe de sécurité pour l' EC2 instance. Ajoutez les règles d'entrée et de sortie suivantes :	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises

	• Règle 1 pour les appels entrants :
	  • Pour Type, choisissez TCP personnalisé.
	  • Pour Protocol (Protocole), choisissez TCP.
	  • Pour Plage de ports, choisissez 2626 (port par défaut pour le démon du contrôleur Precisely) ou le numéro de port du démon du contrôleur exécuté sur le mainframe.
	  • Pour Source, choisissez le bloc CIDR.
	• Règle 2 pour les appels entrants :
	  • Pour Type, choisisse z Custom TCP (TCP personnalisé).
	  • Pour Protocole, choisisse z SSH.
	  • Pour la plage de ports, choisissez 22.
	  • Pour Source, choisisse z une adresse IP ou une liste de préfixes.
	• Règle entrante 3 :
	  • Pour Type, choisisse z Custom TCP (TCP personnalisé).	

Tâche	Description	Compétences requises
	• Pour Protocol (Protocole), choisissez TCP. • Pour la plage de ports, choisissez 9092-9098. • Pour Source, choisissez le bloc CIDR. • Règle 1 pour le trafic sortant : • Pour Type, choisisse z Custom TCP (TCP personnalisé). • Pour Protocol (Protocole), choisissez TCP. • Pour la plage de ports, choisissez 9092-9098. • Pour Source, choisissez le bloc CIDR. • Règle 2 pour le trafic sortant : • Pour Type, choisisse z Custom TCP (TCP personnalisé). • Pour Protocol (Protocole), choisissez TCP. • Pour Plage de ports, choisissez 2626 (port par défaut pour le démon du contrôleur Precisely) ou le numéro de port du démon du contrôleur exécuté sur le mainframe.	

Tâche	Description	Compétences requises
	• Pour Source, choisissez le bloc CIDR. Notez le nom du groupe de sécurité. Vous devrez faire référence au nom lorsque vous lancerez l' EC2 instance et que vous configurerez le cluster Amazon MSK.	
Créez une politique IAM et un rôle IAM.	1. Pour créer une politique IAM et un rôle IAM, suivez les instructions de la documentation AWS. La politique IAM autorise l'accès à la création de rubriques sur le cluster Amazon MSK et à l'envoi de données vers ces rubriques. 2. Après avoir créé le rôle IAM, associez-lui la politique. Notez le nom du rôle IAM. Ce rôle sera utilisé comme profil d'instance IAM lorsque vous lancerez l' EC2 instance.	DevOps ingénieur, administrateur système AWS

Tâche	Description	Compétences requises
Provisionnez une EC2 instance.	Pour configurer une EC2 instance afin d'exécuter Precisely CDC et de vous connecter à Amazon MSK, procédez comme suit : 1. Connectez-vous à AWS Marketplace et abonnez-vous à AWS Mainframe Modernization – Réplication de données pour IBM z/OS. 2. Sélectionnez l'AMI parmi les abonnements gérés, puis choisissez Lancer une nouvelle instance. 3. Fournissez d'autres détails de configuration, tels que le nom de l'instance, le type d'instance, la paire de clés, le VPC et les sous-rése aux. Pour plus d'informa tions, consultez la EC2 documentation Amazon. 4. Dans la liste déroulante, choisissez le groupe de sécurité que vous avez créé précédemment. 5. Sous Détails avancés, profil d'instance IAM, vous devez sélectionner le rôle que vous avez créé précédemm ent.	Administrateur AWS, DevOps ingénieur

Tâche	Description	Compétences requises
	6. Choisissez Launch instance (Lancer une instance).	

Configurer Amazon MSK

Tâche	Description	Compétences requises
Créez le cluster Amazon MSK.	Pour créer un cluster Amazon MSK, procédez comme suit : 1. Connectez-vous à la AWS Management Console console Amazon MSK et ouvrez-la à https://console.aws.amazon.com/msk/l'adresse. 2. Choisissez Créer un cluster. 3. Pour la méthode de création du cluster, choisissez Création personnalisée, et pour le type de cluster, choisissez Provisioned. 4. Attribuez un nom au cluster. 5. Mettez à jour les paramètres du cluster selon vos besoins et conservez les valeurs par défaut pour les autres paramètres. 6. Notez la version < Kafka>. Vous en aurez besoin lors de la configuration du client Kafka.	AWS DevOps, administrateur du cloud

Tâche	Description	Compétences requises
	7. Choisissez Suivant. 8. Choisissez le même VPC et les mêmes sous-réseaux que ceux que vous avez utilisés pour l' EC2 instance Precisely, puis choisissez le groupe de sécurité que vous avez créé précédemment. 9. Dans la section Paramètres de sécurité, activez l'authentification basée sur les rôles SASL/SCRAM et IAM. Precisely Connect CDC utilise le protocole SASL/SCRAM (Simple Authentication and Security Layer/Salted Challenge Response Mechanism), et IAM est nécessaire pour se connecter à Amazon Redshift. 10. Choisissez Suivant. 11. Pour la révision, choisissez la méthode de livraison des journaux de surveillance et de courtage. 12. Choisissez Next, puis Create the cluster. La création d'un cluster provisionné typique prend jusqu'à 15 minutes. Une fois le	

Tâche	Description	Compétences requises
	cluster créé, son statut passe de Création à Actif.	

Tâche	Description	Compétences requises
Configurez l'authentification SASL/SCRAM.	Pour configurer l'authentification SASL/SCRAM pour un cluster Amazon MSK, procédez comme suit : 1. Pour configurer un secret dans Secrets Manager, suivez les instructions de la AWS documentation. 2. Ouvrez la console Amazon MSK et sélectionnez le cluster Amazon MSK que vous avez créé précédemment. 3. Choisissez l'onglet Propriétés. 4. Choisissez Associer des secrets, choisissez les secrets, sélectionnez la clé secrète que vous avez créée, puis choisissez Associer des secrets. Vous verrez un message de confirmation semblable au suivant : `Successfully associated 1 secret for cluster <chosen cluster name>` 5. Choisissez le nom du cluster.	Architecte du cloud

Tâche	Description	Compétences requises
	6. Dans le résumé du cluster, choisissez Afficher les informations sur le client. 7. Notez la chaîne de connexion du point de terminaison privé pour le type d'authentification SASL/SCRAM.	

Tâche	Description	Compétences requises

Créez la rubrique Amazon MSK.	Pour créer la rubrique Amazon MSK, procédez comme suit :
	
	1. Connectez-vous à l' EC2 instance que vous avez créée précédemment et installez les dernières mises à jour en exécutant la commande suivante :
	
	`sudo yum update -y`
	
	2. Installez les bibliothèques Java et Kafka en exécutant la commande suivante :
	
	`sudo yum install -y java-11 librdkafka librdkafka-devel`
	
	3. Pour créer un dossier nommé `kafka` dans `/home/ec2-user` , naviguez jusqu'à ce dossier et exécutez la commande suivante :
	
	`mkdir kafka;cd kafka`
	
	4. Téléchargez la bibliothèque `kafka` cliente `kafka` dans le dossier, en la `<YOUR MSK VERSION>` remplaçant par la version de Kafka que vous avez notée lors de la création du cluster Amazon MSK :
		Administrateur du cloud

Tâche	Description	Compétences requises

	`wget https://archive.apache.org/dist/kafka//kafka_2.13-<YOUR MSK VERSION>.tgz`
	5. Pour extraire le fichier téléchargé, exécutez la commande suivante en remplaçant `YOUR MSK VERSION>` :
	`tar -xzf kafka_2.13-<YOUR MSK VERSION>.tgz`
	6. Pour accéder au `kafka libs` répertoire et télécharger le fichier Java Archive (JAR) d'authentification Java IAM, exécutez les commandes suivantes en remplaçant `<YOUR MSK VERSION>` :
	`cd kafka_2.13-<YOUR MSK VERSION>/libs`
	`wget https://github.com/aws/aws-msk-iam-auth/releases/download/v1.1.1/aws-msk-iam-auth-1.1.1-all.jarkafka`
	7. Pour accéder au `bin` répertoire Kafka et créer le `client.properties`	

Tâche	Description	Compétences requises

	fichier, exécutez les commandes suivantes :
	
	`cd /home/ec2-user/kafka/kafka_2.13-<YOUR MSK VERSION>/bin`
	`cat >client.properties`
	
	8. Mettez à jour le `client.properties` fichier avec le contenu suivant :
	
	`security.protocol=SASL_SSL`
	`sasl.mechanism=AWS_MSK_IAM`
	`sasl.jaas.config=software.amazon.msk.auth.iam.IAMLoginModule required;`
	`sasl.client.callback.handler.class=software.amazon.msk.auth.iam.IAMClientCallbackHandler`
	
	9. Pour créer un sujet Kafka, accédez à la corbeille Kafka et exécutez la commande suivante, en remplaçant par `<kafka broker>` le point de terminaison privé du serveur IAM bootstrap que vous avez noté lors de la création du cluster Amazon MSK :	

Tâche	Description	Compétences requises
	`./kafka-topics.sh --bootstrap-server <kafka broker> --command-config client.properties --create --replication-factor 3 –partitions 6 --topic <topic name>` 10. Lorsque le message `Created topic <topic name>` apparaît, notez le nom du sujet.	

Configurer le moteur Precisely Apply sur Amazon EC2

Tâche	Description	Compétences requises
Configurez les scripts Precisely pour répliquer les modifications apportées aux données.	Pour configurer les scripts Precisely Connect CDC afin de répliquer les données modifiées depuis le mainframe vers la rubrique Amazon MSK, procédez comme suit : 1. Pour créer un nom de dossier précis et le remplacer par ce dossier, exécutez la commande suivante : `mkdir /home/ec2-user/precisely;cd /home/ec2-user/precisely`	Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises

	2. Pour créer deux dossiers à l'intérieur du dossier appelé avec précision`ddls`, `scripts` puis passer au `scripts` dossier, exécutez la commande suivante :
	`mkdir scripts;mkdir ddls;cd scripts`
	3. Pour créer un fichier nommé `sqdata_kafka_producer.conf` dans le `scripts` dossier, exécutez la commande suivante :
	`cat >sqdata_kafka_producer.conf`
	4. Mettre à jour le `sqdata_kafka_producer.conf` fichier avec le contenu suivant :
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=<User Name>`
	`sasl.password=<Password>`
	`metadata.broker.list=<SASL/SCRAM Bootstrap servers>`	

Tâche	Description	Compétences requises
	Note Effectuez la mise à jour `<SASL/SCRAM Bootstrap servers>` avec la liste des courtiers Amazon MSK SASL/SCRAM que vous avez précédemment configurée. Mettez à jour `<User Name>` et `<Password>` utilisez le nom d'utilisateur et le mot de passe que vous avez définis précédemment dans Secrets Manager. 5. Créez un `script.sqd` fichier dans le `scripts` dossier. `cat >script.sqd` Le moteur Apply permet `script.sqd` de traiter les données sources et de les répliquer vers la cible. Pour un exemple de script Apply	

Tâche	Description	Compétences requises

	Engine, consultez la section Informations supplémentaires.
	6. Pour accéder au `ddls` dossier et créer un fichier .ddl pour chaque table DB2, exécutez les commandes suivantes :
	`cd /home/ec2-user/precisely/ddls`
	`cat >mem_details.ddl`
	`cat >mem_plans.ddl`
	Par exemple, les fichiers .ddl, consultez la section Informations supplémentaires.	

Tâche	Description	Compétences requises

Générez la clé ACL du réseau.	Pour générer la clé de liste de contrôle d'accès réseau (ACL réseau), procédez comme suit :
	
	1. Pour exporter le chemin `sqdata` d'installation, exécutez la commande suivante :
	
	`export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
	
	2. Pour accéder au `/home/ec2-user` répertoire et générer la clé ACL réseau, exécutez les commandes suivantes :
	
	`cd /home/ec2-user`
	`sqdutil keygen --force`
	
	Une fois les clés publiques et privées générées, le message suivant s'affiche :
	
	`SQDUT04I Generating a private key in file /home/ec2-user/.nacl/id_nacl`
	`SQDC017I sqdutil(pid=27344) terminated successfully`
		Architecte du cloud, AWS DevOps

Tâche	Description	Compétences requises
	3. Notez la clé publique générée qui est stockée dans le `.nacl` dossier.	

Préparation de l'environnement source du mainframe

Tâche	Description	Compétences requises
Configurez les valeurs par défaut dans l'écran ISPF.	Pour configurer les paramètres par défaut dans l'Interactive System Productivity Facility (ISPF), suivez les instructions de la documentation Precisely.	Administrateur système mainframe
Configurez le démon du contrôleur.	Pour configurer le démon du contrôleur, procédez comme suit : 1. Sur l'écran du menu principal de SQData z/OS, choisissez l'option 2. 2. Sur l'écran Ajouter un démon à la liste, dans le champ Nom du démon, entrez le nom du démon, puis appuyez sur Entrée.	Administrateur système mainframe
Configurez l'éditeur.	Pour configurer l'éditeur, procédez comme suit : 1. Sur l'écran du menu principal de SQData z/OS, choisissez l'option 3. Cela vous amène à l'écran	Administrateur système mainframe

Tâche	Description	Compétences requises
	Résumé de Capture/P ublisher. 2. Choisissez l'option permettant d'ajouter un fichier CAB. Cela vous amènera à l'écran Ajouter un fichier CAB à la liste. 3. Dans le champ Nom, entrez le nom du fichier CAB. Pour Db2, entrez le type commeD. 4. Appuyez sur Entrée. Cela vous amène à l'écran Créer un nouveau fichier CAB de capture DB2. 5. Dans le champ ZfS Dir, spécifiez le point de montage du stockage. 6. Appuyez sur Entrée pour enregistrer et continuer.	

Tâche	Description	Compétences requises
Mettez à jour le fichier de configuration du démon.	Pour mettre à jour les informations relatives à l'éditeur dans le fichier de configuration du démon du contrôleur, procédez comme suit : 1. Sur l'écran du menu principal de SQData z/OS, choisissez l'option 2. 2. Entrez S à côté du daemon que vous avez créé pour voir les détails du daemon. 3. Entrez1, puis appuyez sur Entrée pour modifier le fichier des agents. 4. Ajoutez les détails de votre fichier CAB. L'exemple suivant montre les détails d'un fichier CAB nomméDB2ZT0MSK . Utilisez l'ID utilisateur de votre ordinateur central au lieu de. `<userid>` `ÝDB2ZT0MSK¨ type=capture cab=/u/<userid>/sqdata/DB2ZT0MSK.cab` 5. Appuyez sur F3. 6. Entrez 2 pour modifier le fichier ACL. Ajoutez votre `userid` au fichier `acl` de configuration comme	Administrateur système mainframe

Tâche	Description	Compétences requises
	indiqué dans l'exemple suivant : `Ýacls¨ prod=admin,<userid>` 7. Appuyez sur F3 pour enregistrer et quitter.	
Créez la tâche pour démarrer le démon du contrôleur.	Pour créer la tâche, procédez comme suit : 1. Dans Options, entrez`G`. 2. Entrez la fiche JOB, les bibliothèques de tâches et de processus, ainsi que les détails de `Db2 load` la bibliothèque. 3. Entrez les détails du fichier ACL réseau et entrez l'option 2 pour générer le fichier de langage de contrôle des tâches (JCL) dans la bibliothèque de tâches spécifiée.	Administrateur système mainframe

Tâche	Description	Compétences requises
Générez le fichier JCL de l'éditeur de capture.	Pour générer le fichier JCL de l'éditeur de capture, procédez comme suit : 1. Sur l'écran du menu principal de SQData z/OS, choisissez l'option 3. Cela vous amène à l'écran Résumé de Capture/Publisher. 2. Entrez à `S` côté du fichier CAB pour le sélectionner. Cela vous amène à l'écran Db2 Capture/Publisher Detail. 3. Dans Options, entrez `G` les options pour générer la `capture/publisher` tâche. 4. Entrez les bibliothèques de cartes JOB, de tâches et de procédures, ainsi que les détails de la bibliothèque de chargement DB2. 5. Pour créer la tâche, choisissez l'option 4. La tâche est créée dans la bibliothèque de tâches spécifiée dans la bibliothèque de tâches.	Administrateur système mainframe

Tâche	Description	Compétences requises

Vérifiez et mettez à jour le CDC.	1. Vérifiez l'DATACAPTURE indicateur de la table DB2 en exécutant la requête suivante, en remplaçant le nom <table name> de votre table DB2 :
	`SELECT DATACAPTURE FROM SYSIBM.SYSTABLES WHERE NAME='<table name>';`
	Vérifiez que le résultat s'affiche DATACAPTURE sous la formeY.
	2. Si DATACAPTURE ce n'est pas le casY, exécutez la requête suivante pour activer le CDC sur la table DB2, en changeant le <table name> nom de votre table DB2 :
	`ALTER TABLE <table name> DATA CAPTURE CHANGES;`
		Administrateur système mainframe

Tâche	Description	Compétences requises
Soumettez les fichiers JCL.	Soumettez les fichiers JCL suivants que vous avez configurés lors des étapes précédentes : • Fichier JCL pour démarrer le démon du contrôleur • Fichier JCL pour démarrer la capture et la publication Après avoir soumis les fichiers JCL, vous pouvez démarrer le moteur d'application dans Precisely sur l' EC2 instance.	Administrateur système mainframe

Exécutez et validez le CDC

Tâche	Description	Compétences requises
Démarrez le moteur d'application et validez le CDC.	Pour démarrer le moteur d'application sur l' EC2 instance et valider le CDC, procédez comme suit : 1. Pour vous connecter à l' EC2 instance, suivez les instructions de la AWS documentation. 2. Accédez au répertoire qui contient le `script.sqd` fichier : `cd /home/ec2-user/precisely/scripts`	Architecte cloud, développeur d'applications

Tâche	Description	Compétences requises
	3. Pour démarrer le moteur d'application, exécutez la commande de `sqdeng` démarrage suivante : `sqdeng -s script.sqd --identity=/home/ec2-user/.nacl/id_nacl` Le moteur Apply commencera à attendre les mises à jour provenant de la source du mainframe. 4. Pour tester le CDC, insérez ou mettez à jour des enregistrements dans la table DB2. 5. Vérifiez que le journal Apply Engine indique le nombre d'enregistrements capturés et écrits sur la cible.	

Tâche	Description	Compétences requises

Validez les enregistrements relatifs à la rubrique Amazon MSK.	Pour lire le message du sujet Kafka, procédez comme suit :
	1. Pour accéder au `bin` répertoire du chemin d'installation du client Kafka sur l' EC2 instance, exécutez la commande suivante en `<Kafka version>` remplaçant par votre version :
	`cd /home/ec2-user/kafka/kafka_2.13-<Kafka version>/bin`
	2. Pour valider le Db2 CDC écrit sous forme de messages dans le sujet Kafka, exécutez la commande suivante, en `<Topic Name>` remplaçant `<kafka broker>` et par le sujet que vous avez créé précédemment :
	`./kafka-console-consumer.sh --bootstrap-server <kafka broker>:9098 --topic <Topic Name> --from-beginning --consumer.config client.properties`
	3. Vérifiez que les messages correspondent au nombre
		Développeur d'applications, architecte cloud

Tâche	Description	Compétences requises
	d'enregistrements mis à jour dans la table Db2.	

Stockez les données de modification du mainframe dans un entrepôt de données Amazon Redshift Serverless

Tâche	Description	Compétences requises
Configurez Amazon Redshift Serverless.	Pour créer un entrepôt de données Amazon Redshift Serverless, suivez les instructions de la documentation.AWS Sur le tableau de bord Amazon Redshift Serverless, vérifiez que l'espace de noms et le groupe de travail ont été créés et sont disponibles. Pour cet exemple de modèle, le processus peut prendre de 2 à 5 minutes.	Ingénieur de données
Configurez le rôle IAM et la politique de confiance requis pour l'ingestion du streaming.	Pour configurer l'ingestion du streaming sans serveur Amazon Redshift à partir d'Amazon MSK, procédez comme suit : 1. Créez une politique IAM pour Amazon Redshift afin d'accéder à Amazon MSK. En `[region]` remplaçant par le Région AWS pour Amazon MSK, `[account-id]` par votre	Ingénieur de données

Tâche	Description	Compétences requises
	Compte AWS identifiant et [msk-cluster-name] par le nom du cluster Amazon MSK, exécutez le code suivant : `{"Version": "2012-10-17","Statement": [{"Sid": "MSKIAMpolicy","Effect": "Allow","Action": ["kafka-cluster:ReadData","kafka-cluster:DescribeTopic","kafka-cluster:Connect"],"Resource": ["arn:aws:kafka:[region]:[account-id]:cluster/[msk-cluster-name]/*","arn:aws:kafka:[region]:[account-id]:topic/[msk-cluster-name]/*"]},{"Effect": "Allow","Action": ["kafka-cluster:AlterGroup","kafka-cluster:DescribeGroup"],"Resource": ["arn:aws:kafka:[region]:[account-id]:group/[msk-cluster-name]/*"]}]}`	

Tâche	Description	Compétences requises
	Vous pouvez trouver le nom du cluster et le nom de ressource Amazon (ARN) sur la console Amazon MSK. Sur la console, choisissez Résumé du cluster, puis ARN. 2. Pour créer un rôle IAM et associer la politique, suivez les instructions de la AWS documentation. 3. Pour associer le rôle IAM à l'espace de noms Amazon Redshift Serverless, procédez comme suit : a. Connectez-vous à la console, puis ouvrez la console Amazon Redshift à l'adresse . https://console.aws.amazon.com/redshiftv2/ b. Choisissez Serverless dashboard (Tableau de bord sans serveur). c. Choisissez Namespace. d. Choisissez l'onglet Sécurité et chiffrement. e. Choisissez Autorisation, puis attachez le rôle IAM que vous avez créé.	

Tâche	Description	Compétences requises
	4. Dans votre groupe de sécurité Amazon Redshift Serverless, créez une règle entrante avec les informations suivantes : • Pour Type, choisissez Custom TCP (TCP personnalisé). • Pour Protocol (Protocole), choisissez TCP. • Pour la plage de ports, choisissez 9098, 9198. • Pour Source, choisissez le groupe de sécurité Amazon MSK. 5. Dans votre groupe de sécurité Amazon MSK, créez une règle entrante avec les détails suivants : • Pour Type, choisissez Custom TCP (TCP personnalisé). • Pour Protocol (Protocole), choisissez TCP. • Pour la plage de ports, choisissez 9098, 9198. • Pour Source, choisissez le groupe de sécurité Amazon Redshift. Ce modèle utilise le port pour l'authentification IAM pour les configura	

Tâche	Description	Compétences requises
	tions Amazon Redshift et Amazon MSK. Pour plus d'informations, consultez la AWS documentation (étape 2). 6. Activez le routage VPC amélioré pour le groupe de travail Amazon Redshift Serverless. Pour plus d'informations, consultez la documentation AWS.	
Connectez Amazon Redshift Serverless à Amazon MSK.	Pour vous connecter à la rubrique Amazon MSK, créez un schéma externe dans Amazon Redshift Serverles s. Dans l'éditeur de requêtes Amazon Redshift v2, exécutez la commande SQL suivante, en la `'iam_role_arn'` remplaçant par le rôle que vous avez créé précédemment et en remplaçant `'MSK_clus ter_arn` « par l'ARN de votre cluster ». `CREATE EXTERNAL SCHEMA member_schema FROM MSK IAM_ROLE 'iam_role _arn' AUTHENTICATION iam URI 'MSK_cluster_arn';`	Ingénieur en migration

Tâche	Description	Compétences requises
Créez une vue matérialisée.	Pour utiliser les données de la rubrique Amazon MSK dans Amazon Redshift Serverless, créez une vue matérialisée. Dans l'éditeur de requêtes Amazon Redshift v2, exécutez les commandes SQL suivantes, en les `<MSK_Topic_name>` remplaçant par le nom de votre rubrique Amazon MSK. `CREATE MATERIALIZED VIEW member_view AUTO REFRESH YES AS SELECT kafka_partition, kafka_offset, refresh_time, json_parse(kafka_value) AS Data FROM member_schema.<MSK_Topic_name> WHERE CAN_JSON_PARSE(kafka_value);`	Ingénieur en migration

Tâche	Description	Compétences requises

Créez des tables cibles dans Amazon Redshift.	Les tables Amazon Redshift fournissent les entrées pour. QuickSight Ce modèle utilise les tables `member_dtls` et`member_plans` , qui correspondent aux tables Db2 source sur le mainframe.
	
	Pour créer les deux tables dans Amazon Redshift, exécutez les commandes SQL suivantes dans l'éditeur de requêtes Amazon Redshift v2 :
	
	`-- Table 1: members_dtls`
	`CREATE TABLE members_dtls (`
	`memberid INT ENCODE AZ64,`
	`member_name VARCHAR(100) ENCODE ZSTD,`
	`member_type VARCHAR(50) ENCODE ZSTD,`
	`age INT ENCODE AZ64,`
	`gender CHAR(1) ENCODE BYTEDICT,`
	`email VARCHAR(100) ENCODE ZSTD,`
	`region VARCHAR(50) ENCODE ZSTD`
	`) DISTSTYLE AUTO;`
	
	`-- Table 2: member_plans`
	`CREATE TABLE member_plans (`
	`memberid INT ENCODE AZ64,`
		Ingénieur en migration

Tâche	Description	Compétences requises

	<pre>medical_plan CHAR(1)
	ENCODE BYTEDICT,
	dental_plan CHAR(1)
	ENCODE BYTEDICT,
	vision_plan CHAR(1)
	ENCODE BYTEDICT,
	preventive_immuniz
	ation VARCHAR(50)
	ENCODE ZSTD
	) DISTSTYLE AUTO;</pre>	

Créez une procédure stockée dans Amazon Redshift.	Ce modèle utilise une procédure stockée pour synchroniser les données de modification (`INSERT`,`UPDATE`,`DELETE`) du mainframe source vers la table d'entrepôt de données Amazon Redshift cible à des fins d'analyse. QuickSight Pour créer la procédure stockée dans Amazon Redshift, utilisez l'éditeur de requêtes v2 pour exécuter le code de procédure stockée qui se trouve dans le GitHub référentiel.	Ingénieur en migration

Tâche	Description	Compétences requises
Lisez à partir de la vue matérialisée en streaming et chargez vers les tables cibles.	La procédure stockée lit les modifications de données depuis la vue matérialisée en continu et charge les modifications de données dans les tables cibles. Pour exécuter la procédure stockée, utilisez la commande suivante : `call SP_Members_Load();` Vous pouvez utiliser Amazon EventBridge pour planifier les tâches dans votre entrepôt de données Amazon Redshift afin d'appeler cette procédure stockée en fonction de vos exigences en matière de latence des données. EventBridge exécute des tâches à intervalles réguliers . Pour vérifier si l'appel précédent à la procédure est terminé, vous devrez peut-être utiliser un mécanisme tel qu'une machine à AWS Step Functionsétats. Pour plus d'informations, consultez les ressources suivantes : • Création d'une EventBridge règle Amazon exécutée selon un calendrier	Ingénieur en migration

Tâche	Description	Compétences requises
	• Accélérez l'orchestration d'un processus ELT à l'aide AWS Step Functions de l'API Amazon Redshift Data. Une autre option consiste à utiliser l'éditeur de requêtes Amazon Redshift v2 pour planifier l'actualisation. Pour plus d'informations, consultez la section Planification d'une requête avec l'éditeur de requêtes v2.	

Connectez-vous QuickSight aux données dans Amazon Redshift

Tâche	Description	Compétences requises
Configurez QuickSight.	Pour le configurer QuickSigh t, suivez les instructions de la AWS documentation.	Ingénieur en migration
Configurez une connexion sécurisée entre Amazon Redshift QuickSight et Amazon.	Pour configurer une connexion sécurisée entre Amazon Redshift QuickSight et Amazon Redshift, procédez comme suit 1. Pour autoriser les connexions depuis QuickSight Amazon Redshift, ouvrez la console Amazon Redshift et ajoutez une règle d'entrée dans le groupe de sécurité Amazon	Ingénieur en migration

Tâche	Description	Compétences requises
	Redshift. La règle doit autoriser le trafic vers le port 5439 (le port Redshift par défaut) à partir de la plage CIDR où vous l'avez configuré. QuickSight Pour obtenir une liste des adresses IP Régions AWS et de leurs adresses IP, consultez Supporté Régions AWS pour QuickSight. 2. Sur la console Amazon Redshift, choisissez Groupe de travail, Accès aux données, Réseau et sécurité, puis activez Accès public.	

Tâche	Description	Compétences requises
Créez un jeu de données pour QuickSight.	Pour créer un ensemble de données pour QuickSight Amazon Redshift, procédez comme suit : 1. Sur la QuickSight console, dans le volet de navigation, sélectionnez Datasets. 2. Sur la page Jeux de données, choisissez Nouveau jeu de données. 3. Choisissez Redshift Manual Connect. 4. Dans la fenêtre de la nouvelle source de données Redshift, entrez les informations de connexion : • Dans le champ Nom de la source de données, entrez le nom de la source de données Amazon Redshift. • Pour Serveur de base de données, entrez le point de terminaison du cluster Amazon Redshift. Vous pouvez obtenir la valeur du point de terminais on dans le champ Point de terminaison de la section Informations générales pour le groupe de travail du cluster sur le tableau de bord Amazon	Ingénieur en migration

Tâche	Description	Compétences requises
	Redshift Serverless. L'adresse du serveur est la première partie du point de terminaison avant les deux points, comme illustré dans l'exemple suivant : `mfdata-insights.NNNNNNNN.us-east-1.redshift-serverless.amazonaws.com:5439/dev` • Pour le port, entrez `5439` (le port par défaut pour Amazon Redshift). • Entrez le nom de la base de données (après la barre oblique dans le point de terminaison). Dans ce cas, le nom de la base de données est`dev`. • Dans Nom d'utilisateur et mot de passe, entrez le nom d'utilisateur et le mot de passe de la base de données Amazon Redshift. 5. Choisissez Valider la connexion. En cas de succès, vous devriez voir une coche verte indiquant la validation. Si la validatio	

Tâche	Description	Compétences requises
	n échoue, consultez la section Dépannage. 6. Choisissez Create data source.	
Joignez-vous à l'ensemble de données.	Pour créer des analyses dans QuickSight, joignez les deux tables en suivant les instructions de la AWS documentation. Dans le volet Configuration de la jointure, choisissez Left pour le type de jointure. Sous Clauses d'adhésion, utilisez`memberid from member_plans = memberid from members_details` .	Ingénieur en migration

Obtenez des informations commerciales à partir des données du mainframe en utilisant Amazon Q dans QuickSight

Tâche	Description	Compétences requises
Configurez Amazon Q dans QuickSight.	Pour configurer la fonctionnalité Amazon Q dans QuickSight Generative BI, suivez les instructions de la AWS documentation.	Ingénieur en migration
Analysez les données du mainframe et créez un tableau de bord visuel.	Pour analyser et visualiser vos données dans QuickSight, procédez comme suit :	Ingénieur en migration

Tâche	Description	Compétences requises
	1. Pour créer l'analyse des données du mainframe, suivez les instructions de la AWS documentation. Pour le jeu de données, choisissez le jeu de données que vous avez créé. 2. Sur la page d'analyse, choisissez Build visual. 3. Dans la fenêtre Créer un sujet à analyser, choisisse z Mettre à jour le sujet existant. 4. Dans la liste déroulant e Sélectionnez un sujet, choisissez le sujet que vous avez créé précédemment. 5. Choisissez le lien entre les rubriques. 6. Après avoir créé le lien vers le sujet, choisissez Build visual pour ouvrir la fenêtre Amazon Q Build a Visual. 7. Dans la barre d'invite, rédigez vos questions d'analyse. Les exemples de questions utilisés pour ce modèle sont les suivants : • Afficher la répartition des membres par région • Afficher la répartition des membres par âge	

Tâche	Description	Compétences requises
	• Afficher la répartition des membres par sexe • Afficher la répartition des membres par type de plan • Afficher les membres qui n'ont pas terminé leur vaccination préventive Après avoir saisi vos questions, choisissez Créer. Amazon Q in QuickSight crée les visuels. 8. Pour ajouter les éléments visuels à votre tableau de bord visuel, choisissez AJOUTER À L'ANALYSE. Lorsque vous avez terminé, vous pouvez publier votre tableau de bord afin de le partager avec les autres membres de votre organisation. Pour des exemples, consultez le tableau de bord visuel du mainframe dans la section Informations supplémentaires.	

Créez une histoire de données avec Amazon Q à QuickSight partir de données du mainframe

Tâche	Description	Compétences requises
Créez une histoire de données.	Créez une histoire de données pour expliquer les conclusions de l'analyse précédente et générez une recommandation visant à accroître la vaccination préventive des membres : 1. Pour créer l'histoire des données, suivez les instructions de la AWS documentation. 2. Pour l'invite Data Story, utilisez ce qui suit : `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data for this pattern.` Vous pouvez également créer votre propre invite pour générer des récits	Ingénieur en migration

Tâche	Description	Compétences requises
	de données pour d'autres informations commerciales. 3. Choisissez Ajouter des éléments visuels, puis ajoutez ceux qui sont pertinents pour le récit des données. Pour ce modèle, utilisez les visuels que vous avez créés précédemment. 4. Sélectionnez Créer. 5. Par exemple, la sortie d'un récit de données, voir Sortie d'un récit de données dans la section Informations supplémentaires.	
Consultez l'histoire des données générées.	Pour afficher le récit de données généré, choisisse z-le sur la page Récits de données.	Ingénieur en migration
Modifiez un récit de données généré.	Pour modifier le formatage, la mise en page ou les éléments visuels d'un data story, suivez les instructions de la AWS documentation.	Ingénieur en migration
Partagez une histoire de données.	Pour partager une histoire de données, suivez les instructi ons de la AWS documenta tion.	Ingénieur en migration

Résolution des problèmes

Problème	Solution
QuickSight Pour deux Amazon Redshift, la création du jeu de données `Validate Connection` a échoué.	1. Vérifiez que le groupe de sécurité attaché à l'instance Amazon Redshift Serverless autorise le trafic entrant provenant de la plage d'adresses IP associée à la région dans laquelle vous l'avez configurée. QuickSight 2. Vérifiez que le VPC sur lequel Amazon Redshift Serverless est déployé est accessible au public. 3. Vérifiez que vous utilisez le nom d'utilisateur et le mot de passe corrects pour Amazon Redshift. Vous pouvez réinitialiser le nom d'utilisateur et le mot de passe sur la console Amazon Redshift.
La tentative de démarrage du moteur Apply sur l' EC2 instance renvoie le message d'erreur suivant : `-bash: sqdeng: command not found`	Exportez le chemin `sqdata` d'installation en exécutant la commande suivante : `export PATH=$PATH:/usr/sbin:/opt/precisely/di/sqdata/bin`
La tentative de démarrage du moteur d'application renvoie l'une des erreurs de connexion suivantes : • `SQDD018E Cannot connect to transfer socket(rc==0x18468). Agent:<Agent Name > Socket:/u/./sqdata/.DB2ZTOMSK.cab.data` • `SQDUR06E Error opening url cdc://<VPC end point name>:2626/`	Vérifiez le spool du mainframe pour vous assurer que les tâches du démon du contrôleur sont en cours d'exécution.

Problème	Solution
`DB2ZTOMSK/DB2ZTOMSK : errno:112 8 (Unknown error 1128)`	

Ressources connexes

- Générez des informations AWS Mainframe Modernization en utilisant Amazon Q dans QuickSight (modèle)
- Générez des informations sur AWS Mainframe Modernization les données en utilisant Amazon Q in QuickSight (démo)
- AWS Mainframe Modernization - Réplication des données pour IBM z/OS
- Amazon Redshift diffuse l'ingestion vers une vue matérialisée

Informations supplémentaires

Exemples de fichiers .ddl

members_details.ddl

```
CREATE TABLE MEMBER_DTLS (
memberid INTEGER NOT NULL,
member_name VARCHAR(50),
member_type VARCHAR(20),
age INTEGER,
gender CHAR(1),
email VARCHAR(100),
region VARCHAR(20)
);
```

member_plans.ddl

```
CREATE TABLE MEMBER_PLANS (
memberid INTEGER NOT NULL,
medical_plan CHAR(1),
dental_plan CHAR(1),
vision_plan CHAR(1),
preventive_immunization VARCHAR(20)
```

```
);
```

Exemple de fichier .sqd

<kafka topic name>Remplacez-le par le nom de votre rubrique Amazon MSK.

script.sqd

```
-- Name: DB2ZTOMSK: DB2z To MSK JOBNAME DB2ZTOMSK;REPORT EVERY 1;OPTIONS
 CDCOP('I','U','D');-- Source Descriptions
JOBNAME DB2ZTOMSK;
REPORT EVERY 1;
OPTIONS CDCOP('I','U','D');

-- Source Descriptions
BEGIN GROUP DB2_SOURCE;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_details.ddl AS
 MEMBER_DTLS;
DESCRIPTION DB2SQL /var/precisely/di/sqdata/apply/DB2ZTOMSK/ddl/mem_plans.ddl AS
 MEMBER_PLANS;
END GROUP;
-- Source Datastore
DATASTORE cdc://<zos_host_name>/DB2ZTOMSK/DB2ZTOMSK
OF UTSCDC
AS CDCIN
DESCRIBED BY GROUP DB2_SOURCE ;
-- Target Datastore(s)
DATASTORE 'kafka:///<kafka topic name>/key'
OF JSON
AS TARGET
DESCRIBED BY GROUP DB2_SOURCE;
PROCESS INTO TARGET
SELECT
{
REPLICATE(TARGET)
}
FROM CDCIN;
```

Tableau de bord visuel du mainframe

Le visuel de données suivant a été créé par Amazon Q QuickSight pour la question d'analyse `show member distribution by region`.

Le visuel de données suivant a été créé par Amazon Q QuickSight pour la questionshow member distribution by Region who have not completed preventive immunization, in pie chart.

Sortie d'une histoire de données

Les captures d'écran suivantes montrent des sections de l'histoire de données créée par Amazon Q QuickSight pour répondre à l'inviteBuild a data story about Region with most numbers of members. Also show the member distribution by age, member distribution by gender. Recommend how to motivate members to complete immunization. Include 4 points of supporting data for this pattern.

Dans l'introduction, l'histoire des données recommande de choisir la région comptant le plus grand nombre de membres afin de tirer le meilleur parti des efforts de vaccination.

L'histoire des données fournit une analyse du nombre de membres pour les quatre régions. Les régions du nord-est, du sud-ouest et du sud-est comptent le plus grand nombre de membres.

L'histoire des données présente une analyse des membres par âge.

L'histoire des données met l'accent sur les efforts de vaccination dans le Midwest.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Générez des informations sur les données en utilisant AWS Mainframe Modernization et Amazon Q dans QuickSight

Créée par Shubham Roy (AWS), Roshna Razack (AWS) et Santosh Kumar Singh (AWS)

Récapitulatif

Si votre entreprise héberge des données critiques dans un environnement mainframe, il est essentiel de tirer parti de ces données pour stimuler la croissance et l'innovation. En débloquant les données du mainframe, vous pouvez créer des informations commerciales plus rapides, sécurisées et évolutives afin d'accélérer la prise de décision, la croissance et l'innovation basées sur les données dans le cloud Amazon Web Services ()AWS.

Ce modèle présente une solution pour générer des informations commerciales et créer des récits partageables à partir de données du mainframe en utilisant le transfert de AWS Mainframe Modernization fichiers avec BMC et Amazon Q in. QuickSight Les ensembles de données du mainframe sont transférés vers Amazon Simple Storage Service (Amazon S3) à l'aide du transfert de fichiers AWS Mainframe Modernization avec BMC. Une AWS Lambda fonction formate et prépare le fichier de données du mainframe en vue de son chargement sur Amazon QuickSight.

Une fois les données disponibles dans QuickSight, vous pouvez utiliser des instructions en langage naturel avec Amazon Q QuickSight pour créer des résumés des données, poser des questions et générer des récits de données. Vous n'avez pas besoin d'écrire de requêtes SQL ou de vous familiariser avec un outil de business intelligence (BI).

Contexte commercial

Ce modèle présente une solution pour les cas d'utilisation de l'analyse des données sur le mainframe et de l'analyse des données. À l'aide de ce modèle, vous créez un tableau de bord visuel pour les données de votre entreprise. Pour démontrer la solution, ce modèle fait appel à une entreprise de soins de santé qui fournit des plans médicaux, dentaires et ophtalmologiques à ses membres aux États-Unis. Dans cet exemple, les données démographiques des membres et les informations relatives au plan sont stockées dans les ensembles de données du mainframe. Le tableau de bord visuel présente les éléments suivants :

- Répartition des membres par région
- Répartition des membres par sexe
- Répartition des membres par âge
- Répartition des membres par type de plan

- Membres qui n'ont pas terminé leur vaccination préventive

Après avoir créé le tableau de bord, vous générez un récit de données qui explique les informations issues de l'analyse précédente. L'histoire des données fournit des recommandations pour augmenter le nombre de membres ayant effectué des vaccinations préventives.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Ensembles de données mainframe contenant des données commerciales
- Accès pour installer un agent de transfert de fichiers sur le mainframe

Limites

- Le fichier de données de votre ordinateur central doit être dans l'un des formats de fichier pris en charge par QuickSight. Pour obtenir la liste des formats de fichiers pris en charge, consultez la QuickSight documentation Amazon.

  Ce modèle utilise une fonction Lambda pour convertir le fichier mainframe dans un format pris en charge par. QuickSight

Architecture

Le schéma suivant montre une architecture permettant de générer des informations commerciales à partir des données du mainframe à l'aide AWS Mainframe Modernization du transfert de fichiers avec BMC et Amazon Q. QuickSight

Le schéma suivant illustre le flux de travail suivant :

1. Un ensemble de données mainframe contenant des données commerciales est transféré vers Amazon S3 à l'aide AWS Mainframe Modernization du transfert de fichiers avec BMC.
2. La fonction Lambda convertit le fichier qui se trouve dans le compartiment S3 de destination du transfert de fichiers au format CSV (valeurs séparées par des virgules).
3. La fonction Lambda envoie le fichier converti au compartiment S3 du jeu de données source.

4. Les données du fichier sont ingérées par QuickSight.
5. Les utilisateurs accèdent aux données dans QuickSight. Vous pouvez utiliser Amazon Q QuickSight pour interagir avec les données à l'aide d'instructions en langage naturel.

Outils

Services AWS

- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Mainframe Modernization Le transfert de fichiers avec BMC convertit et transfère les ensembles de données du mainframe vers Amazon S3 pour des cas d'utilisation liés à la modernisation, à la migration et à l'augmentation du mainframe.
- Amazon QuickSight est un service de BI à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique. Ce modèle utilise les fonctionnalités de BI générative d'Amazon Q dans QuickSight.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Bonnes pratiques

- Lorsque vous créez les rôles AWS Identity and Access Management (IAM) pour le transfert de AWS Mainframe Modernization fichiers avec BMC et la fonction Lambda, suivez le principe du moindre privilège.
- Assurez-vous que votre jeu de données source prend en charge les types de données pour QuickSight. Si votre jeu de données source contient des types de données non pris en charge, convertissez-les en types de données pris en charge. Pour plus d'informations sur les types de données mainframe non pris en charge et sur la manière de les convertir en types de données pris en charge par Amazon Q dans QuickSight, consultez la section Ressources associées.

Épopées

Configurer le transfert AWS Mainframe Modernization de fichiers avec BMC

Tâche	Description	Compétences requises
Installez l'agent de transfert de fichiers.	Pour installer l'agent de transfert de AWS Mainframe Modernization fichiers sur votre ordinateur central, suivez les instructions de la AWS documentation.	Administrateur système mainframe
Créez un compartiment S3 pour le transfert de fichiers sur le mainframe.	Créez un compartiment S3 pour stocker le fichier de sortie de AWS Mainframe Modernization File Transfer with BMC. Dans le schéma d'architecture, il s'agit du compartiment de destination du transfert de fichiers.	Ingénieur en migration
Créez le point de terminaison du transfert de données.	1. Créez un compartiment S3 pour préparer le fichier mainframe d'entrée pour le transfert de AWS Mainframe Modernization fichiers avec BMC. 2. Pour créer le point de terminaison de transfert de données du mainframe, suivez les instructions de la AWS documentation.	Spécialiste de la modernisation des mainframes AWS

Convertissez l'extension de nom de fichier mainframe pour QuickSight l'intégration

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment S3 pour que la fonction Lambda copie le fichier mainframe converti de la source vers le compartiment de destination final.	Ingénieur en migration
Créez une fonction Lambda.	Pour créer une fonction Lambda qui modifie l'extension du fichier et copie le fichier mainframe dans le compartiment de destination, procédez comme suit : 1. Connectez-vous à la AWS Lambda console AWS Management Console et naviguez jusqu'à celle-ci. 2. Choisissez Créer une fonction, puis sélectionnez Auteur à partir de zéro. 3. Dans Nom de la fonction, entrez le nom de votre fonction. 4. Dans la liste déroulante Runtime, choisissez Python.3.X. 5. Développez Modifier le rôle d'exécution par défaut, puis choisissez Créer un nouveau rôle avec des	Ingénieur en migration

Tâche	Description	Compétences requises
	autorisations Lambda de base. 6. Choisissez Créer une fonction. 7. Choisissez l'onglet Code, puis collez le code `S3CopyLambda.py` Python fourni dans la section Informations supplémentaires. Le code Python a été généré à l'aide d'Amazon Q Developer dans l'environnement de développement intégré (IDE) Microsoft Visual Studio. 8. Modifiez le `destination_bucket_name` nom du compartiment S3 que vous avez créé précédemment et `change destination_file_key` le nom du fichier du mainframe. 9. Déployez la fonction Lambda.	

Tâche	Description	Compétences requises
Créez un déclencheur Amazon S3 pour appeler la fonction Lambda.	Pour configurer un déclencheur qui invoque la fonction Lambda, procédez comme suit : 1. Sur la console Lambda, ouvrez la page Fonctions. 2. Choisissez la fonction Lambda. 3. Dans Vue d'ensemble des fonctions, choisissez Ajouter un déclencheur. 4. Dans la liste déroulante Configuration du déclencheur, choisissez S3. 5. Dans le champ Bucket, entrez le nom de votre bucket source. 6. Dans la liste déroulante Type d'événement, sélectionnez Tous les événements de création d'objets. 7. Cochez la case Je reconnais qu'il n'est pas recommandé d'utiliser le même compartiment S3 en entrée et en sortie, puis choisissez Ajouter. Pour en savoir plus, consultez Didacticiel : Utilisation d'un	Responsable de la migration

Tâche	Description	Compétences requises
	déclencheur Amazon S3 pour appeler une fonction Lambda.	
Fournissez des autorisations IAM pour la fonction Lambda.	Des autorisations IAM sont requises pour que la fonction Lambda puisse accéder aux compartiments S3 du jeu de données source et de destination du transfert de fichiers. Mettez à jour la politique associée au rôle d'exécution de la fonction Lambda en autorisant `s3:GetObject` et en autorisant le `s3:DeleteObject` compartiment S3 de destination du transfert de fichiers et l'`s3:PutObject` accès au compartiment S3 du jeu de données source. Pour plus d'informations, consultez la section Créer une politique d'autorisations dans Tutoriel : Utilisation d'un déclencheur Amazon S3 pour appeler une fonction Lambda.	Responsable de la migration

Définition d'une tâche de transfert de données sur un mainframe

Tâche	Description	Compétences requises
Créez une tâche de transfert pour copier le fichier du mainframe dans le compartiment S3.	Pour créer une tâche de transfert de fichiers sur mainframe, suivez les instructi	Ingénieur en migration

Tâche	Description	Compétences requises
	ons de la AWS Mainframe Modernization documentation. **Note** Spécifiez le codage de page de code source comme IBM1047 et le codage de page de code cible comme UTF-8.	
Vérifiez la tâche de transfert.	Pour vérifier que le transfert de données est réussi, suivez les instructions de la AWS Mainframe Modernization documentation. Vérifiez que le fichier mainframe se trouve dans le compartiment S3 de destination pour le transfert de fichiers.	Responsable de la migration

Tâche	Description	Compétences requises
Vérifiez la fonction de copie Lambda.	Vérifiez que la fonction Lambda est lancée et que le fichier est copié avec une extension .csv dans le compartiment S3 du jeu de données source. Le fichier .csv créé par la fonction Lambda est le fichier de données d'entrée pour. QuickSight Pour des exemples de données, consultez le `Sample-data-member-healthcare-APG` fichier dans la section Pièces jointes.	Responsable de la migration

Connect QuickSight aux données du mainframe

Tâche	Description	Compétences requises
Configurez QuickSight.	Pour le configurer QuickSigh t, suivez les instructions de la AWS documentation.	Responsable de la migration
Créez un jeu de données pour QuickSight.	Pour créer un ensemble de données pour QuickSight, suivez les instructions de la AWS documentation. Le fichier de données d'entrée est le fichier d'ordinateur central converti créé lorsque vous avez défini la tâche de transfert de données de l'ordinateur central.	Responsable de la migration

Obtenez des informations commerciales à partir des données du mainframe en utilisant Amazon Q dans QuickSight

Tâche	Description	Compétences requises
Configurez Amazon Q dans QuickSight.	Cette fonctionnalité nécessite l'édition Enterprise. Pour configurer Amazon Q dans QuickSight, procédez comme suit : 1. Pour obtenir le module complémentaire Amazon Q, suivez les instructions Étape 1 : Obtenir le module complémentaire Q dans la AWS documentation. 2. Pour utiliser les fonctionn alités de BI générative d'Amazon Q, mettez à niveau les comptes de vos utilisateurs. Suivez les instructions de la AWS documentation. 3. Créez une rubrique Amazon Q en utilisant le jeu de données que vous avez créé précédemment. Suivez les instructions de la AWS documentation. 4. Pour configurer les métadonnées du sujet de manière à ce qu'elles soient adaptées au langage naturel, suivez les instructi	Responsable de la migration

Tâche	Description	Compétences requises
	ons de la documenta tion.AWS	

Tâche	Description	Compétences requises
Analysez les données du mainframe et créez un tableau de bord visuel.	Pour analyser et visualiser vos données dans QuickSight, procédez comme suit : 1. Pour créer l'analyse des données du mainframe, suivez les instructions de la AWS documentation. Pour le jeu de données, choisissez le jeu de données créé à l'étape précédente. 2. Sur la page d'analyse, choisissez Build visual. 3. Dans la fenêtre Créer un sujet à analyser, choisisse z Mettre à jour le sujet existant. 4. Dans la liste déroulant e Sélectionnez un sujet, choisissez le sujet que vous avez créé précédemment. 5. Choisissez le lien entre les rubriques. 6. Après avoir créé le lien vers le sujet, choisissez Build visual pour ouvrir la fenêtre Amazon Q Build a Visual. 7. Dans la barre d'invite, rédigez vos questions d'analyse. Les exemples de questions utilisés pour ce modèle sont les suivants :	Ingénieur en migration

Tâche	Description	Compétences requises
	• Afficher la répartition des membres par région • Afficher la répartition des membres par âge • Afficher la répartition des membres par sexe • Afficher la répartition des membres par type de plan • Afficher le membre qui n'a pas terminé sa vaccination préventive Après avoir saisi vos questions, choisissez Créer. Amazon Q in QuickSight crée les visuels. 8. Pour ajouter les éléments visuels à votre tableau de bord visuel, choisissez AJOUTER À L'ANALYSE. Lorsque vous avez terminé, vous pouvez publier votre tableau de bord afin de le partager avec les autres membres de votre organisation. Pour des exemples, consultez le tableau de bord visuel du mainframe dans la section Informations supplémentaires.	

Créez un récit de données avec Amazon Q à QuickSight partir des données du mainframe

Tâche	Description	Compétences requises
Créez une histoire de données.	Créez une histoire de données pour expliquer les conclusions de l'analyse précédente et générer une recommandation visant à accroître la vaccination préventive des membres : 1. Pour créer l'histoire des données, suivez les instructions de la AWS documentation. 2. Pour l'invite Data Story, utilisez ce qui suit : `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data for this pattern.` Vous pouvez également créer votre propre invite pour générer des récits	Ingénieur en migration

Tâche	Description	Compétences requises
	de données pour d'autres informations commerciales. 3. Choisissez Ajouter des éléments visuels, puis ajoutez ceux qui sont pertinents pour le récit des données. Pour ce modèle, utilisez les visuels que vous avez créés précédemment. 4. Sélectionnez Créer. 5. Par exemple, la sortie d'un récit de données, voir Sortie d'un récit de données dans la section Informations supplémentaires.	
Consultez l'histoire des données générées.	Pour consulter l'histoire des données générées, suivez les instructions de la AWS documentation.	Responsable de la migration
Modifiez un récit de données généré.	Pour modifier le formatage, la mise en page ou les éléments visuels d'un data story, suivez les instructions de la AWS documentation.	Responsable de la migration
Partagez une histoire de données.	Pour partager une histoire de données, suivez les instructi ons de la AWS documenta tion.	Ingénieur en migration

Résolution des problèmes

Problème	Solution
Impossible de découvrir les fichiers ou ensembles de données du mainframe saisis dans les critères de recherche des ensembles de données pour Créer une tâche de transfert dans Transfert de AWS Mainframe Modernization fichiers avec BMC.	1. Vérifiez d'abord la connexion en choisissant les points de terminaison du transfert de données sur la console AWS Mainframe Modernization Transférer avec BMC. Si le dernier battement cardiaque est supérieur à deux minutes, la connexion pour le transfert de fichiers n'a pas été établie. Si le dernier battement de cœur est inférieur à 2 minutes pour l'agent exécuté sur le mainframe, la connexion à l'agent est réussie. Passez à l'étape 2. 2. Vérifiez la AWS Secrets Manager configuration. Une clé secrète doit être configurée dans Secrets Manager avec une clé `userId` (I majuscule) avec la valeur de l'ID utilisateur du mainframe et une clé `password` avec la valeur du mot de passe du mainframe . Les clés `password` secrètes `userId` et majuscules distinguent les majuscules des minuscules et doivent être saisies telles quelles.

Ressources connexes

Pour convertir des types de données mainframe tels que PACKED-DECIMAL (COMP-3) ou BINARY (COMP ou COMP-4) en un type de données pris en charge par, consultez les modèles suivants : QuickSight

- Convertissez et décompressez les données EBCDIC en ASCII à l'aide de Python AWS
- Convertissez des fichiers mainframe du format EBCDIC au format ASCII délimité par des caractères dans Amazon S3 en utilisant AWS Lambda

Informations supplémentaires

S3 CopyLambda .py

Le code Python suivant a été généré à l'aide d'une invite avec Amazon Q Developer dans un IDE :

```
#Create a lambda function triggered by S3. display the S3 bucket name and key
import boto3
s3 = boto3.client('s3')
def lambda_handler(event, context):
print(event)
bucket = event['Records'][0]['s3']['bucket']['name']
key = event['Records'][0]['s3']['object']['key']
print(bucket, key)
#If key starts with object_created, skip copy, print "copy skipped". Return lambda with
 key value.
if key.startswith('object_created'):
print("copy skipped")
return {
'statusCode': 200,
'body': key
}
# Copy the file from the source bucket to the destination bucket.
 Destination_bucket_name = 'm2-filetransfer-final-opt-bkt'. Destination_file_key =
 'healthdata.csv'
copy_source = {'Bucket': bucket, 'Key': key}
s3.copy_object(Bucket='m2-filetransfer-final-opt-bkt', Key='healthdata.csv',
 CopySource=copy_source)
print("file copied")
#Delete the file from the source bucket.
s3.delete_object(Bucket=bucket, Key=key)
return {
'statusCode': 200,
'body': 'Copy Successful'
}
```

Tableau de bord visuel du mainframe

Le visuel de données suivant a été créé par Amazon Q QuickSight pour la question d'analyse `show member distribution by region`.

Le visuel de données suivant a été créé par Amazon Q QuickSight pour la questionshow member distribution by Region who have not completed preventive immunization, in pie chart.

Sortie d'une histoire de données

Les captures d'écran suivantes montrent des sections de l'histoire de données créée par Amazon Q QuickSight pour répondre à l'invite `Build a data story about Region with most numbers of members. Also show the member distribution by medical plan, vision plan, dental plan. Recommend how to motivate members to complete immunization. Include 4 points of supporting data.`

Dans l'introduction, l'histoire des données recommande de choisir la région comptant le plus grand nombre de membres afin de tirer le meilleur parti des efforts de vaccination.

L'histoire des données fournit une analyse du nombre de membres pour les trois principales régions et désigne le Sud-Ouest comme la principale région axée sur les efforts de vaccination.

> **Note**
>
> Les régions du sud-ouest et du nord-est comptent chacune huit membres. Cependant, le Sud-Ouest compte un plus grand nombre de membres qui ne sont pas complètement vaccinés. Il est donc plus susceptible de bénéficier des initiatives visant à augmenter les taux de vaccination.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Intégrez le contrôleur universel Stonebranch à la modernisation du mainframe AWS

Créée par Vaidy Sankaran (AWS), Robert Lemieux (Stonebranch), Huseyin Gomleksizoglu (Stonebranch) et Pablo Alonso Prieto (AWS)

Récapitulatif

Ce modèle explique comment intégrer l'orchestration de la charge de travail du Stonebranch Universal Automation Center (UAC) au service de modernisation du mainframe Amazon Web Services (AWS). Le service de modernisation du mainframe AWS migre et modernise les applications du mainframe vers le cloud AWS. Il propose deux modèles : la replateforme de modernisation du mainframe AWS avec la technologie Micro Focus Enterprise et le refactor automatisé de modernisation du mainframe AWS avec AWS Blu Age.

Stonebranch UAC est une plateforme d'automatisation et d'orchestration informatiques en temps réel. L'UAC est conçu pour automatiser et orchestrer les tâches, les activités et les flux de travail sur les systèmes informatiques hybrides, qu'ils soient sur site ou sur AWS. Les entreprises clientes utilisant des systèmes mainframe sont en train de passer à des infrastructures et des applications modernisées centrées sur le cloud. Les outils et services professionnels de Stonebranch facilitent la migration des planificateurs existants et des fonctionnalités d'automatisation vers le cloud AWS.

Lorsque vous migrez ou modernisez vos programmes mainframe vers le cloud AWS à l'aide du service AWS Mainframe Modernization, vous pouvez utiliser cette intégration pour automatiser la planification par lots, accroître l'agilité, améliorer la maintenance et réduire les coûts.

Ce modèle fournit des instructions pour intégrer le planificateur Stonebranch aux applications mainframe migrées vers le service de modernisation du mainframe AWS Micro Focus Enterprise Runtime. Ce modèle est destiné aux architectes de solutions, aux développeurs, aux consultants, aux spécialistes de la migration et aux autres personnes travaillant dans les domaines des migrations, des modernisations, des opérations ou. DevOps

Résultat ciblé

Ce modèle vise à fournir les résultats cibles suivants :

- Possibilité de planifier, d'automatiser et d'exécuter des tâches par lots sur mainframe exécutées dans le service AWS Mainframe Modernization (environnement d'exécution Microfocus) de Stonebranch Universal Controller.
- Surveillez les processus par lots de l'application à partir du contrôleur universel Stonebranch.

- Start/Restart/Rerun/Stoples traitements par lots sont effectués automatiquement ou manuellement à partir du contrôleur universel Stonebranch.
- Récupérez les résultats des processus par lots de modernisation du mainframe AWS.
- Capturez les CloudWatch journaux AWS des tâches par lots dans Stonebranch Universal Controller.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une application Micro Focus Bankdemo avec des fichiers JCL (langage de contrôle des tâches) et un processus par lots déployé dans un environnement de service AWS Mainframe Modernization (exécution Micro Focus)
- Connaissances de base sur la création et le déploiement d'une application mainframe exécutée sur Micro Focus Enterprise Server
- Connaissances de base du contrôleur universel Stonebranch
- Licence d'essai Stonebranch (contactez Stonebranch)
- Instances Amazon Elastic Compute Cloud (Amazon EC2) pour Windows ou Linux (par exemple, xlarge) avec un minimum de quatre cœurs, 8 Go de mémoire et 2 Go d'espace disque
- Apache Tomcat version 8.5.x ou 9.0.x
- Oracle Java Runtime Environment (JRE) ou OpenJDK version 8 ou 11
- Édition compatible avec Amazon Aurora MySQL
- Compartiment Amazon Simple Storage Service (Amazon S3) pour le référentiel d'exportation
- Amazon Elastic File System (Amazon EFS) pour les connexions à l'agent Stonebranch Universal Message Service (OMS) pour une haute disponibilité (HA)
- Fichiers d'installation de Stonebranch Universal Controller 7.2 Universal Agent 7.2
- Modèle de planification des tâches de modernisation du mainframe AWS (dernière version publiée du fichier .zip)

Limites

- Le produit et la solution ont été testés et leur compatibilité validée uniquement avec OpenJDK 8 et 11.

- Le modèle de planification des tâches aws-mainframe-modernization-stonebranch-integration fonctionnera uniquement avec le service AWS Mainframe Modernization.
- Ce modèle de planification des tâches ne fonctionnera que sur une édition Unix, Linux ou Windows des agents Stonebranch.
- Certains services AWS ne sont pas disponibles dans toutes les régions AWS. Pour connaître la disponibilité par région, consultez la section Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Architecture de l'état cible

Le schéma suivant montre l'exemple d'environnement AWS requis pour ce projet pilote.

1. Le Stonebranch Universal Automation Center (UAC) comprend deux composants principaux : le contrôleur universel et les agents universels. Stonebranch OMS est utilisé comme bus de messages entre le contrôleur et les agents individuels.
2. La base de données Stonebranch UAC est utilisée par Universal Controller. La base de données peut être compatible avec MySQL, Microsoft SQL Server, Oracle ou Aurora MySQL.
3. Service de modernisation du mainframe AWS : environnement d'exécution Micro Focus avec l'BankDemo application déployée. Les fichiers de BankDemo l'application seront stockés dans un compartiment S3. Ce compartiment contient également les fichiers JCL du mainframe.
4. Stonebranch UAC peut exécuter les fonctions suivantes pour l'exécution par lots :
    a. Démarrez un traitement par lots en utilisant le nom de fichier JCL qui existe dans le compartiment S3 lié au service de modernisation du mainframe AWS.
    b. Obtenez le statut de l'exécution du traitement par lots.
    c. Attendez que l'exécution du traitement par lots soit terminée.
    d. Récupère les journaux du traitement par lots exécuté.
    e. Réexécutez les tâches par lots qui ont échoué.
    f. Annulez le traitement par lots pendant qu'il est en cours d'exécution.
5. Stonebranch UAC peut exécuter les fonctions suivantes pour l'application :
    a. Démarrer l'application

b. Obtenir le statut de la demande
c. Attendez que l'application soit démarrée ou arrêtée
d. Arrêter l'application
e. Récupère les journaux du fonctionnement de l'application

Conversion d'emplois à Stonebranch

Le schéma suivant représente le processus de conversion des emplois de Stonebranch au cours du processus de modernisation. Il décrit comment les plannings de travail et les définitions de tâches sont convertis dans un format compatible capable d'exécuter les tâches par lots d'AWS Mainframe Modernization.

1. Pour le processus de conversion, les définitions de tâches sont exportées depuis le système mainframe existant.
2. Les fichiers JCL peuvent être chargés dans le compartiment S3 pour l'application Mainframe Modernization afin que ces fichiers JCL puissent être déployés par le service AWS Mainframe Modernization.
3. L'outil de conversion convertit les définitions de tâches exportées en tâches UAC.
4. Une fois que toutes les définitions de tâches et tous les plannings de tâches ont été créés, ces objets seront importés dans le contrôleur universel. Les tâches converties exécutent ensuite les processus dans le service AWS Mainframe Modernization au lieu de les exécuter sur le mainframe.

Architecture UAC de Stonebranch

Le schéma d'architecture suivant représente un active-active-passive modèle de contrôleur universel haute disponibilité (HA). Stonebranch UAC est déployé dans plusieurs zones de disponibilité pour fournir une haute disponibilité et prendre en charge la reprise après sinistre (DR).

Contrôleur universel

Deux serveurs Linux sont fournis en tant que contrôleurs universels. Les deux se connectent au même point de terminaison de base de données. Chaque serveur héberge une application Universal Controller et un OMS. La version la plus récente d'Universal Controller est utilisée au moment de son approvisionnement.

Les contrôleurs universels sont déployés dans l'application Web Tomcat en tant que document ROOT et sont servis sur le port 80. Ce déploiement facilite la configuration de l'équilibreur de charge frontal.

Le protocole HTTP via TLS ou HTTPS est activé à l'aide du certificat générique Stonebranch (par exemple,). `https://customer.stonebranch.cloud` Cela permet de sécuriser la communication entre le navigateur et l'application.

OMS

Un agent universel et un OMS (Opswise Message Service) résident sur chaque serveur Universal Controller. Tous les agents universels déployés par le client sont configurés pour se connecter aux deux services OMS. OMS agit comme un service de messagerie commun entre les agents universels et le contrôleur universel.

Amazon EFS monte un répertoire spool sur chaque serveur. OMS utilise ce répertoire de spouls partagé pour conserver les informations de connexion et de tâche communiquées aux contrôleurs et aux agents. OMS fonctionne en mode haute disponibilité. Si l'OMS actif tombe en panne, l'OMS passif a accès à toutes les données et reprend automatiquement les opérations actives. Les agents universels détectent cette modification et se connectent automatiquement au nouvel OMS actif.

Database (Base de données)

Amazon Relational Database Service (Amazon RDS) héberge la base de données UAC, avec Amazon Aurora MySQL comme moteur compatible. Amazon RDS aide à gérer et à proposer des sauvegardes planifiées à intervalles réguliers. Les deux instances d'Universal Controller se connectent au même point de terminaison de base de données.

Équilibreur de charge

Un Application Load Balancer est configuré pour chaque instance. L'équilibreur de charge dirige le trafic vers le contrôleur actif à tout moment. Les noms de domaine de vos instances pointent vers les points de terminaison respectifs de l'équilibreur de charge.

URLs

Chacune de vos instances possède une URL, comme illustré dans l'exemple suivant.

Environnement	Instance

Production	`customer.stonebranch.cloud`
Développement (hors production)	`customerdev.stonebranch.cloud`
Tests (hors production)	`customertest.stonebranch.cloud`

> **Note**
>
> Les noms des instances hors production peuvent être définis en fonction de vos besoins.

Haute disponibilité

La haute disponibilité (HA) est la capacité d'un système à fonctionner en continu sans défaillance pendant une période donnée. Ces défaillances incluent, sans toutefois s'y limiter, le stockage, les retards de réponse aux communications du serveur causés par des problèmes de processeur ou de mémoire, et la connectivité réseau.

Pour répondre aux exigences de haute disponibilité :

- Toutes les EC2 instances, bases de données et autres configurations sont mises en miroir dans deux zones de disponibilité distinctes au sein de la même région AWS.
- Le contrôleur est approvisionné via une Amazon Machine Image (AMI) sur deux serveurs Linux situés dans les deux zones de disponibilité. Par exemple, si vous êtes approvisionné dans la région Europe eu-west-1, vous disposez d'un contrôleur universel dans la zone de disponibilité eu-west-1a et dans la zone de disponibilité eu-west-1c.
- Aucune tâche n'est autorisée à s'exécuter directement sur les serveurs d'applications et aucune donnée n'est autorisée à être stockée sur ces serveurs.
- L'Application Load Balancer effectue des contrôles de santé sur chaque contrôleur universel afin d'identifier le contrôleur actif et de diriger le trafic vers celui-ci. En cas de problème avec un serveur, l'équilibreur de charge met automatiquement le contrôleur universel passif en état actif. L'équilibreur de charge identifie ensuite la nouvelle instance de contrôleur universel active à partir des bilans de santé et commence à diriger le trafic. Le basculement se produit en quatre minutes sans perte de travail, et l'URL du frontend reste la même.
- Le service de base de données compatible Aurora MySQL stocke les données du contrôleur universel. Pour les environnements de production, un cluster de base de données est créé avec

deux instances de base de données situées dans deux zones de disponibilité différentes au sein d'une même région AWS. Les deux contrôleurs universels utilisent une interface Java Database Connectivity (JDBC) qui pointe vers un seul point de terminaison de cluster de bases de données. En cas de problème avec une instance de base de données, le point de terminaison du cluster de bases de données pointe dynamiquement vers l'instance saine. Aucune intervention manuelle n'est requise.

Backup et purge

Le contrôleur universel Stonebranch est configuré pour sauvegarder et purger les anciennes données selon le calendrier indiqué dans le tableau.

Type	Schedule
Activité	7 jours
Audit	90 jours
Historique	60 jours

Les données de sauvegarde antérieures aux dates indiquées sont exportées au format .xml et stockées dans le système de fichiers. Une fois le processus de sauvegarde terminé, les anciennes données sont purgées de la base de données et archivées dans un compartiment S3 pendant un an maximum pour les instances de production.

Vous pouvez ajuster ce calendrier dans l'interface de votre contrôleur universel. Cependant, l'augmentation de ces délais peut entraîner un temps d'arrêt plus long pendant la maintenance.

Outils

Services AWS

- AWS Mainframe Modernization est une plateforme native du cloud AWS qui vous aide à moderniser vos applications mainframe pour les adapter aux environnements d'exécution gérés par AWS. Il fournit des outils et des ressources pour vous aider à planifier et à implémenter la migration et la modernisation.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon. EC2

- Amazon Elastic File System (Amazon EFS) vous aide à créer et à configurer des systèmes de fichiers partagés dans le cloud AWS.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS. Ce modèle utilise Amazon Aurora MySQL Compatible Edition.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les EC2 instances Amazon, les conteneurs et les adresses IP dans une ou plusieurs zones de disponibilité. Ce modèle utilise un Application Load Balancer.

Branche en pierre

- Universal Automation Center (UAC) est un système de produits d'automatisation de la charge de travail d'entreprise. Ce modèle utilise les composants UAC suivants :
  - Universal Controller, une application Web Java exécutée dans un conteneur Web Tomcat, est la solution de planification de tâches d'entreprise et de courtier d'automatisation de la charge de travail d'Universal Automation Center. Le Controller présente une interface utilisateur permettant de créer, de surveiller et de configurer les informations du Controller ; gère la logique de planification ; traite tous les messages à destination et en provenance d'Universal Agents ; et synchronise une grande partie des opérations de haute disponibilité d'Universal Automation Center.
  - Universal Agent est un agent de planification indépendant du fournisseur qui collabore avec le planificateur de tâches existant sur toutes les principales plateformes informatiques, qu'elles soient existantes ou distribuées. Tous les planificateurs exécutés sous z/Series, i/Series, Unix, Linux ou Windows sont pris en charge.
- Universal Agent est un agent de planification indépendant du fournisseur qui collabore avec le planificateur de tâches existant sur toutes les principales plateformes informatiques, qu'elles soient existantes ou distribuées. Tous les planificateurs exécutés sous z/Series, i/Series, Unix, Linux ou Windows sont pris en charge.
- Stonebranch aws-mainframe-modernization-stonebranch -integration AWS Mainframe Modernization Universal Extension est le modèle d'intégration permettant d'exécuter, de surveiller et de réexécuter des tâches par lots dans la plateforme AWS Mainframe Modernization.

Code

Le code de ce modèle est disponible dans le GitHub référentiel aws-mainframe-modernization-stonebranch-integration.

Épopées

Installez Universal Controller et Universal Agent sur Amazon EC2

Tâche	Description	Compétences requises
Téléchargez les fichiers d'installation.	Téléchargez l'installation depuis les serveurs Stonebranch. Pour obtenir les fichiers d'installation, contactez Stonebranch.	Architecte du cloud
Lancez l' EC2 instance.	Vous aurez besoin d'environ 3 Go d'espace supplémentaire pour les installations d'Universal Controller et d'Universal Agent. Prévoyez donc au moins 30 Go d'espace disque pour l'instance. Ajoutez le port 8080 au groupe de sécurité afin qu'il soit accessible.	Architecte du cloud
Vérifiez les prérequis.	Avant l'installation, procédez comme suit : 1. Installez Java comme décrit dans la section Téléchargement de l'environnement d'exécution Java. `$ sudo yum -y update`	Administrateur cloud, administrateur Linux

Tâche	Description	Compétences requises

	``
	$ sudo yum install
	 java-11-amazon-cor
	retto
	``
	Assurez-vous d'utiliser l'une des versions de JAVA prises en charge. La commande précédente devrait installer java-11. Vérifiez la version Java et assurez-vous d'utiliser la version 11 avant de continuer.
	2. Comme décrit dans Installation d'Apache Tomcat, exécutez les commandes suivantes.
	``
	$ sudo yum install
	 tomcat tomcat-admin-
	webapps
	$ sudo systemctl
	 enable tomcat
	$ sudo systemctl start
	 tomcat
	``
	3. Créez une base de données Amazon Aurora comme décrit dans Création et connexion à un cluster de bases de données Aurora MySQL. Utilisez l'édition compatible avec Amazon Aurora MySQL.
	Choisissez un nom d'utilisateur principal et un mot de	

Tâche	Description	Compétences requises
	passe principal. Conservez les valeurs par défaut pour le reste des paramètres.	

Tâche	Description	Compétences requises

Installez le contrôleur universel.	1. Téléchargez le fichier `universal-controller-7.2.0.0.tar` d'installation sur l' EC2 instance.
	2. Désarchivez les fichiers d'installation `temp` dans un dossier.
	`$ tar -xvf universal-controller-7.2.0.0.tar`
	3. Autorisez l'exécution du script d'installation.
	`$ chmod a+x install-controller.sh`
	4. Installez le contrôleur. Cet exemple utilise la commande suivante pour installer Universal Controller sous `/usr/share/tomcat` . Utilisez la base de données Amazon Aurora que vous avez créée lors des étapes précédentes.
	`$ sudo ./install-controller.sh --tomcat-dir /usr/share/tomcat/ --controller-file universal-controller-7.2.0.0-build.145.war --dbuser admin --dbpass`
		Architecte cloud, administrateur Linux

Tâche	Description	Compétences requises
	“****” --dbname uc --rdbms mysql --dburl jdbc:mysql://database-2-instance-1.cih63miincgy.us-east-1.rds.amazonaws.com:3306/ La dernière ligne du résultat du script doit être « Installation terminée ». 5. Accédez à l'URL suivante dans l' EC2 instance. http://<public_ip>:8080/uc 6. Sur l'écran de connexion, saisissez ops.admin dans la section Nom d'utilisateur et laissez le champ Mot de passe vide. 7. Définissez un nouveau mot de passe pour l'ops.admin utilisateur.	

Tâche	Description	Compétences requises

Installez Universal Agent.	1. Téléchargez le fichier `sb-7.2.0.1-linux-3.10-x86_64.tar.Z` d'installation sur l' EC2 instance.
	2. Connectez-vous à l' EC2 instance.
	3. Désarchivez le package d'installation de l'agent universel.
	`$ zcat sb-7.2.0.1-linux-3.10-x86_64.tar.Z | tar xvf -`
	4. Exécutez la commande suivante.
	`$ sudo ./unvinst --oms_servers 7878@localhost --oms_autostart yes --python yes`
	5. Créez un fichier PAM.
	`$ cp /etc/pam.d/login /etc/pam.d/ucmd`
	6. Activez le démarrage automatique pour Universal Agent.
	`$ /sbin/restorecon -v /etc/rc.d/init.d/ubrokerd`
		Administrateur cloud, administrateur Linux

Tâche	Description	Compétences requises
Ajoutez OMS à Universal Controller.	1. Connectez-vous à Universal Controller avec l'`ops.admin` utilisateur. 2. Choisissez le menu Services dans le coin supérieur gauche de l'écran, puis choisissez le menu Serveurs OMS dans le système 3. Dans le champ Adresse du serveur OMS`localhost` , tapez, puis enregistrez. 4. Vous verrez l'état du serveur OMS comme connecté et l'état de la session comme opération nel.	Administrateur d'Universal Controller

Importez l'extension universelle AWS Mainframe Modernization et créez une tâche

Tâche	Description	Compétences requises
Importer un modèle d'intégration.	Pour cette étape, vous avez besoin de l'extension universelle AWS Mainframe Modernization. Assurez-vous que la dernière version publiée du fichier .zip est téléchargée. 1. Connectez-vous au contrôleur universel avec l'`ops.admin` utilisateur.	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	2. Accédez à Services, Importer un modèle d'intégration. 3. Sélectionnez le fichier .zip du modèle d'intégration (`aws_mainframe_modernization_stonebranch_extension.zip`), puis choisissez Importer. Une fois le modèle d'intégration importé, vous verrez les tâches de modernisation du mainframe AWS sous Services disponibles.	

Tâche	Description	Compétences requises
Activez les informations d'identification résolubles.	1. Accédez aux services et aux tâches de modernisation du mainframe AWS. 2. Sur le panneau de droite, renseignez les champs obligatoires : • Nom : Nouvelle tâche de modernisation du mainframe • Agent : sélectionnez le seul agent (AGNT0001). Dans la section Détails de la modernisation du mainframe AWS : • Action : répertorier les environnements • Informations d'identification AWS : si un rôle AWS Identity and Access Management (IAM) a été ajouté à l' EC2 instance, vous pouvez laisser ce champ vide. Si vous voulez utiliser `AWSAccessKeyID` et`AWSSecretKey` , choisissez l'icône () à côté du champ. Dans la fenêtre Informations d'identification qui s'ouvre, entrez les informati	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	ons suivantes, puis enregistrez. • Nom : Informations d'identification pour la modernisation du mainframe AWS • Utilisateur d'exécution : saisissez l'ID de la clé d'accès AWS dans ce champ. • Mot de passe d'exécuti on : écrivez la clé secrète AWS dans ce champ. • Point final : assurez-vous que le point de terminaison possède la bonne région AWS. L'argument par défaut est `https://m2.us-east-1.amazonaws.com` . • Région : entrez la région du service de modernisa tion du mainframe AWS. L'argument par défaut est `us-east-1` . 3. Conservez les valeurs par défaut dans les autres champs et enregistrez la tâche.	

Tâche	Description	Compétences requises
Lancez la tâche.	1. En haut du panneau de droite, choisissez Launch Task. 2. Dans la fenêtre de confirmation, choisisse z Launch. Ensuite, la console Universal Controlle r affichera un message similaire au message suivant. 08-24 10 h 11 h 49 Lancement réussi de la tâche universelle « Nouvelle tâche de modernisation du mainframe » avec l'instanc e de tâche sys_id NC8 1661291493634146313 E38 OZJY. DB8 3. Accédez aux instances Si vous ne voyez pas l'onglet Instances, cliquez sur la flèche droite pour faire défiler la page vers la droite. 4. Ouvrez le menu contextue l (clic droit) de l'instanc e de tâche dans la liste, choisissez Extraire la sortie, puis choisissez Soumettre dans la section Extraire la sortie	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	5. Dans la fenêtre Retrieve Output, vous verrez la liste des environnements dans STDOUT.	

Tester le démarrage d'une tâche par lots

Tâche	Description	Compétences requises
Créez une tâche pour le traitement par lots.	1. Accédez aux services et aux tâches de modernisation du mainframe AWS. 2. Sur le panneau de droite, renseignez les champs obligatoires : • Nom : Nouvelle tâche de modernisation du mainframe • Agent : sélectionnez le seul agent (AGNT0001). Dans la section Détails de la modernisation du mainframe AWS : • Action : démarrer le traitement par lots (ou démarrer le traitement par lots et attendre que la tâche soit terminée dans AWS) • Informations d'identification AWS : si un rôle IAM a été ajouté à l' EC2 instance, vous pouvez	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	laisser ce champ vide. Si vous voulez utiliser `AWSAccessKeyID` et`AWSSecretKey` , choisissez l'icône () à côté du champ. • Point final : assurez-vous que le point de terminaison possède la bonne région AWS. L'argument par défaut est https://m2.us-east-1.amazonaws.com. • Région : entrez la région du service de modernisation du mainframe AWS. L'argument par défaut est `us-east-1` . • Application : cliquez sur l'icône à côté du champ (), puis choisissez Soumettre dans les choix d'applications d'actualisation. Cela permettra de se connecter au service AWS Mainframe Modernization et de renvoyer la liste des applications. Vous pouvez maintenant sélectionner l'application dans la liste déroulante. Sélectionnez l'application dans laquelle vous	

Tâche	Description	Compétences requises
	souhaitez exécuter le traitement par lots. • Nom du fichier JCL : `RUNHELLO.jcl` • Attendre le succès ou l'échec : si cette option est sélectionnée, la tâche attendra que le traitement par lots soit considéré comme un succès ou un échec. • Intervalle d'interrogation : il s'agit de la durée entre chaque interrogation. • Extraire les journaux d'exécution : si cette option est sélectionnée, les journaux seront extraits automatiquement une fois le traitement par lots terminé. • Format du journal : il s'agit du format des journaux à imprimer. Il peut être au format texte ou JSON. 3. Conservez les valeurs par défaut dans les autres champs et enregistrez la tâche.	

Tâche	Description	Compétences requises
Lancez la tâche.	1. En haut du panneau de droite, choisissez Launch Task. 2. Dans la fenêtre de confirmation, choisisse z Launch. Ensuite, la console Universal Controlle r affichera un message similaire au message suivant. 08-24 11 h 11 h 59 Lancement réussi de la tâche universelle « Mainframe Modernization Start Batch » avec l'instanc e de tâche sys_id. <sys id> 3. Accédez aux instances Si vous ne voyez pas l'onglet Instances, cliquez sur la flèche droite pour faire défiler la page vers la droite. 4. Ouvrez le menu contextue l (clic droit) de l'instanc e de tâche dans la liste, choisissez Extraire la sortie, puis choisissez Soumettre dans la section Extraire la sortie 5. Dans la fenêtre Retrieve Output, vous verrez la liste	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	des environnements dans STDOUT.	

Création d'un flux de travail pour plusieurs tâches

Tâche	Description	Compétences requises
Copiez les tâches.	1. Ouvrez le menu contextuel (clic droit) de la tâche dont vous souhaitez créer des copies, puis choisissez Copier. 2. Dans la fenêtre Copy AWS Mainframe Modernization Task, entrez le nouveau nom suivant pour la nouvelle tâche : Mainframe Modernization Start Batch -. RUNAWS2 3. Copiez à nouveau la tâche en utilisant le nom suivant : Mainframe Modernization Start Batch -RUNAWS3. 4. Copiez à nouveau avec la tâche, en utilisant le nom suivant : Mainframe Modernization Start Batch - RUNAWS4. 5. Copiez la tâche une dernière fois en utilisant le nom suivant : Mainframe Modernization Start Batch - FOOBAR.	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
Mettre à jour les tâches.	1. Ouvrez (double-cliquez) la RUNAWS2 tâche Mainframe Modernization Start Batch, remplacez le champ Nom du fichier JCL par et `RUNAWS2.jcl` enregistrez. 2. Ouvrez (double-cliquez) la RUNAWS3 tâche Mainframe Modernization Start Batch, remplacez le champ Nom du fichier JCL par et `RUNAWS3.jcl` enregistrez. 3. Ouvrez (double-cliquez) la RUNAWS4 tâche Mainframe Modernization Start Batch, remplacez le champ Nom du fichier JCL par et `RUNAWS4.jcl` enregistrez. 4. Ouvrez (double-cliquez) la tâche Mainframe Moderniza tion Start Batch - FOOBAR, remplacez le champ Nom du fichier JCL par et enregistrez. *`MISSING.j cl`* Cette tâche échouera car la valeur du nom de fichier JCL est incorrecte.	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
Créez un flux de travail.	1. Accédez à Services, Workflows. 2. Sur le panneau de droite, saisissez Mainframe Modernization Workflow dans le champ Nom, puis enregistrez. 3. Dans le panneau de droite, choisissez Modifier le flux de travail. 4. Dans l'onglet Éditeur de flux de travail, le bouton Ajouter une tâche (+). 5. Dans la fenêtre de recherche de tâches, choisissez Rechercher pour voir toutes les tâches du contrôleur universel. 6. Cliquez sur l'icône située à côté de Mainframe Modernization Start Batch Task, puis faites-la glisser vers un endroit vide dans l'éditeur de flux de travail. 7. Répétez la même action pour les autres tâches de modernisation du mainframe et placez-le s comme indiqué dans la section Informations supplémentaires. 8. Cliquez sur le bouton Connect () et connectez	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	les tâches entre elles. Pour associer une tâche à une autre, cliquez au milieu d'une tâche et faites-la glisser vers la tâche cible. 9. Connectez les tâches comme indiqué dans la section Informations supplémentaires et enregistrez le flux de travail. 10. Cliquez avec le bouton droit sur un emplacement vide dans l'éditeur de flux de travail, choisissez Launch Workflow, puis OK.	

Tâche	Description	Compétences requises
Vérifiez l'état du flux de travail.	1. Dans le menu de gauche, choisissez l'activité 2. Au milieu de la fenêtre, choisissez Démarrer. Vous verrez la liste des instances de tâches dans la liste. 3. Ouvrez (double-cliquez) le flux de travail de modernisation du mainframe dans la liste, ou ouvrez le menu contextuel (clic droit) et choisissez Commandes des tâches du flux de travail, Afficher le flux de travail. Vous verrez les tâches comme indiqué dans la section Informations supplémentaires. La deuxième tâche était censée échouer car vous avez utilisé un fichier JCL manquant.	Administrateur du contrôleur universel

Résoudre les problèmes liés à l'échec des tâches par lots et les réexécuter

Tâche	Description	Compétences requises
Corrigez la tâche qui a échoué et réexécutez-la.	1. Ouvrez (double-cliquez) la tâche qui a échoué pour voir son erreur.	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	2. Deux options s'offrent à vous pour corriger l'échec de la tâche. • Corrigez le nom du fichier JCL et définissez-le sur`F00BAR.jcl` . • Ajoutez le nom de fichier JCL correct au nom de fichier JCL (Temp). Ce champ remplacera le champ Nom du fichier JCL. Pour ce pilote, choisisse z la deuxième option et enregistrez l'instance de tâche. 3. Dans le moniteur de flux de travail, ouvrez le menu contextuel (clic droit) de la tâche ayant échoué, puis choisissez Commandes, Réexécuter. 4. Après cela, toutes les tâches seront terminées avec succès.	

Création de tâches liées à l'application, démarrage et arrêt de l'application

Tâche	Description	Compétences requises
Créez l'action Démarrer l'application.	1. Accédez aux services et aux tâches de modernisa tion du mainframe AWS.	Administrateur d'Universal Controller

Tâche	Description	Compétences requises
	2. Sur le panneau de droite, renseignez les champs obligatoires. • Nom : Application de démarrage de la modernisation du mainframe • Agent : Sélectionnez le seul agent (AGNT0001) Dans la section Détails de la modernisation du mainframe AWS : • Action : démarrer l'application • Informations d'identif ication AWS : si un rôle IAM a été ajouté à l' EC2 instance, vous pouvez laisser ce champ vide. Si vous voulez utiliser `AWSAccessKeyID` et`AWSSecretKey` , sélectionnez les informati ons d'identification que vous avez créées auparavant. • Point final : assurez-vous que le point de terminaison possède la bonne région. L'argument par défaut est `https://m2.us-east-1.amazonaws.com` .	

Tâche	Description	Compétences requises
	• Région : entrez la région du service de modernisation du mainframe AWS. L'argument par défaut est `us-east-1` . • Application : cliquez sur l'icône à côté du champ (), puis choisissez Soumettre dans les choix d'applications d'actualisation. Cela permettra de se connecter au service AWS Mainframe Modernization et de renvoyer la liste des applications. Vous pouvez maintenant sélectionner l'application dans la liste déroulante. Sélectionnez l'application dans laquelle vous souhaitez exécuter le traitement par lots. • Attendre le succès ou l'échec : si cette option est sélectionnée, la tâche attendra que le traitement par lots soit considéré comme un succès ou un échec. • Intervalle d'interrogation : il s'agit de la durée entre chaque interrogation.	

Tâche	Description	Compétences requises
	• Extraire les journaux d'exécution : si cette option est sélection née, les journaux seront extraits automatiquement une fois le traitement par lots terminé. • Format du journal : il s'agit du format des journaux à imprimer. Il peut être au format texte ou JSON. 3. Conservez les valeurs par défaut dans les autres champs et enregistrez la tâche. 4. Copiez maintenant cette tâche et créez-en une pour Stop Application. Changez le nom en Mainframe Moderinization Stop Application, et modifiez l'action en Stop Application.	

Création d'une tâche d'annulation de l'exécution par lots

Tâche	Description	Compétences requises
Créez l'action Annuler le lot.	1. Accédez aux services et aux tâches de modernisa tion du mainframe AWS.	

Tâche	Description	Compétences requises
	2. Sur le panneau de droite, renseignez les champs obligatoires. • Nom : Modernisation du mainframe Annuler l'exécution par lots • Agent : Sélectionnez le seul agent (AGNT0001) Dans la section Détails de la modernisation du mainframe AWS : • Action : Annuler l'exécuti on par lots • Informations d'identif ication AWS : si un rôle IAM a été ajouté à l' EC2 instance, vous pouvez laisser ce champ vide. Si vous voulez utiliser `AWSAccessKeyID` et`AWSSecretKey` , sélectionnez les informati ons d'identification que vous avez créées auparavant. • Point final : assurez-vous que le point de terminaison possède la bonne région. L'argument par défaut est `https://m2.us-east -1.amazonaws.com` .	

Tâche	Description	Compétences requises
	• Région : entrez la région du service de modernisation du mainframe AWS. L'argument par défaut est `us-east-1` . • Application : cliquez sur l'icône à côté du champ (), puis choisissez Soumettre dans les choix d'applications d'actualisation. Cela permettra de se connecter au service AWS Mainframe Modernization et de renvoyer la liste des applications. Vous pouvez maintenant sélectionner l'application dans la liste déroulante. Sélectionnez l'application dans laquelle vous souhaitez exécuter le traitement par lots. • Attendre le succès ou l'échec : si cette option est sélectionnée, la tâche attendra que le traitement par lots soit considéré comme un succès ou un échec. • Intervalle d'interrogation : il s'agit de la durée entre chaque interrogation.	

Tâche	Description	Compétences requises
	• Extraire les journaux d'exécution : si cette option est sélection née, les journaux seront extraits automatiquement une fois le traitement par lots terminé. • Format du journal : il s'agit du format des journaux à imprimer. Il peut être au format texte ou JSON. 3. Conservez les valeurs par défaut dans les autres champs et enregistrez la tâche.	

Ressources connexes

- Contrôleur universel
- Agent universel
- Paramètres LDAP
- Authentification unique SAML
- Outil de conversion Xpress

Informations supplémentaires

Icônes dans l'éditeur de flux de travail

Toutes les tâches connectées

État du flux de travail

Migrez et répliquez des fichiers VSAM vers Amazon RDS ou Amazon MSK à l'aide de Connect from Precisely

Créée par Prachi Khanna (AWS) et Boopathy GOPALSAMY (AWS)

Récapitulatif

Ce modèle explique comment migrer et répliquer des fichiers VSAM (Virtual Storage Access Method) d'un mainframe vers un environnement cible dans le cloud AWS à l'aide de Connect from Precisely. Les environnements cibles couverts par ce modèle incluent Amazon Relational Database Service (Amazon RDS) et Amazon Managed Streaming for Apache Kafka Kafka (Amazon MSK). Connect utilise la capture des données de modification (CDC) pour surveiller en permanence les mises à jour de vos fichiers VSAM sources, puis transférer ces mises à jour vers un ou plusieurs de vos environnements cibles AWS. Vous pouvez utiliser ce modèle pour atteindre vos objectifs de modernisation des applications ou d'analyse de données. Par exemple, vous pouvez utiliser Connect pour migrer vos fichiers d'application VSAM vers le cloud AWS avec une faible latence, ou migrer vos données VSAM vers un entrepôt de données ou un lac de données AWS pour des analyses capables de tolérer des latences de synchronisation supérieures à celles requises pour la modernisation des applications.

Conditions préalables et limitations

Prérequis

- IBM z/OS V2R1 ou version ultérieure
- Serveur de transactions CICS pour z/OS (CICS TS) V5.1 ou version ultérieure (capture de données CICS/VSAM)
- IBM MQ 8.0 ou version ultérieure
- Conformité aux exigences de sécurité z/OS (par exemple, autorisation APF pour les bibliothèques de SQData charge)
- Les journaux de restauration VSAM sont activés
- (Facultatif) Version de restauration CICS VSAM (CICS VR) pour capturer automatiquement les journaux CDC
- Un compte AWS actif
- Un Amazon Virtual Private Cloud (VPC) doté d'un sous-réseau accessible par votre ancienne plateforme

- Une licence VSAM Connect de Precisely

Limites

- Connect ne prend pas en charge la création automatique de tables cibles sur la base de schémas ou de cahiers VSAM source. Vous devez définir la structure de table cible pour la première fois.
- Pour les cibles autres que le streaming telles qu'Amazon RDS, vous devez spécifier le mappage source de conversion en cible dans le script de configuration Apply Engine.
- Les fonctions de journalisation, de surveillance et d'alerte sont mises en œuvre par le biais de composants externes (tels qu'Amazon CloudWatch) APIs et nécessitent des composants externes pour être pleinement opérationnelles.

Versions du produit

- SQData 40134 pour z/OS
- SQData 4.0.43 pour Amazon Linux Amazon Machine Image (AMI) sur Amazon Elastic Compute Cloud (Amazon) EC2

Architecture

Pile technologique source

- Langage de contrôle des tâches (JCL)
- Shell z/OS Unix et outil de productivité du système interactif (ISPF)
- Utilitaires VSAM (IDCAMS)

Pile technologique cible

- Amazon EC2
- Amazon MSK
- Amazon RDS
- Amazon VPC

Architecture cible

Migration de fichiers VSAM vers Amazon RDS

Le schéma suivant montre comment migrer des fichiers VSAM vers une base de données relationnelle, telle qu'Amazon RDS, en temps réel ou presque en temps réel en utilisant l'agent/éditeur CDC dans l'environnement source (mainframe sur site) et le moteur Apply dans l'environnement cible (AWS Cloud).

Le diagramme montre le flux de travail par lots suivant :

1. Connect capture les modifications apportées à un fichier en comparant les fichiers VSAM à partir de fichiers de sauvegarde pour identifier les modifications, puis envoie les modifications au flux de journal.
2. L'éditeur consomme les données du flux de journal du système.
3. L'éditeur communique les modifications des données capturées à un moteur cible via TCP/IP. Le Controller Daemon authentifie les communications entre les environnements source et cible.
4. Le moteur d'application de l'environnement cible reçoit les modifications de l'agent Publisher et les applique à une base de données relationnelle ou non relationnelle.

Le diagramme montre le flux de travail en ligne suivant :

1. Connect capture les modifications apportées au fichier en ligne à l'aide d'une réplication de journal, puis diffuse les modifications capturées dans un flux de journal.
2. L'éditeur consomme les données du flux de journal du système.
3. L'éditeur communique les modifications des données capturées au moteur cible via TCP/IP. Le Controller Daemon authentifie les communications entre les environnements source et cible.
4. Le moteur d'application de l'environnement cible reçoit les modifications de l'agent Publisher, puis les applique à une base de données relationnelle ou non relationnelle.

Migration de fichiers VSAM vers Amazon MSK

Le schéma suivant montre comment diffuser des structures de données VSAM d'un mainframe vers Amazon MSK en mode haute performance et comment générer automatiquement des conversions de schéma JSON ou AVRO qui s'intègrent à Amazon MSK.

Le diagramme montre le flux de travail par lots suivant :

1. Connect capture les modifications apportées à un fichier à l'aide de CICS VR ou en comparant les fichiers VSAM des fichiers de sauvegarde pour identifier les modifications. Les modifications capturées sont envoyées au flux de données.
2. L'éditeur consomme les données du flux de journal du système.
3. L'éditeur communique les modifications des données capturées au moteur cible via TCP/IP. Le Controller Daemon authentifie les communications entre les environnements source et cible.
4. Le Replicator Engine qui fonctionne en mode de traitement parallèle divise les données dans une unité de cache de travail.
5. Les threads de travail capturent les données du cache.
6. Les données sont publiées sur les rubriques Amazon MSK à partir des threads de travail.
7. Les utilisateurs appliquent les modifications depuis Amazon MSK à des cibles telles qu'Amazon DynamoDB, Amazon Simple Storage Service (Amazon S3) OpenSearch ou Amazon Service à l'aide de connecteurs.

Le diagramme montre le flux de travail en ligne suivant :

1. Les modifications apportées au fichier en ligne sont enregistrées à l'aide d'une copie du journal. Les modifications capturées sont diffusées dans le flux journal.
2. L'éditeur consomme les données du flux de journal du système.
3. L'éditeur communique les modifications des données capturées au moteur cible via TCP/IP. Le Controller Daemon authentifie les communications entre les environnements source et cible.
4. Le Replicator Engine qui fonctionne en mode de traitement parallèle divise les données dans une unité de cache de travail.
5. Les threads de travail capturent les données du cache.
6. Les données sont publiées sur les rubriques Amazon MSK à partir des threads de travail.
7. Les utilisateurs appliquent les modifications depuis Amazon MSK à des cibles telles que DynamoDB, Amazon S3 ou Service à l'aide de OpenSearch connecteurs.

Outils

- Amazon Managed Streaming for Apache Kafka (Amazon MSK) est un service entièrement géré qui vous permet de créer et d'exécuter des applications utilisant Apache Kafka pour traiter les données de streaming.

- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.

Épopées

Préparation de l'environnement source (mainframe)

Tâche	Description	Compétences requises
Installez Connect CDC 4.1.	1. Contactez l'équipe de Support de Precisely pour obtenir une licence et des packages d'installation. 2. Utilisez un exemple JCLs pour installer Connect CDC 4.1. Pour obtenir des instructions, consultez la section Installer Connect CDC (SQData) à l'aide de JCL dans la documentation Precisely. 3. Exécutez la `SETPROG APF` commande pour autoriser les bibliothèques de chargement Connect SQData.v4NNN.LoadLib.	Développeur/administrateur du mainframe IBM
Configurez le répertoire zFS.	Pour configurer un répertoire ZFS, suivez les instructions des répertoires de variables ZfS dans la documentation Precisely. **Note** Controller Daemon et système de fichiers	Développeur/administrateur du mainframe IBM

Tâche	Description	Compétences requises
	Capture/Publisher agent configurations are stored in the z/OS UNIX Systems Services (appelé ZFS). Les agents Controller Daemon, Capture, Storage et Publisher nécessitent une structure de répertoire ZFS prédéfinie pour stocker un petit nombre de fichiers.	
Configurez les ports TCP/IP.	Pour configurer les ports TCP/IP, suivez les instructions des ports TCP/IP de la documentation Precisely. **Note** Le Controller Daemon nécessite des ports TCP/IP sur les systèmes sources. Les ports sont référencés par les moteurs des systèmes cibles (où les données de modification capturées sont traitées).	Développeur/administrateur du mainframe IBM

Tâche	Description	Compétences requises
Créez un flux de log z/OS.	Pour créer un flux de journal z/OS, suivez les instructions de la section Créer des flux de journaux de système z/OS dans la documentation de Precisely. **Note** Connect utilise le flux de données pour capturer et diffuser des données entre votre environnement source et votre environnement cible pendant la migration. Pour un exemple de JCL qui crée un système z/OS LogStream, voir Create z/OS system LogStreams dans la documentation Precisely.	Développeur de mainframe IBM
Identifiez et autorisez IDs les utilisateurs de ZFS et les tâches démarrées.	Utilisez RACF pour accorder l'accès au système de fichiers OMVS ZfS. Pour un exemple de JCL, voir Identifier et autoriser un utilisateur ZFS et une tâche démarrée IDs dans la documentation Precisely.	Développeur/administrateur du mainframe IBM

Tâche	Description	Compétences requises
Générez les clés publiques/privées z/OS et le fichier clé autorisé.	Exécutez le JCL pour générer la paire de clés. Pour un exemple, voir Exemple de paire de clés dans la section Informations supplémentaires de ce modèle. Pour obtenir des instructions, consultez la section Générer des clés publiques et privées z/OS et un fichier de clé autorisé dans la documenta tion de Precisely.	Développeur/administrateur du mainframe IBM

Activez le CICS VSAM Log Replicate et attachez-le au flux de journal.	Exécutez le script JCL suivant :
	
	`//STEP1 EXEC PGM=IDCAM S`
	`//SYSPRINT DD SYSOUT=*`
	`//SYSIN DD *`
	`ALTER SQDATA.CI CS.FILEA -`
	`LOGSTREAMID(SQDATA .VSAMCDC.LOG1) -`
	`LOGREPLICATE`
		Développeur/administrateur du mainframe IBM

Tâche	Description	Compétences requises

Activez le journal de restauration de fichiers VSAM via un FCT.	Modifiez la table de contrôle des fichiers (FCT) pour refléter les modifications de paramètres suivantes :
	`Configure FCT Parms`
	`  CEDA ALT FILE(name) GROUP(groupname)`
	`  DSNAME(data set name)`
	`  RECOVERY(NONE|BACKOUTONLY|ALL)`
	`  FWDRECOVLOG(NO|1-99)`
	`  BACKUPTYPE(STATIC|DYNAMIC)`
	`  RECOVERY PARAMETERS`
	`  RECOVery : None | Backoutonly | All`
	`  Fwdrecovlog : No | 1-99`
	`  BAckuptype : Static | Dynamic`
		Développeur/administrateur du mainframe IBM

Configurez le CDCz journal pour l'agent Publisher.	1. Créez le fichier CAB de CDCz Log Publisher. 2. Chiffrez les données publiées. 3. Préparez le JCL CDCz Log Publisher Runtime.	Développeur/administrateur du mainframe IBM

Tâche	Description	Compétences requises
Activez le démon Controller.	1. Ouvrez le panneau ISPF et exécutez la commande suivante pour ouvrir le menu Precisely : `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Pour configurer le Controller Daemon, choisissez l'option 2 dans le menu.	Développeur/administrateur du mainframe IBM
Activez l'éditeur.	1. Ouvrez le panneau ISPF et exécutez la commande suivante pour ouvrir le menu Precisely : `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Pour configurer l'éditeur, choisissez l'option 3 dans le menu et I pour insérer.	Développeur/administrateur du mainframe IBM

Tâche	Description	Compétences requises
Activez le flux de log.	1. Ouvrez le panneau ISPF et exécutez la commande suivante pour ouvrir le menu Precisely : `EXEC 'SQDATA.V4nnnnn.ISPFLIB(SQDC$STA)' 'SQDATA.V4nnnnn'` 2. Pour configurer le logstream, choisissez l'option 4 dans le menu et I pour insérer. Entrez ensuite le nom du flux de journal créé lors des étapes précédentes.	Développeur/administrateur du mainframe IBM

Préparation de l'environnement cible (AWS)

Tâche	Description	Compétences requises
Installez Precisely sur une EC2 instance.	Pour installer Connect from Precisely sur l'AMI Amazon Linux pour Amazon EC2, suivez les instructions de la section Installer Connect CDC (SQData) sous UNIX dans la documentation de Precisely.	AWS général
Ouvrez les ports TCP/IP.	Pour modifier le groupe de sécurité afin d'inclure les ports Controller Daemon pour l'accès entrant et sortant, suivez les instructions TCP/IP de la documentation Precisely.	AWS général

Tâche	Description	Compétences requises
Créez des répertoires de fichiers.	Pour créer des répertoires de fichiers, suivez les instructions de la section Préparer l'environnement d'application cible dans la documentation Precisely.	AWS général

Créez le fichier de configuration Apply Engine.	Créez le fichier de configuration d'Apply Engine dans le répertoire de travail d'Apply Engine. L'exemple de fichier de configuration suivant montre Apache Kafka comme cible :
	`builtin.features=SASL_SCRAM`
	`security.protocol=SASL_SSL`
	`sasl.mechanism=SCRAM-SHA-512`
	`sasl.username=`
	`sasl.password=`
	`metadata.broker.list=`
	Note
	Pour plus d'informations, consultez la section Sécurité dans la documentation d'Apache Kafka.
		AWS général

Tâche	Description	Compétences requises
Créez des scripts pour le traitement d'Apply Engine.	Créez les scripts permettant au moteur Apply de traiter les données sources et de les répliquer vers la cible. Pour plus d'informations, consultez la section Création d'un script d'application du moteur dans la documentation Precisely.	AWS général
Exécutez les scripts.	Utilisez les `SQDENG` commandes `SQDPARSE` et pour exécuter le script. Pour plus d'informations, consultez la section Analyse d'un script pour zOS dans la documentation Precisely.	AWS général

Valider l'environnement

Tâche	Description	Compétences requises
Validez la liste des fichiers VSAM et des tables cibles pour le traitement par le CDC.	1. Validez les fichiers VSAM, y compris les journaux de réplication, les journaux de restauration, les paramètres FCT et le flux de journal. 2. Validez les tables de base de données cibles, en indiquant notamment si les tables sont créées conformément à la définition de schéma requise, à l'accès aux tables et à d'autres critères.	AWS général, Mainframe

Tâche	Description	Compétences requises
Vérifiez que le SQData produit Connect CDC est lié.	Exécutez une tâche de test et vérifiez que le code de retour de cette tâche est 0 (Réussite). **Note** Les messages d'état du moteur Connect CDC SQData Apply doivent afficher des messages de connexion active.	AWS général, Mainframe

Exécuter et valider des scénarios de test (Batch)

Tâche	Description	Compétences requises
Exécutez le traitement par lots sur le mainframe.	Exécutez la tâche d'applica tion par lots à l'aide d'une JCL modifiée. Incluez dans la JCL modifiée les étapes suivantes : 1. Effectuez une sauvegarde des fichiers de données. 2. Comparez le fichier de sauvegarde avec les fichiers de données modifiés, générez le fichier delta, puis notez le nombre d'enregistrements delta indiqué dans les messages. 3. Transférez le fichier delta vers le flux de log z/OS.	AWS général, Mainframe

Tâche	Description	Compétences requises
	4. Exécutez le JCL. Pour un exemple de JCL, voir Prepare file compare capture JCL dans la documentation Precisely.	
Vérifiez le flux de données.	Consultez le flux journal pour vérifier que vous pouvez voir les données de modification relatives à la tâche par lots terminée sur le mainframe.	AWS général, Mainframe
Validez les dénombrements pour les modifications du delta source et pour la table cible.	Pour confirmer que les enregistrements sont comptabilisés, procédez comme suit : 1. Recueillez le nombre de deltas source à partir des messages JCL par lots. 2. Surveillez le moteur d'application pour connaître le nombre d'enregis trements insérés, mis à jour ou supprimés dans le fichier VSAM par niveau d'enregis trement. 3. Interrogez la table cible pour connaître le nombre d'enregistrements. 4. Comparez et comptez tous les différents nombres d'enregistrements.	AWS général, Mainframe

Exécuter et valider des scénarios de test (en ligne)

Tâche	Description	Compétences requises
Exécutez la transaction en ligne dans une région CICS.	1. Exécutez la transaction en ligne pour valider le scénario de test. 2. Validez le code d'exécution de la transaction (RC=0 — Success).	Développeur de mainframe IBM
Vérifiez le flux de données.	Vérifiez que le flux journal contient des modifications spécifiques des niveaux d'enregistrement.	Développeur de mainframe AWS
Validez le nombre dans la base de données cible.	Surveillez le moteur d'application pour connaître le nombre record de niveaux.	Précisément, Linux
Validez le nombre d'enregistrements et les enregistrements de données dans la base de données cible.	Interrogez la base de données cible pour valider le nombre d'enregistrements et les enregistrements de données.	AWS général

Ressources connexes

- VSAM z/OS (documentation précise)
- Appliquer le moteur (documentation précise)
- Moteur Replicator (documentation précise)
- Le flux de log (documentation IBM)

Informations supplémentaires

Exemple de fichier de configuration

Voici un exemple de fichier de configuration pour un flux de journal dont l'environnement source est un mainframe et l'environnement cible est Amazon MSK :

```
 -- JOBNAME -- PASS THE SUBSCRIBER NAME
 -- REPORT  progress report will be produced after "n" (number) of Source records
processed.

 JOBNAME VSMTOKFK;
 --REPORT EVERY 100;
 -- Change Op has been ‘I’ for insert, ‘D’ for delete , and ‘R’ for Replace. For RDS
it is 'U' for update
 -- Character Encoding on z/OS is Code Page 1047, on Linux and UNIX it is Code Page
819 and on Windows, Code Page 1252
 OPTIONS
 CDCOP('I', 'U', 'D'),
 PSEUDO NULL = NO,
 USE AVRO COMPATIBLE NAMES,
 APPLICATION ENCODING SCHEME = 1208;

 --       SOURCE DESCRIPTIONS

 BEGIN GROUP VSAM_SRC;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       TARGET DESCRIPTIONS

 BEGIN GROUP VSAM_TGT;
 DESCRIPTION COBOL ../copybk/ACCOUNT AS account_file;
 END GROUP;

 --       SOURCE DATASTORE (IP & Publisher name)

 DATASTORE cdc://10.81.148.4:2626/vsmcdct/VSMTOKFK
 OF VSAMCDC
 AS CDCIN
 DESCRIBED BY GROUP VSAM_SRC ACCEPT ALL;

 --       TARGET DATASTORE(s) - Kafka and topic name

 DATASTORE 'kafka:///MSKTutorialTopic/key'
 OF JSON
```

```
  AS CDCOUT
  DESCRIBED BY GROUP VSAM_TGT FOR INSERT;

  --       MAIN SECTION

  PROCESS INTO
  CDCOUT
  SELECT
  {
  SETURL(CDCOUT, 'kafka:///MSKTutorialTopic/key')
  REMAP(CDCIN, account_file, GET_RAW_RECORD(CDCIN, AFTER), GET_RAW_RECORD(CDCIN,
 BEFORE))
  REPLICATE(CDCOUT, account_file)
  }
  FROM CDCIN;
```

Exemple de paire de clés

Voici un exemple de la façon d'exécuter la JCL pour générer la paire de clés :

```
//SQDUTIL EXEC PGM=SQDUTIL //SQDPUBL DD DSN=&USER..NACL.PUBLIC, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPKEY DD DSN=&USER..NACL.PRIVATE, //
 DCB=(RECFM=FB,LRECL=80,BLKSIZE=21200), // DISP=(,CATLG,DELETE),UNIT=SYSDA, //
 SPACE=(TRK,(1,1)) //SQDPARMS DD  keygen //SYSPRINT DD SYSOUT= //SYSOUT DD SYSOUT=* //
SQDLOG DD SYSOUT=* //*SQDLOG8 DD DUMMY
```

Modernisez la gestion des sorties du mainframe AWS en utilisant Rocket Enterprise Server et PageCenter LRS X

Créée par Shubham Roy (AWS), Abraham Rondon (Micro Focus) et Guy Tucker (Levi, Ray and Shoup Inc)

Récapitulatif

En modernisant la gestion des sorties de votre mainframe, vous pouvez réaliser des économies, atténuer la dette technique liée à la maintenance des systèmes existants et améliorer la résilience et l'agilité grâce aux technologies natives du DevOps cloud d'Amazon Web Services (AWS). Ce modèle vous montre comment moderniser les charges de travail de gestion des sorties critiques de votre mainframe sur le cloud AWS. Le modèle utilise Rocket Enterprise Server comme environnement d'exécution pour une application mainframe modernisée, avec Levi, Ray & Shoup, Inc. (LRS) VPSX/MFI (Micro Focus Interface) comme serveur d'impression et LRS X comme serveur d'archives. PageCenter LRS PageCenter X fournit des solutions de gestion des sorties pour la visualisation, l'indexation, la recherche, l'archivage et la sécurisation de l'accès aux résultats commerciaux.

Le modèle est basé sur l'approche de modernisation du mainframe replateforme. Les applications mainframe sont migrées par AWS Mainframe Modernization sur Amazon Elastic Compute Cloud (Amazon). EC2 Les charges de travail de gestion des sorties du mainframe sont migrées vers Amazon EC2, et une base de données mainframe, telle qu'IBM Db2 for z/OS, est migrée vers Amazon Relational Database Service (Amazon RDS). Le serveur d'intégration d'annuaire LRS (LRS/DIS) fonctionne avec AWS Directory Service pour Microsoft Active Directory pour l'authentification et l'autorisation des flux de travail de gestion des sorties.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Charge de travail de gestion des sorties du mainframe.
- Connaissances de base sur la façon de reconstruire et de fournir une application mainframe qui s'exécute sur Rocket Enterprise Server. Pour plus d'informations, consultez la fiche technique du serveur Rocket Enterprise dans la documentation du logiciel Rocket.
- Connaissances de base des solutions et concepts d'impression cloud LRS. Pour plus d'informations, consultez la section Modernisation des sorties dans la documentation LRS.

- Logiciel et licence Rocket Enterprise Server. Pour plus d'informations, contactez Rocket Software.
- VPSX/MFI, LRS PageCenterX, LRS/Queue, and LRS/DISLogiciels et licences LRS. Pour plus d'informations, contactez LRS. Vous devez fournir les noms d'hôte des EC2 instances sur lesquelles les produits LRS seront installés.

> **Note**
>
> Pour plus d'informations sur les considérations relatives à la configuration des charges de travail de gestion des sorties du mainframe, consultez la section Considérations de la section Informations supplémentaires de ce modèle.

Versions du produit

- Serveur Rocket Enterprise 10.0
- LRS VPSX/MFI
- LRS PageCenter X V1R3 ou version ultérieure

Architecture

Pile technologique source

- Système d'exploitation — IBM z/OS
- Langage de programmation — Langage orienté métier (COBOL), langage de contrôle des tâches (JCL) et système de contrôle des informations clients (CICS)
- Base de données : IBM Db2 pour z/OS, base de données IBM Information Management System (IMS) et méthode d'accès au stockage virtuel (VSAM)
- Sécurité : Resource Access Control Facility (RACF), CA Top Secret pour z/OS et Access Control Facility 2 () ACF2
- Solutions d'impression et d'archivage : produits de sortie et d'impression IBM mainframe z/OS (IBM Infoprint Server pour z/OS, LRS et CA Deliver) et solutions d'archivage (CA Deliver, ASG Mobius ou CA Bundle)

Architecture de la source

Le schéma suivant montre une architecture d'état actuelle typique pour une charge de travail de gestion des sorties d'un mainframe.

Le schéma suivant illustre le flux de travail suivant :

1. Les utilisateurs effectuent des transactions commerciales sur un système d'engagement (SoE) basé sur une application IBM CICS écrite en COBOL.
2. Le SoE invoque le service mainframe, qui enregistre les données des transactions commerciales dans une base de données system-of-records (SoR) telle qu'IBM Db2 for z/OS.
3. Le SoR conserve les données commerciales du SoE.
4. Le planificateur de tâches par lots lance une tâche par lots pour générer une sortie d'impression.
5. Le traitement par lots extrait les données de la base de données. Il met en forme les données en fonction des besoins de l'entreprise, puis il génère des résultats commerciaux tels que des relevés de facturation, des cartes d'identité ou des relevés de prêt. Enfin, le traitement par lots achemine la sortie vers la gestion des sorties pour le formatage, la publication et le stockage de la sortie en fonction des exigences de l'entreprise.
6. La gestion des sorties reçoit le résultat du traitement par lots. La gestion des sorties indexe, organise et publie la sortie vers une destination spécifiée dans le système de gestion des sorties, telle que les solutions LRS PageCenter X (comme illustré dans ce modèle) ou CA View.
7. Les utilisateurs peuvent afficher, rechercher et récupérer le résultat.

Pile technologique cible

- Système d'exploitation — Windows Server exécuté sur Amazon EC2
- Calcul — Amazon EC2
- Stockage — Amazon Elastic Block Store (Amazon EBS) et FSx Amazon pour Windows File Server
- Langage de programmation : COBOL, JCL et CICS
- Base de données — Amazon RDS
- Sécurité — Microsoft AD géré par AWS
- Impression et archivage : solution d'impression LRS (VPSX) et d'archivage (PageCenterX) sur AWS
- Environnement d'exécution mainframe — Rocket Enterprise Server

Architecture cible

Le schéma suivant montre l'architecture d'une charge de travail de gestion des sorties du mainframe déployée dans le cloud AWS.

Le schéma suivant illustre le flux de travail suivant :

1. Le planificateur de tâches par lots lance une tâche par lots pour créer des résultats, tels que des relevés de facturation, des cartes d'identité ou des relevés de prêt.
2. Le traitement par lots du mainframe (replatformé sur Amazon EC2) utilise le runtime Rocket Enterprise Server pour extraire les données de la base de données de l'application, appliquer une logique métier aux données et les formater. Il envoie ensuite les données vers une destination de sortie à l'aide du module de sortie d'imprimante Rocket Software (documentation OpenText Micro Focus).
3. La base de données de l'application (un SoR qui s'exécute sur Amazon RDS) conserve les données pour l'impression.
4. L'agent de VPSX/MFI printing solution is deployed on Amazon EC2, and its operational data is stored in Amazon EBS. LRS VPSX/MFI uses the TCP/IP-based LRS/Queue transmission LRS pour collecter les données de sortie via l'API JES Print Exit de Rocket Software.

   LRS VPSX/MFI effectue le prétraitement des données, tel que la traduction EBCDIC vers ASCII. Il effectue également des tâches plus complexes, notamment la conversion de flux de données exclusifs aux ordinateurs centraux tels que IBM Advanced Function Presentation (AFP) et Xerox Line Conditioned Data Stream (LCDS) en flux de données de visualisation et d'impression plus courants tels que le langage de commande d'imprimante (PCL) et le PDF.

   Pendant la période de maintenance de LRS PageCenter X, LRS échange VPSX/MFI persists the output queue and serves as backup for the output queue. LRS VPSX/MFI connects and sends output to LRS PageCenterX by using the LRS/Queue protocol. LRS/Queue à la fois l'état de préparation et l'achèvement des tâches afin de garantir le transfert des données.

   Remarques :

   Pour plus d'informations sur les données d'impression transmises de Rocket Software Print Exit aux mécanismes de traitement par lots du mainframe pris en LRS/Queue and LRS VPSX/MFI charge, voir Capture des données d'impression dans la section Informations supplémentaires.

Le LRS VPSX/MFI peut effectuer des contrôles de santé au niveau du parc d'imprimantes. Pour plus d'informations, consultez la section Contrôles de santé du parc d'imprimantes dans la section Informations supplémentaires de ce modèle.

5. La solution de gestion des sorties LRS PageCenter X est déployée sur Amazon EC2 et ses données opérationnelles sont stockées sur Amazon FSx pour Windows File Server. LRS PageCenter X fournit un système central de gestion des rapports contenant tous les fichiers importés dans LRS PageCenter X et permettant à tous les utilisateurs d'accéder aux fichiers. Les utilisateurs peuvent consulter le contenu d'un fichier spécifique ou effectuer des recherches dans plusieurs fichiers pour trouver des critères correspondants.

   Le serveur d'applications LRS/NetX component is a multi-threaded web application server that provides a common runtime environment for the LRS PageCenterX application and other LRS applications. The LRS/Web Connect component is installed on your web server and provides a connector from the web server to the LRS/NetX Web.
6. LRS PageCenter X fournit un espace de stockage pour les objets du système de fichiers. Les données opérationnelles de LRS PageCenter X sont stockées dans le serveur de fichiers Amazon FSx pour Windows.
7. L'authentification et l'autorisation de gestion des sorties sont effectuées par AWS Managed Microsoft AD avec LRS/DIS.

> **Note**
>
> La solution cible ne nécessite généralement pas de modifications de l'application pour s'adapter aux langages de formatage du mainframe, tels qu'IBM AFP ou Xerox LCDS.

Architecture de l'infrastructure AWS

Le schéma suivant montre une architecture d'infrastructure AWS hautement disponible et sécurisée pour une charge de travail de gestion des sorties sur mainframe.

Le schéma suivant illustre le flux de travail suivant :

1. Le planificateur de lots lance le processus de traitement par lots et est déployé sur Amazon EC2 dans plusieurs zones de disponibilité pour une haute disponibilité (HA).

> **Note**
>
> Ce modèle ne couvre pas la mise en œuvre du planificateur de lots. Pour plus d'informations sur la mise en œuvre, consultez la documentation du fournisseur de logiciels pour votre planificateur.

2. Le traitement par lots du mainframe (écrit dans un langage de programmation tel que JCL ou COBOL) utilise la logique métier de base pour traiter et générer des documents imprimés, tels que des relevés de facturation, des cartes d'identité et des relevés de prêt. Le traitement par lots est déployé EC2 sur Amazon dans deux zones de disponibilité pour HA. Il utilise l'API Rocket Software Print Exit pour acheminer la sortie d'impression vers LRS VPSX/MFI pour le prétraitement des données.
3. Le serveur d'impression LRS VPSX/MFI est déployé sur Amazon EC2 dans deux zones de disponibilité pour HA (paire redondante active et veille). Il utilise Amazon EBS comme magasin de données opérationnel. Le Network Load Balancer effectue une vérification de l'état des instances LRS VPSX/MFI. EC2 Si une instance active est défectueuse, l'équilibreur de charge achemine le trafic vers les instances en veille active situées dans l'autre zone de disponibilité. Les demandes d'impression sont conservées dans la file d'attente des tâches LRS localement dans chacune des EC2 instances. En cas de panne, une instance défaillante doit être redémarrée avant que les services LRS puissent reprendre le traitement de la demande d'impression.

> **Note**
>
> Le LRS VPSX/MFI peut également effectuer des contrôles de santé au niveau du parc d'imprimantes. Pour plus d'informations, consultez la section Contrôles de santé du parc d'imprimantes dans la section Informations supplémentaires de ce modèle.

4. La gestion des sorties LRS PageCenter X est déployée sur Amazon EC2 dans deux zones de disponibilité pour HA (paire redondante active et veille). Il utilise le serveur de fichiers Amazon FSx pour Windows comme magasin de données opérationnel. Si une instance active est défectueuse, l'équilibreur de charge effectue une vérification de l'état des instances LRS PageCenter X et achemine le trafic vers les EC2 instances de secours situées dans l'autre zone de disponibilité.
5. Un Network Load Balancer fournit un nom DNS pour intégrer le serveur LRS VPSX/MFI à LRS X. PageCenter

> **Note**
>
> Le LRS PageCenter X prend en charge un équilibreur de charge de couche 4.

6. LRS PageCenter X utilise le serveur de fichiers Amazon FSx pour Windows comme magasin de données opérationnel déployé sur deux zones de disponibilité pour HA. LRS PageCenter X ne comprend que les fichiers qui se trouvent dans le partage de fichiers, et non dans une base de données externe.
7. AWS Managed Microsoft AD est utilisé avec LRS/DIS pour effectuer l'authentification et l'autorisation du flux de travail de gestion des sorties. Pour plus d'informations, voir Authentification et autorisation de sortie d'impression dans la section Informations supplémentaires.

Outils

Services AWS

- AWS Directory Service pour Microsoft Active Directory permet à vos charges de travail sensibles aux annuaires et à vos ressources AWS d'utiliser Microsoft Active Directory dans le cloud AWS.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Elastic Load Balancing (ELB) répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les EC2 instances Amazon, les conteneurs et les adresses IP dans une ou plusieurs zones de disponibilité. Ce modèle utilise un Network Load Balancer.
- Amazon FSx fournit des systèmes de fichiers qui prennent en charge les protocoles de connectivité standard du secteur et offrent une disponibilité et une réplication élevées dans les régions AWS. Ce modèle utilise le serveur de fichiers Amazon FSx pour Windows.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.

Autres outils

- Le logiciel LRS PageCenter X fournit une solution évolutive de gestion du contenu des documents et des rapports qui aide les utilisateurs à tirer le meilleur parti des informations grâce à des fonctionnalités automatisées d'indexation, de chiffrement et de recherche avancée.
- LRS VPSX/MFI (Micro Focus Interface), développé conjointement par LRS et Rocket Software, capture le résultat d'une bobine JES de Rocket Software et le transmet de manière fiable à une destination d'impression spécifiée.
- LRS/Queue is a transmission agent that's TCP/IP based. LRS VPSX/MFI uses LRS/Queuepour collecter ou capturer des données d'impression via l'interface de programmation JES Print Exit de Rocket Software.
- Le serveur d'intégration d'annuaire LRS (LRS/DIS) est utilisé pour l'authentification et l'autorisation pendant le flux de travail d'impression.
- Rocket Enterprise Server est un environnement de déploiement d'applications pour les applications mainframe. Il fournit l'environnement d'exécution pour les applications mainframe migrées ou créées à l'aide de n'importe quelle version de Rocket Enterprise Developer.

Épopées

Configuration du runtime Rocket et déploiement d'une application batch pour mainframe

Tâche	Description	Compétences requises
Configurez le runtime et déployez une application de démonstration.	Pour configurer Rocket Enterprise Server sur Amazon EC2 et déployer l'application de BankDemo démonstration du logiciel Rocket, suivez les instructions du guide de l'utilisateur d'AWS Mainframe Modernization. L' BankDemo application est une application batch sur ordinateur central qui crée puis lance une sortie d'impression.	Architecte du cloud

Configurer un serveur d'impression LRS sur Amazon EC2

Tâche	Description	Compétences requises
Créez une instance Amazon EC2 Windows.	Pour lancer une instance Amazon EC2 Windows, suivez les instructions de la section Lancer une EC2 instance Amazon dans la EC2 documentation Amazon. Utilisez le même nom d'hôte que celui que vous avez utilisé pour votre licence de produit LRS. Votre instance doit répondre aux exigences matérielles et logicielles suivantes pour LRS VPSX/MFI : • Processeur : double cœur • RAM — 16 GO • Disque dur : 500 Go • EC2 Instance minimale : `m5.xlarge` • Système d'exploitation — Windows • Logiciel : Internet Informati on Services (IIS) ou Apache **Note** Les exigences matérielles et logiciell es ci-dessus sont destinées à un petit	Architecte du cloud

Tâche	Description	Compétences requises
	parc d'imprimantes (environ 500 à 1 000). Pour connaître toutes les exigences, consultez vos contacts LRS et AWS. 1. Lorsque vous créez votre instance Windows, vérifiez que le EC2 nom d'hôte est le même que celui utilisé pour la licence du produit LRS. 2. Connectez-vous à votre EC2 instance en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. 3. Dans le menu Démarrer de Windows, recherchez et ouvrez le Gestionnaire de serveur. 4. Dans le Gestionnaire de serveur, choisissez Tableau de bord, Démarrage rapide, Ajouter des rôles et des fonctionnalités, puis choisissez Rôles de serveur. 5. Dans Rôles de serveur, choisissez WebServer (IIS),	

Tâche	Description	Compétences requises
	puis choisissez Développement d'applications. 6. Dans Développement d'applications, cochez la case CGI. 7. Pour installer CGI, suivez les instructions de l'assistant d'ajout de rôles et de fonctionnalités de Windows Server Manager. 8. Ouvrez le port 5500 dans le pare-feu Windows de l' EC2 instance pour la communication LRS/Queue.	

Tâche	Description	Compétences requises
Installez LRS VPSX/MFI sur l'instance. EC2	1. Connectez-vous à votre EC2 instance. 2. Ouvrez le lien vers la page de téléchargement du produit contenu dans le message électronique LRS que vous auriez dû recevoir. **Note** Les produits LRS sont distribués par transfert électroni que de fichiers (EFT). 3. Téléchargez LRS VPSX/ MFI et décompressez le fichier (dossier par défaut :). `c:\LRS` 4. Pour installer LRS VPSX/ MFI, lancez le programme d'installation du produit LRS à partir du dossier décompressé. 5. Dans le menu Sélectionner les fonctionnalités, sélection nez VPSX® Server, puis cliquez sur Suivant pour démarrer le processus d'installation. Vous recevrez un message de confirmat	Architecte du cloud

Tâche	Description	Compétences requises
	ion lorsque l'installation sera terminée.	
Installez LRS/Queue.	1. Connectez-vous à votre EC2 instance de serveur Rocket Enterprise. 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans le message électronique LRS que vous devriez avoir reçu, téléchargez LRS/Queue , puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS pour installer LRS/Queue. 4. Suivez les instructions du programme d'installation du produit LRS pour terminer le processus d'installation.	Architecte du cloud

Tâche	Description	Compétences requises
Installez LRS/DIS.	Il LRS/DIS product often is included in LRS VPSX installation. However, if LRS/DIS n'a pas été installé avec LRS VPSX. Procédez comme suit pour l'installer : 1. Connectez-vous à votre instance LRS EC2 VPSX/MFI. 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans le message électronique LRS que vous devriez avoir reçu, téléchargez LRS/DIS, puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS. 4. Dans le programme d'installation du produit LRS, développez LRS Misc Tools, sélectionnez LRS DIS, puis Next. 5. Suivez le reste des instructions du programme d'installation du produit LRS pour terminer le processus d'installation.	Architecte du cloud

Tâche	Description	Compétences requises
Créer un groupe cible.	Créez un groupe cible en suivant les instructions de la section Créer un groupe cible pour votre Network Load Balancer. Lorsque vous créez le groupe cible, enregistrez l'instance LRS VPSX/MFI EC2 en tant que cible : 1. Sur la page Spécifier les détails du groupe, pour Choisir un type de cible, sélectionnez Instances. 2. Pour Protocole, choisissez TCP. 3. Pour Port, choisissez 5500. 4. Sur la page Enregistrer les cibles, dans la section Instances disponibles, sélectionnez l'instance LRS EC2 VPSX/MFI.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un Network Load Balancer.	Pour créer le Network Load Balancer, suivez les instructions de la documentation d'Elastic Load Balancing. Votre Network Load Balancer achemine le trafic depuis Rocket Enterprise Server vers l'instance LRS VPSX/MFI. EC2 Lorsque vous créez le Network Load Balancer, choisissez les valeurs suivantes sur la page Listeners and Routing : 1. Pour Protocol (Protocole), choisissez TCP. 2. Pour Port, choisissez 5500. 3. Pour Action par défaut, choisissez Transférer vers pour le groupe cible que vous avez créé précédemment.	Architecte du cloud

Intégrez Rocket Enterprise Server à LRS/Queue and LRS VPSX/MFI

Tâche	Description	Compétences requises
Configurez le serveur Rocket Enterprise pour l'intégration de LRS/Queue.	1. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de	Architecte du cloud

Tâche	Description	Compétences requises
	la EC2 documentation Amazon. 2. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration de Rocket Enterprise Server. 3. Dans la barre de menu, choisissez NATIVE. 4. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO pour votre région Enterprise Server. 5. Depuis Général dans le volet de navigation de gauche, faites défiler la page vers le bas jusqu'à la section Supplémentaire pour configurer les variables d'environnement (`LRSQ_ADDRESS` ,`LRSQ_PORT` ,`LRSQ_COMMAND`) afin qu'elles pointent vers LRSQ. • Pour LRSQ_ADDRESS, entrez l'adresse IP ou le nom DNS du Network Load Balancer que vous avez créé précédemment.	

Tâche	Description	Compétences requises
	• Pour LRSQ_PORT, entrez VPSX LRSQ Listener Port (5500). • Pour LRSQ_COMMAND, entrez l'emplacement du chemin de l'exécutable LRSQ. **Note** LRS prend actuellement en charge une limite maximale de 50 caractères pour les noms DNS. Si votre nom DNS comporte plus de 50 caractères, vous pouvez utiliser l'adresse IP du Network Load Balancer comme alternative.	

Tâche	Description	Compétences requises
Configurez le serveur Rocket Enterprise pour l'intégration LRS VPSX/MFI.	1. Copiez le `VPSX_MFI_R2` dossier depuis le programme d'installation LRS VPSX/MFI vers l'emplacement du serveur Rocket Enterprise à l'adresse. `C\BANKDEMO\print` 2. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de la EC2 documentation Amazon. 3. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration de Rocket Enterprise Server. 4. Dans la barre de menu, choisissez NATIVE. 5. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO. 6. Sous BANKDEMO, choisissez JES. 7. Sous JES Program Path, ajoutez le `DLL(VPSX_MFI_R2)` chemin depuis`C\BANKDEMO\print` .	Architecte du cloud

Configurer la file d'attente d'impression et les utilisateurs de l'impression

Tâche	Description	Compétences requises
Associez le module Rocket Software Print Exit au processus d'exécution du serveur d'impression par lots Rocket Enterprise Server.	1. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de la EC2 documentation Amazon. 2. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration du serveur Rocket Focus Enterprise. 3. Dans la barre de menu, choisissez NATIVE. 4. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO. 5. Sous BANKDEMO, choisissez JES et faites défiler l'écran vers le bas jusqu'à Imprimantes. 6. Dans Imprimantes, associez le module Rocket Software Print Exit (LRSPRTE6 pour Batch) au processus d'exécuti on du serveur (SEP) de l'imprimante par lots Rocket Enterprise Server. Cela permet le routage des sorties d'impression vers LRS VPSX/MFI.	Architecte du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations sur la configuration, consultez la section Utilisation de la sortie dans la documentation de OpenText Micro Focus.	

Tâche	Description	Compétences requises
Créez une file d'attente de sortie d'impression dans LRS VPSX/MFI et intégrez-la à LRS X. PageCenter	1. Connectez-vous à votre instance LRS EC2 VPSX/MFI. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, sélectionnez Imprimantes. 4. Choisissez Ajouter, puis sélectionnez Ajouter une imprimante. 5. Sur la page Configuration de l'imprimante, dans Nom de l'imprimante, saisissez Local. 6. Pour VPSX ID, entrez. VPS1 7. Pour CommType, sélectionnez TCP/IP/LRSQ. 8. Pour Host/IP Address, entrez l'adresse IP du Network Load Balancer situé devant les instances LRS X. PageCenter EC2 9. Pour le port distant, entrez 5800. 10. Pour Remote Queue, entrez le nom du dossier de documents LRS PageCenter X dans lequel la sortie sera stockée. 11. Choisissez Ajouter.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un utilisateur d'impression dans LRS VPSX/MFI.	1. Connectez-vous à votre instance LRS EC2 VPSX/MFI. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, choisissez Security, puis Users. 4. Dans la colonne Nom d'utilisateur, choisissez admin, puis Copier. 5. Dans la fenêtre Maintenance du profil utilisateur, pour Nom d'utilisateur, entrez un nom d'utilisateur (par exemple, PrintUser). 6. Dans Description, entrez une brève description (par exemple, Utilisateur pour le test d'impression). 7. Choisissez Mettre à jour. Cela crée un utilisateur d'impression (par exemple, PrintUser). 8. Dans le volet de navigation, sous Utilisateur, choisissez le nouvel utilisateur que vous avez créé. 9. Dans le menu Commande, sélectionnez Sécurité. 10. Sur la page Règles de sécurité, choisissez toutes	Architecte du cloud

Tâche	Description	Compétences requises
	les options de sécurité de l'imprimante et de sécurité des tâches applicables, puis sélectionnez Enregistrer. 11. Pour ajouter votre nouvel utilisateur d'impression au groupe des administrateurs, dans le volet de navigation, choisissez Sécurité, puis Configurer. 12. Dans la fenêtre de configuration de la sécurité, ajoutez votre nouvel utilisateur d'impression dans la colonne Administrateur.	

Configurer un serveur LRS PageCenter X sur Amazon EC2

Tâche	Description	Compétences requises
Créez une instance Amazon EC2 Windows.	Lancez une instance Amazon EC2 Windows en suivant les instructions de l'étape 1 : Lancer une instance dans la EC2 documentation Amazon. Utilisez le même nom d'hôte que celui que vous avez utilisé pour votre licence de produit LRS. Votre instance doit répondre aux exigences matérielles et	Architecte du cloud

Tâche	Description	Compétences requises
	logicielles suivantes pour LRS PageCenter X : • Processeur : double cœur • RAM — 16 GO • Disque dur : 500 Go • EC2 Instance minimale : `m5.xlarge` • Système d'exploitation — Windows • Logiciel : IIS ou Apache **Note** Les exigences matérielles et logiciell es ci-dessus sont destinées à un petit parc d'imprimantes (environ 500 à 1 000). Pour connaître toutes les exigences, consultez vos contacts LRS et AWS. 1. Lorsque vous créez votre instance Windows, vérifiez que le EC2 nom d'hôte est le même que celui utilisé pour la licence du produit LRS. 2. Connectez-vous à votre EC2 instance en suivant	

Tâche	Description	Compétences requises
	les instructions de la EC2 documentation Amazon. 3. Dans le menu Démarrer de Windows, recherchez et ouvrez le Gestionnaire de serveur. 4. Dans le Gestionnaire de serveur, choisissez Tableau de bord, Démarrage rapide, Ajouter des rôles et des fonctionnalités, puis choisissez Rôles de serveur. 5. Dans Rôles de serveur, choisissez WebServer (IIS), puis choisissez Développement d'applications. 6. Dans Développement d'applications, cochez la case CGI. 7. Pour installer CGI, suivez les instructions de l'assistant d'ajout de rôles et de fonctionnalités de Windows Server Manager. 8. Ouvrez le port 5800 pour le TCP/IP traffic in the Windows firewall of the EC2 instance. LRS VPSX uses the TCPIP/LRSQ protocole entrant sur le port 5800 pour communiquer avec le LRS X. PageCenter	

Tâche	Description	Compétences requises
Installez LRS PageCenter X sur l' EC2 instance.	1. Connectez-vous à votre EC2 instance. 2. Ouvrez le lien vers la page de téléchargement du produit contenu dans le message électronique LRS que vous auriez dû recevoir. **Note** Les produits LRS sont distribués par transfert électroni que de fichiers (EFT). 3. Téléchargez LRS PageCenter X et décompressez le fichier (dossier par défaut `:c:\LRS`). 4. Pour installer LRS PageCenter X, lancez le programme d'installation du produit LRS à partir du dossier décompressé. 5. Dans le menu Sélection ner les fonctionnalités, sélectionnez PageCente rX, puis cliquez sur Suivant pour démarrer le processus d'installation. Vous recevrez un message de confirmat	Architecte du cloud

Tâche	Description	Compétences requises
	ion lorsque l'installation sera terminée.	

Tâche	Description	Compétences requises
Installez LRS/DIS.	Il LRS/DIS product often is included in LRS VPSX installation. However, if LRS/DIS n'a pas été installé avec LRS VPSX. Procédez comme suit pour l'installer : 1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans l'e-mail LRS que vous devriez avoir reçu, téléchargez LRS/DIS, puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS. 4. Dans le programme d'installation du produit LRS, développez LRS Misc Tools, sélectionnez LRS DIS, puis Next. 5. Suivez le reste des instructions du programme d'installation du produit LRS pour terminer le processus d'installation.	Architecte du cloud

Tâche	Description	Compétences requises
Créer un groupe cible.	Créez un groupe cible en suivant les instructions de la section Créer un groupe cible pour votre Network Load Balancer. Lorsque vous créez le groupe cible, enregistrez l' EC2 instance LRS PageCenter X en tant que cible : 1. Sur la page Spécifier les détails du groupe, pour Choisir un type de cible, sélectionnez Instances. 2. Pour Protocole, choisissez TCP. 3. Pour Port, choisissez 5800. 4. Sur la page Enregistrer les cibles, dans la section Instances disponibles, sélectionnez l' EC2 instance LRS PageCenter X.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un Network Load Balancer.	Pour créer le Network Load Balancer, suivez les instructions de la documentation d'Elastic Load Balancing. Votre Network Load Balancer achemine le trafic depuis LRS VPSX/MFI vers l'instance LRS X. PageCenter EC2 Lorsque vous créez le Network Load Balancer, choisissez les valeurs suivantes sur la page Listeners and Routing : 1. Pour Protocol (Protocole), choisissez TCP. 2. Pour Port, choisissez 5800. 3. Pour Action par défaut, choisissez Transférer vers pour le groupe cible que vous avez créé précédemment.	Architecte du cloud

Configuration des fonctionnalités de gestion des sorties dans LRS X PageCenter

Tâche	Description	Compétences requises
Activez la fonction d'importation dans LRS X. PageCenter	Vous pouvez utiliser la fonction LRS PageCenter X Import pour reconnaître les sorties arrivant sur LRS PageCenter X selon des critères tels que le nom du Job	Architecte du cloud

Tâche	Description	Compétences requises
	ou le Form ID. Vous pouvez ensuite acheminer les sorties vers des dossiers spécifiques dans LRS X. PageCenter Pour activer la fonction d'importation, procédez comme suit : 1. Connectez-vous à votre EC2 instance LRS PageCenter X en suivant les instructions de la EC2 documentation Amazon. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'Explorateur de dossiers, choisissez Admin. 4. Sur la page Configura tion, choisissez Avancé, Paramètre d'importation. 5. Dans la section Paramètre s d'importation, cochez la case Importation avancée. 6. Pour valider les modificat ions, choisissez Mettre à jour.	

Tâche	Description	Compétences requises
Configurez la politique de conservation des documents.	LRS PageCenter X utilise une politique de conservation des documents pour décider de la durée de conservation d'un document dans PageCenter LRS X. Pour configurer la politique de conservation des documents, procédez comme suit : 1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'Explorateur de dossiers, choisissez Admin. 4. Sur la page Admin, choisissez Archive Group List/General admin, puis choisissez Retention policy. 5. Dans la section Politique de rétention, choisissez Ajouter pour créer une politique de rétention. 6. Sur la page Informations sur la politique de rétention , entrez le nom, la descripti on et la durée de conservat ion des documents de la politique de rétention.	Architecte du cloud

Tâche	Description	Compétences requises
	7. Pour enregistrer vos modifications et créer la politique, cliquez sur OK.	

Tâche	Description	Compétences requises
Créez une règle pour acheminer le document de sortie vers un dossier spécifique dans LRS X. PageCenter	Dans LRS PageCenter X, Destination détermine le chemin du dossier où la sortie sera envoyée lorsque cette destination est invoquée par Report Definition. Pour cet exemple, créez un dossier basé sur le dossier Form ID dans la définition du rapport et enregistrez la sortie dans ce dossier. 1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'explorateur de dossiers, choisissez Admin, Advance Import, Destinati on. 4. Dans la section Destinati on, choisissez Ajouter pour ouvrir le formulaire de maintenance des destinati ons. 5. Sur le formulaire Destinati on Maintenance, entrez les valeurs suivantes : • Nom de la destination — Formulaire • Description : descripti on de la destination,	Architecte du cloud

Tâche	Description	Compétences requises
	telle que la structure de dossiers basée sur un formulaire • Type de destination : dossier • Paramètres du dossier : chemin du dossier d'importation (le chemin du dossier qui sera créé dans PageCenter X lorsque le document arrivera ; par exemple, le chemin **`/Test/&FORM/&IMPORTDATE/&IMPORTTIME`** créera un dossier de base, un **`Test`** sous-dossier basé sur le nom du formulaire, un sous-dossier basé sur la date d'importation **`STD`**, puis un sous-dossier basé sur l'heure d'importation) • Nom du document : nom dynamique attribué à un document lorsqu'il est stocké dans le dossier. 6. Dans la liste déroulante, choisissez une politique de rétention. Par exemple, choisissez Year1 pour conserver le document pendant 1 an.	

Tâche	Description	Compétences requises
	7. Pour enregistrer les modifications, cliquez sur OK.	

Tâche	Description	Compétences requises
Créez une définition de rapport.	1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'explorateur de dossiers, choisissez Admin, Advance Import, Report Definition, puis sélectionnez Ajouter. 4. Sur la page de maintenance de la définition du rapport, sous l'onglet Général, entrez le nom de la définitio n du rapport. 5. Dans l'onglet Général, sous Champs, vous pouvez spécifier des critères de sélection tels que le nom du poste, le formulaire, la classe et l'auteur. Par exemple, vous pouvez saisir le nom de Job MFIDEMO. La valeur du nom de la tâche sera le nom de la tâche par lots qui générera la sortie d'impress ion. 6. Dans l'onglet Destination, sous Destination disponibl e, choisissez la destinati	Architecte du cloud

Tâche	Description	Compétences requises
	on créée précédemment (formulaire). 7. Choisissez Ajouter pour ajouter la destination du formulaire en tant que destination assignée. **Note** Cet exemple inclut une définition de rapport dans laquelle une sortie générée par le MFIDEMO et acheminée vers LRS PageCenter X est enregistrée dans la structure de dossiers définie dans la définition de destination.	

Configurer l'authentification et l'autorisation pour la gestion des sorties

Tâche	Description	Compétences requises
Créez un domaine Microsoft AD géré par AWS avec des utilisateurs et des groupes.	1. Pour créer un répertoire sur AWS Managed Microsoft AD, suivez les instructions de la section Création de votre répertoire AWS Managed Microsoft AD.	Architecte du cloud

Tâche	Description	Compétences requises
	2. Pour déployer une EC2 instance (gestionnaire Active Directory) et installer les outils Active Directory afin de gérer votre AWS Managed Microsoft AD, suivez les instructions de l'étape 3 : Déployer une EC2 instance pour gérer votre AWS Managed Microsoft AD. 3. Pour vous connecter à votre EC2 instance, suivez les instructions de la EC2 documentation Amazon. **Note** Lorsque vous vous connectez à l' EC2 instance, dans la fenêtre de sécurité Windows, entrez les informations d'identification de l'administrateur pour le répertoire que vous avez créé à l'étape 1. 4. Dans le menu Démarrer de Windows, sous Outils d'administration Windows, sélectionnez Utilisateurs et	

Tâche	Description	Compétences requises
	ordinateurs Active Directory . 5. Pour créer un utilisateur d'impression dans le domaine Active Directory, suivez les instructions de la section Créer un utilisateur.	
Joignez les EC2 instances à un domaine Microsoft AD géré par AWS.	Associez les PageCenter instances LRS VPSX/MFI et LRS X à EC2 votre domaine Microsoft AD géré par AWS automatiquement (documentation du centre de connaissances AWS) ou manuellement (documentation AWS Directory Service).	Architecte du cloud

Tâche	Description	Compétences requises
Configurez et intégrez LRS/DIS à AWS Managed Microsoft AD pour l'instance LRS X. PageCenter EC2	1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'Explorateur de dossiers, choisissez Admin. 4. Sur la page Configuration, dans la section Paramètres de sécurité, pour Type de sécurité, sélectionnez LRS/DIS. 5. Entrez vos préférences pour les autres options dans la section Paramètres de sécurité. 6. Dans le menu Démarrer de Windows, ouvrez le dossier PageCenterX, choisissez Server Start, puis Server Stop. 7. Connectez-vous à LRS PageCenter X à l'aide de votre nom d'utilisateur et de votre mot de passe Active Directory.	Architecte du cloud

Tâche	Description	Compétences requises
Configurer un groupe d'importation pour importer la sortie de LRS VPSX vers LRS X. PageCenter	1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'explorateur de dossiers, choisissez Admin, Security admin, Groups. 4. Dans la section Groupes, choisissez Ajouter pour ouvrir le formulaire des préférences de groupe. 5. Dans le formulaire de préférences de groupe, entrez les valeurs du nom du groupe et de la descripti on. 6. Développez les options générales, puis cochez la case Importer. 7. Pour enregistrer les modifications, cliquez sur OK.	Architecte du cloud

Tâche	Description	Compétences requises
Ajoutez une règle de sécurité au groupe d'importation.	1. Ouvrez le menu contextuel (clic droit) du groupe d'importation. 2. Choisissez Advance, puis Security. 3. Dans la section Sécurité, choisissez Importer, puis cochez la case Sous-dossier. 4. Pour enregistrer les modifications, choisissez Appliquer.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un utilisateur dans LRS PageCenter X pour effectuer l'importation des sorties depuis LRS VPSX/MFI.	Lorsque vous créez un utilisateur dans LRS PageCenter X pour effectuer une importation de sortie, le nom d'utilisateur doit être le même que l'ID VPSX de la file d'attente de sortie d'impress ion dans LRS VPSX/MFI. Dans cet exemple, l'identifiant VPSX est. VPS1 1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'explorateur de dossiers, choisissez Admin, Security admin, User. 4. Choisissez Ajouter pour ouvrir le formulaire de mise à jour du profil utilisateur. 5. Dans Maintenance du profil utilisateur, dans Nom d'utilisateur, entrez VPS1.	Architecte du cloud

Tâche	Description	Compétences requises
Ajoutez l'utilisateur LRS PageCenter X Import au groupe Import uniquement.	Pour fournir les autorisations nécessaires à l'importation de documents de LRS VPSX vers LRS PageCenter X, procédez comme suit : 1. Connectez-vous à votre EC2 instance LRS PageCenter X. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'explorateur de dossiers, choisissez Admin, Security admin, Groups. 4. Dans la section Groupes, ouvrez le menu contextue l (clic droit) du groupe Importer uniquement, puis choisissez Avancé, Sécurité. 5. Sur la page Dossiers de sécurité (ImportOnly), choisissez l'onglet Utilisate ur. 6. Dans l'onglet Utilisateur, sous Nom, sélectionnez l'utilisateur VPS1dans la liste déroulante, puis choisissez Appliquer.	Architecte du cloud

Tâche	Description	Compétences requises
Configurez LRS/DIS with AWS Managed Microsoft AD for the LRS VPSX/MFI EC2 l'instance.	1. Connectez-vous à votre instance LRS EC2 VPSX/MFI. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, choisissez Security, puis Configure. 4. Sur la page Configuration de la sécurité, dans la section Paramètres de sécurité, pour Type de sécurité, sélectionnez LRS/DIS (externe). 5. Entrez vos préférences pour les autres options dans la section Paramètres de sécurité. 6. Dans le menu Démarrer de Windows, ouvrez le dossier LRS Output Management, choisissez Server Start, puis Server Stop. 7. Connectez-vous à LRS VPSX/MFI à l'aide de votre nom d'utilisateur et de votre mot de passe Active Directory.	Architecte du cloud

Configurer le serveur de fichiers Amazon FSx pour Windows en tant que magasin de données opérationnelles pour LRS X PageCenter

Tâche	Description	Compétences requises
Créez un système de fichiers pour LRS X. PageCenter	Pour utiliser le serveur de fichiers Amazon FSx pour Windows comme magasin de données opérationnel pour LRS PageCenter X dans un environnement multi-AZ, suivez les instructions de l'étape 1 : Création de votre système de fichiers.	Architecte du cloud
Mappez le partage de fichiers à l' EC2 instance LRS PageCenter X.	Pour mapper le partage de fichiers créé à l'étape précédente à l' EC2 instance LRS PageCenter X, suivez les instructions de l'étape 2 : mapper votre partage de fichiers à une EC2 instance exécutant Windows Server.	Architecte du cloud
Mappez le répertoire de contrôle LRS PageCenter X et le répertoire des dossiers principaux sur le lecteur de partage FSx réseau Amazon.	1. Connectez-vous à votre EC2 instance LRS PageCenter X en suivant les instructions de la EC2 documentation Amazon. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans l'Explorateur de dossiers, choisissez Admin, Configuration. 4. Sur la page Configuration, choisissez Répertoires, puis	Architecte du cloud

Tâche	Description	Compétences requises
	sélectionnez Répertoire de contrôle. 5. Dans Répertoires de contrôle, entrez`\\FSx file share DNS name \share\cntl` . 6. Dans le répertoire des dossiers principaux, entrez`\\FSx file share DNS name\share\mstr` .	

Tester un flux de travail de gestion des sorties

Tâche	Description	Compétences requises
Lancez une demande d'impression par lots depuis l' BankDemo application Rocket Software.	1. Ouvrez l'émulateur 3270-terminal dans votre instance Rocket Enterprise Server. EC2 2. Connectez-vous à l' BankDemo applicati on en exécutant la commande`connect 127.0.0.1:9278` . 3. Sur l'interface de ligne de BankDemo commande, dans le champ ID utilisate ur, entrez B0001. Dans le champ Mot de passe, entrez une clé non vide. 4. Pour l'option Demander l'impression de relevés, entrez X sur la ligne vide.	Ingénieur de test

Tâche	Description	Compétences requises
	5. Dans la section Envoyer l'instruction par, pour Mail, entrez Y, puis appuyez sur F10.	

Tâche	Description	Compétences requises
Vérifiez la sortie d'impression dans LRS X. PageCenter	1. Connectez-vous à votre EC2 instance LRS PageCenter X en suivant les instructions de la EC2 documentation Amazon. 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web PCX. 3. Dans le volet de navigation, ouvrez le dossier Test, ouvrez le dossier STD, puis ouvrez le dossier avec la date d'exécution de la tâche, par exemple `08-03-2023` (MM-DD-YYYY). **Note** Il s'agit de la même structure de dossiers que celle définie dans l'article Créez une règle pour acheminer le document de sortie vers un dossier spécifique dans LRS PageCenter X. 4. Ouvrez le fichier `formtest-STD.txt` . Vous pouvez maintenant voir la sortie imprimée d'un	Ingénieur de test

Tâche	Description	Compétences requises
	relevé de compte avec des colonnes pour le numéro de compte. , Description, date, montant et solde. Pour un exemple, voir la `batch_print_output` pièce jointe de ce modèle.	

Ressources connexes

- LRS
- Flux de données de présentation des fonctions avancées (documentation IBM)
- Flux de données conditionné par ligne (LCDS) (documentation Compart)
- Optimisation des charges de travail du mainframe d'entreprise sur AWS avec Micro Focus (article de blog)
- Modernisez les charges de travail d'impression en ligne de votre mainframe sur AWS (AWS Prescriptive Guidance)
- Modernisez les charges de travail d'impression par lots de votre mainframe sur AWS (AWS Prescriptive Guidance)

Informations supplémentaires

Considérations

Au cours de votre processus de modernisation, vous pouvez envisager une grande variété de configurations pour les processus par lots et en ligne du mainframe et les résultats qu'ils génèrent. La plate-forme centrale a été personnalisée par chaque client et fournisseur qui l'utilise avec des exigences particulières qui ont une incidence directe sur l'impression. Par exemple, votre plateforme actuelle peut intégrer le flux de données IBM AFP ou Xerox LCDS dans le flux de travail actuel. En outre, les caractères de commande du chariot de l'ordinateur central et les mots de commande des canaux peuvent affecter l'apparence de la page imprimée et nécessiter un traitement spécial. Dans le cadre du processus de planification de la modernisation, nous vous recommandons d'évaluer et de comprendre les configurations de votre environnement d'impression spécifique.

Capture de données d'impression

Rocket Software Print Exit transmet les informations nécessaires au LRS VPSX/MFI pour traiter efficacement le fichier spool. Les informations se composent de champs transmis dans les blocs de contrôle appropriés, tels que les suivants :

- NOM DU POSTE
- PROPRIÉTAIRE (IDENTIFIANT UTILISATEUR)
- DESTINATION
- FORMULAIRE
- NOM DE FICHIER
- ÉCRIVAIN

Le LRS VPSX/MFI prend en charge les mécanismes de traitement par lots du mainframe suivants pour capturer des données depuis Rocket Enterprise Server :

- Instructions COBOL BATCHprint/spool processing using standard z/OS JCL SYSOUT DD/ OUTPUT.
- Instructions BATCH COBOL print/spool processing using standard z/OS JCL CA-SPOOL SUBSYS DD.
- IMS/COBOL print/spooltraitement à l'aide de l'interface CBLTDLI. Pour obtenir la liste complète des méthodes prises en charge et des exemples de programmation, consultez la documentation LRS incluse dans la licence de votre produit.

Contrôles de santé du parc d'imprimantes

Le LRS VPSX/MFI (LRS LoadX) peut effectuer des contrôles de santé approfondis, y compris la gestion des appareils et l'optimisation opérationnelle. La gestion des périphériques permet de détecter les défaillances d'une imprimante et d'acheminer la demande d'impression vers une imprimante saine. Pour plus d'informations sur les contrôles de santé approfondis des parcs d'imprimantes, consultez la documentation LRS incluse dans la licence de votre produit.

Authentification et autorisation d'impression

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or a Lightweight Directory Access Protocol (LDAP) server. In addition to basic print

authorization, LRS/DISpeut également appliquer des contrôles de sécurité d'impression de niveau granulaire dans les cas d'utilisation suivants :

- Gérez les personnes autorisées à parcourir la tâche d'impression.
- Gérez le niveau de navigation des offres d'emploi des autres utilisateurs.
- Gérez les tâches opérationnelles, par exemple la sécurité au niveau de la commande, telle que la mise en attente ou la libération, la purge, la modification, la copie et le réacheminement. La sécurité peut être configurée par l'ID utilisateur ou par le groupe, comme dans le cas d'un groupe de sécurité Active Directory ou d'un groupe LDAP.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Modernisez l'application CardDemo mainframe en utilisant AWS Transform

Créée par Santosh Kumar Singh (AWS) et Cheryl du Preez (AWS)

Récapitulatif

AWS Transformest conçu pour accélérer la modernisation des applications mainframe. Il utilise l'IA générative pour rationaliser le processus de modernisation du mainframe. Il automatise les tâches complexes, telles que l'analyse du code existant, la documentation du mainframe, l'extraction des règles métier, la décomposition des applications monolithiques dans le domaine métier et le refactoring du code. Il accélère les projets de modernisation en automatisant des tâches complexes, telles que l'analyse des applications et la planification des séquences de migration. Lorsque vous décomposez des applications monolithiques, AWS Transform séquencez intelligemment la transformation des applications mainframe, ce qui vous permet de transformer les fonctions métiers en parallèle. AWS Transform peut accélérer la prise de décision et améliorer l'agilité opérationnelle et l'efficacité de la migration.

Ce modèle fournit des step-by-step instructions pour vous aider à tester les capacités de modernisation du mainframe AWS Transform by using CardDemo, qui est un exemple d'application mainframe open source.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- AWS IAM Identity Center, activé
- Autorisations permettant aux administrateurs d'activer AWS Transform
- Autorisations permettant aux administrateurs d'accepter les demandes de connexion Amazon Simple Storage Service (Amazon S3) pour AWS Transform l'application Web

Limites

- AWS Transform n'est disponible que dans certains cas Régions AWS. Pour obtenir la liste complète des régions prises en charge, consultez la section Régions prises en charge pour AWS Transform.
- AWS Transform prend en charge l'analyse du code, la génération de documents, l'extraction des règles métier, la décomposition et le refactoring du langage COBOL (Common Business-

Oriented Language) vers Java. Pour plus d'informations, consultez les sections Fonctionnalités et fonctionnalités clés et Types de fichiers pris en charge pour la transformation des applications mainframe.

- Il existe un quota de service pour les capacités de transformation du mainframe dans AWS Transform. Pour plus d'informations, consultez la section Quotas pour AWS Transform.
- Pour collaborer sur un espace de travail partagé, tous les utilisateurs doivent être des utilisateurs enregistrés de la même instance AWS IAM Identity Center que celle associée à votre instance de l'application AWS Transform Web.
- Le compartiment Amazon S3 AWS Transform doit se trouver dans la même Compte AWS région.

Architecture

Le schéma suivant montre l'architecture que vous avez configurée dans ce modèle.

Le schéma suivant illustre le flux de travail suivant :

1. AWS Transform utilise un connecteur pour accéder à l'application CardDemo mainframe, qui est stockée dans un compartiment Amazon S3.
2. AWS Transform permet AWS IAM Identity Center de gérer l'accès et l'authentification des utilisateurs. Le système met en œuvre plusieurs niveaux de contrôles de sécurité pour l'authentification, l'autorisation, le chiffrement et la gestion des accès afin de protéger le code et les artefacts pendant le traitement. Les utilisateurs interagissent avec l' AWS Transform agent via une interface de chat. Vous pouvez fournir des instructions à l'agent AI pour des tâches spécifiques en anglais. Pour plus d'informations, consultez Human in the loop (HITL) dans la AWS Transform documentation.
3. L'agent AI interprète les instructions de l'utilisateur, crée un plan de travail, divise le travail en tâches exécutables et l'exécute de manière autonome. Les utilisateurs peuvent examiner et approuver la transformation. Les tâches de transformation sont les suivantes :
   - Analyse du code : AWS Transform analyse le code de chaque fichier pour obtenir des détails tels que le nom du fichier, le type de fichier, les lignes de code et leurs chemins. L'agent analyse le code source, exécute des classifications, crée des mappages de dépendances et identifie les artefacts manquants. Il identifie également les composants dupliqués.
   - Génération de documents : AWS Transform génère de la documentation pour l'application mainframe. En analysant le code, il peut créer automatiquement une documentation détaillée

des programmes d'application, y compris des descriptions de la logique métier, des flux, des intégrations et des dépendances présents dans vos anciens systèmes.

- Extraction de la logique métier : AWS Transform analyse les programmes COBOL pour documenter leur logique métier de base, afin de vous aider à comprendre la logique métier fondamentale.
- Décomposition du code : AWS Transform décompose le code en domaines qui tiennent compte des dépendances entre les programmes et les composants. Le regroupement de fichiers et de programmes connexes au sein d'un même domaine améliore l'organisation et permet de préserver la structure logique de l'application lors de sa décomposition en composants plus petits.
- Planification de la vague de migration — Sur la base des domaines que vous avez créés pendant la phase de décomposition, AWS Transform génère un plan de vague de migration avec un ordre de modernisation recommandé.
- Refactorisation du code : AWS Transform refactorise le code de tous les fichiers de domaine ou de certains fichiers de domaine en code Java. L'objectif de cette étape est de préserver la logique métier critique de l'application tout en la refactorisant pour en faire une application Java modernisée et optimisée pour le cloud.

4. AWS Transform stocke le code refactorisé, les documents générés, les artefacts associés et les bibliothèques d'exécution dans votre compartiment Amazon S3. Vous pouvez effectuer les actions suivantes :
   - Accédez au dossier d'exécution de votre compartiment Amazon S3.
   - Créez et déployez l'application en suivant la section Création et déploiement de votre application modernisée après le refactoring figurant dans la documentation. AWS Transform
   - Via l'interface de chat, demandez et téléchargez un échantillon ou un modèle AWS CloudFormation Hashicorp Terraform. AWS Cloud Development Kit (AWS CDK) Ces modèles peuvent vous aider à déployer les AWS ressources nécessaires pour prendre en charge l'application refactorisée.
   - Utilisez Reforge pour améliorer la qualité du code refactorisé en utilisant de grands modèles de langage (). LLMs Le moteur de refactorisation préserve l'équivalence fonctionnelle du COBOL tout en le transformant en code Java. La reforge est une étape facultative qui est disponible après la transformation. Cette étape permet LLMs de restructurer le code pour qu'il ressemble étroitement à Java natif, ce qui peut améliorer la lisibilité et la maintenabilité. Reforge ajoute également des commentaires lisibles par l'homme pour vous aider à comprendre le code, et met en œuvre des modèles de codage modernes et les meilleures pratiques.

Outils

Services AWS

- AWS Transformutilise l'IA agentic pour vous aider à accélérer la modernisation des charges de travail existantes, telles que .NET, le mainframe et les charges de travail. VMware
- AWS IAM Identity Centervous permet de gérer de manière centralisée l'accès par authentification unique (SSO) à vos applications Comptes AWS et à celles du cloud.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

Vous pouvez utiliser l'application open source pour AWS CardDemoordinateur central comme exemple d'application pour démarrer la modernisation du mainframe.

Bonnes pratiques

- Commencez modestement : commencez par un code petit et moins complexe (15 000 à 20 000 lignes de code) pour comprendre comment AWS Transform analyse et transforme les applications mainframe.
- Combinez avec l'expertise humaine — Utilisez-le AWS Transform comme accélérateur tout en appliquant l'expertise humaine pour des résultats optimaux.
- Révision et test approfondis — Passez toujours en revue le code transformé avec soin et effectuez des tests complets pour valider l'équivalence fonctionnelle après la transformation.
- Fournir des commentaires — Pour fournir des commentaires et des suggestions d'amélioration, utilisez le bouton Envoyer des commentaires dans le AWS Management Console ou créez un dossier auprès de AWS Support. Pour plus d'informations, consultez la section Création d'un dossier de support. Vos commentaires sont précieux pour l'amélioration des services et le développement futur.

Épopées

Préparation de l'application mainframe

Tâche	Description	Compétences requises
Créez un compartiment.	Créez un compartiment Amazon S3 dans le même compartiment Compte AWS et dans la région où AWS Transform il est activé. Vous utilisez ce compartiment pour stocker le code de l'applica tion mainframe, et vous AWS Transform l'utilisez pour stocker les documents générés, le code refactorisé et les autres fichiers associés à la transformation. Pour obtenir des instructions, consultez la section Création d'un compartiment dans la documentation Amazon S3.	AWS général
Préparez l'exemple d'applica tion pour ordinateur central.	1. Entrez la commande suivante pour cloner le CardDemoréférentiel sur votre station de travail locale : `git clone https://g ithub.com/aws-samp les/aws-mainframe- modernization-card demo.git` 2. Créez un nouveau dossier nommé`carddemo`.	Développeur d'applications, DevOps ingénieur

Tâche	Description	Compétences requises
	3. Copiez le `app` dossier, qui contient le code source du mainframe, depuis le référentiel cloné vers le `carddemo` dossier. 4. Compressez le `cardemo` dossier dans un fichier ZIP. 5. Téléchargez le fichier ZIP dans le compartiment Amazon S3 que vous avez créé. Pour obtenir des instructions, consultez la section Chargement d'objets dans la documentation Amazon S3.	

Configurer IAM Identity Center et AWS Transform

Tâche	Description	Compétences requises
Ajoutez des utilisateurs à IAM Identity Center.	Ajoutez vos utilisateurs potentiels à IAM Identity Center. Suivez les instructions de la section Ajout d'utilisateurs dans IAM Identity Center dans la AWS Transform documentation.	Administrateur AWS
Activez AWS Transform et ajoutez des utilisateurs.	1. Activer AWS Transform. Suivez les instructions de la section Activer AWS Transform. 2. Ajoutez des utilisateurs à AWS Transform. Suivez les	Administrateur AWS

Tâche	Description	Compétences requises
	instructions de la section Ajouter des utilisateurs à AWS Transform.	
Configurez l'accès des utilisateurs à l'application AWS Transform Web.	Chaque utilisateur doit accepter l'invitation pour accéder à l'application AWS Transform Web. Suivez les instructions de la section Acceptation de l'invitation dans la AWS Transform documentation.	Développeur d'applications, propriétaire de l'application
Connectez-vous à l'application AWS Transform Web.	Suivez les instructions de la section Se connecter à AWS Transform.	Développeur d'applications, propriétaire de l'application
Configurez un espace de travail.	Configurez un espace de travail dans lequel les utilisateurs peuvent collaborer dans l'application AWS Transform Web. Suivez les instructions de la section Configuration de votre espace de travail dans la AWS Transform documentation.	Administrateur AWS

Transformez l'application mainframe

Tâche	Description	Compétences requises
Créez une tâche de transformation.	Créez une tâche de transformation pour moderniser l'application CardDemo mainframe. Pour obtenir des instructions,	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	consultez la section Créer et démarrer une tâche dans la AWS Transform documentation. Lorsque vous êtes invité à définir les objectifs dans l'interface de AWS Transform chat, choisissez Effectuer la modernisation du mainframe (IBM z/OS vers AWS), puis sélectionnez Analyser le code, Générer la documentation technique, Logique métier, Décomposer le code, Planifier la séquence de migration et Transformer le code en Java.	
Configurez le connecteur.	Établissez un connecteur vers le compartiment Amazon S3 qui contient l'application CardDemo mainframe. Ce connecteur permet d'accéder AWS Transform aux ressources du bucket et d'exécuter des fonctions de transformation consécutives. Pour obtenir des instructions, consultez la section Configuration d'un connecteur dans la AWS Transform documentation.	Administrateur AWS

Tâche	Description	Compétences requises
Effectuez une analyse de code.	1. Sur la page Spécifier l'emplacement des actifs, entrez le chemin du compartiment Amazon S3 pour le fichier `carddemo` ZIP que vous avez chargé. 2. Choisissez Approuver et envoyer à AWS Transform . Il commence à analyser le code. 3. Surveillez l'état dans l'onglet Worklog. 4. Lorsque l'analyse est terminée, sous Analyser le code dans le volet de navigation de gauche, choisissez Afficher les résultats de l'analyse du code. 5. (Facultatif) Choisissez Télécharger pour télécharger la liste complète des ressources, le code source manquant et le fichier de dépendance. Pour plus d'informations, consultez la section Analyse du code dans la AWS Transform documentation.	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
Générez de la documentation technique.	1. Dans le volet de navigation de gauche, sous Générer la documentation technique, choisissez Sélectionner les fichiers et configurer les paramètres. 2. Développez COBOL ou JCL, puis sélectionnez un ou plusieurs fichiers. 3. Choisissez le niveau de détail de la documentation : • Résumé — Fournit une vue d'ensemble de haut niveau de chaque fichier inclus dans le champ d'application. Donne également un résumé d'une ligne de chaque fichier. • Spécification fonctionnelle détaillée : fournit des informations complètes pour chaque fichier inclus dans le périmètre de transformation de l'application mainframe. Certains détails incluent la logique et le flux, les règles métier identifiées, le flux de données, les dépendances, le traitement des entrées et des sorties et divers détails des transactions.	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	4. Choisissez Envoyer à AWS Transform. 5. Surveillez la progression dans l'onglet Worklog. **Note** Le temps de génération des documents varie de quelques minutes à quelques heures, selon le nombre de fichiers et de lignes de code. 6. Lorsque vous avez terminé, sélectionnez Consulter les résultats de la documenta tion. 7. Accédez au document généré via l'application Web ou téléchargez-le. La documentation générée est également stockée dans le compartiment Amazon S3. 8. Explorez la documenta tion générée en posant des questions spécifiques dans l'interface de chat. Par exemple, vous pouvez dire « Dites-moi les fonctionn alités de CBACT01C ».	

Tâche	Description	Compétences requises
	Pour plus d'informations, voir Génération de documentation technique dans la AWS Transform documentation.	

Tâche	Description	Compétences requises
Extrayez la logique métier.	1. Dans le volet de navigation de gauche, développez Extract business logic, puis sélectionnez Select files for business logic extraction. 2. Développez COBOL ou JCL, puis sélectionnez un ou plusieurs fichiers. 3. Choisissez Envoyer à AWS Transform. 4. Surveillez la progression dans l'onglet Worklog. **Note** Le temps d'extraction de la logique métier varie de quelques minutes à quelques heures, selon le nombre de fichiers et de lignes de code. 5. Lorsque l'extraction est terminée, choisissez Examiner les résultats de l'extraction de la logique métier. 6. Sélectionnez un fichier COBOL ou JCL, puis choisissez Afficher. 7. Modifiez le champ d'application dans le diagramme de	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	flux et les règles fonctionn elles pour passer en revue les différents niveaux des organigrammes, y compris le code correspondant. 8. (Facultatif) Passez en revue la logique métier générée, qui est stockée au format JSON dans votre compartiment Amazon S3. Pour plus d'informations, voir Extraire la logique métier dans la AWS Transform documenta tion.	

Tâche	Description	Compétences requises
Décomposez le code.	1. Dans le volet de navigation de gauche, développez le code, puis choisissez Décomposer en domaines. 2. Dans la liste Actions, sélectionnez Créer un domaine. 3. Entrez un nom pour le nouveau domaine, tel que `Bill payment`. 4. (Facultatif) Fournissez une description. 5. Dans la barre de recherche Rechercher des fichiers `CB00`, recherchez puis sélectionnez le fichier. 6. Choisissez Marquer comme graine. 7. Vérifiez que le drapeau de départ passe de Non à Oui. 8. Choisissez Créer. 9. Choisissez Enregistrer. 10. Choisissez Decompose. 11. Passez en revue le résultat de décomposition en choisissant le nom de domaine. 12. Lorsque la décomposition est terminée, choisissez Envoyer vers AWS Transform.	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	Pour plus d'informations sur la décomposition et les germes, consultez la section Décomposition dans la AWS Transform documentation.	
Planifiez les vagues de migration.	Planifiez les vagues de migration de l' CardDemo application. Suivez les instructions de la section Planification des vagues de migration dans la AWS Transform documentation pour revoir et modifier le plan des vagues.	Développeur d'applications, propriétaire de l'application
Refactorisez le code.	1. Refactorisez l'application CardDemo mainframe en code Java dans tous les fichiers de domaine ou dans certains fichiers de domaine. Suivez les instructions du code Refactor de la AWS Transform documentation. 2. Une fois le processus de refactorisation terminé, créez et déployez l'application Java modernisée. Suivez les instructions de la section Créez et déployez votre application modernisée après le refactoring dans la documentation. AWS Transform	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
(Facultatif) Utilisez Reforge pour améliorer le code Java.	1. Créez une nouvelle tâche, puis entrez un objectif de`Reforge the code`. 2. Entrez le nom d'un projet qui a été modernisé grâce à AWS Transform. Ce projet doit se trouver dans votre compartiment Amazon S3. 3. Entrez la liste des classes Java qui indique les classes de service à reforger. 4. Passez en revue la sortie générée dans le compartiment Amazon S3. Pour plus d'informations, consultez Reforge dans la AWS Transform documentation.	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
Simplifiez le déploiement.	AWS Transform peut fournir des modèles d'infrastructure sous forme de code (IaC) pour CloudFormation AWS CDK, ou Terraform. Ces modèles vous aident à déployer des composants de base, notamment des ressources de calcul, de base de données, de stockage et de sécurité. 1. Dans l'interface de AWS Transform chat, demandez les modèles en saisissan t`Share the mainframe refactor <service> templates` , où se `<service>` trouve l'un des services iAc pris en charge. 2. Déployez le modèle en utilisant le service de votre choix. Consultez par exemple les ressources suivantes : • Création d'une pile depuis la CloudFormation console (CloudFormation documentation) • Déployer AWS CDK des applications (AWS CDK documentation)	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	• Construire une infrastructure (documentation Terraform) Pour plus d'informations, consultez la section Capacités de déploiement dans la AWS Transform documentation.	

Résolution des problèmes

Problème	Solution
Vous ne pouvez pas afficher le code source ou le document généré dans l'application AWS Transform Web.	Ajoutez une politique à l'autorisation CORS pour le compartiment Amazon S3 afin de l'autoriser AWS Transform comme origine. Pour plus d'informations, consultez la section Autorisations CORS du compartiment S3 dans la AWS Transform documentation.

Ressources connexes

AWS documentation

- Transformation des applications mainframe (AWS Transform documentation)

Autres AWS ressources

- Accélérez votre processus de modernisation des mainframes à l'aide d'agents d'intelligence artificielle avec AWS Transform (article de AWS blog)
- AWS Transform FAQs
- AWS IAM Identity Center FAQs

Vidéos et didacticiels

- Présentation d'Amazon Q Developer : Transform (AWS Skill Builder)
- AWS re:Invent 2024 - Modernisez plus rapidement les applications mainframe à l'aide d'Amazon Q Developer () YouTube
- AWS re:Invent 2024 - Automatiser la migration et la modernisation pour accélérer la transformation () YouTube
- AWS re:Invent 2024 - Toyota stimule l'innovation et améliore l'efficacité opérationnelle grâce à la génération AI () YouTube

> **Note**
>
> AWS Transform était auparavant connu sous le nom d'Amazon Q Developer transform for mainframe.

Modernisez les charges de travail d'impression par lots du mainframe AWS en utilisant Rocket Enterprise Server et LRS VPSX/MFI

Créée par Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) et Kevin Yung (AWS)

Récapitulatif

Ce modèle vous montre comment moderniser les charges de travail d'impression par lots critiques de votre mainframe sur le cloud Amazon Web Services (AWS) en utilisant Rocket Enterprise Server comme environnement d'exécution pour une application mainframe modernisée et LRS VPSX/MFI (Micro Focus Interface) comme serveur d'impression. Le modèle est basé sur l'approche de modernisation du mainframe replateforme. Cette approche consiste à migrer les tâches par lots de votre mainframe vers Amazon Elastic Compute Cloud (Amazon EC2) et à migrer votre base de données mainframe, telle qu'IBM DB2 for z/OS, vers Amazon Relational Database Service (Amazon RDS). L'authentification et l'autorisation pour le flux de travail d'impression modernisé sont effectuées par AWS Directory Service pour Microsoft Active Directory, également connu sous le nom d'AWS Managed Microsoft AD. Le serveur d'informations d'annuaire LRS (LRS/DIS) est intégré à AWS Managed Microsoft AD. En modernisant vos charges de travail d'impression par lots, vous pouvez réduire les coûts d'infrastructure informatique, atténuer la dette technique liée à la maintenance des systèmes existants, supprimer les silos de données, accroître l'agilité et l'efficacité grâce à un DevOps modèle et tirer parti des ressources à la demande et de l'automatisation dans le cloud AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une charge de travail d'impression ou de gestion des sorties sur ordinateur central
- Connaissances de base sur la façon de reconstruire et de fournir une application mainframe qui s'exécute sur Rocket Enterprise Server (pour plus d'informations, consultez la fiche technique du serveur Rocket Enterprise dans la documentation Rocket.)
- Connaissances de base des solutions et concepts d'impression cloud LRS
- Logiciel et licence Rocket Enterprise Server (Pour plus d'informations, contactez le service commercial de Rocket.)
- VPSX/MFI, LRS/Queue, and LRS/DISLogiciels et licences LRS (Pour plus d'informations, contactez le service commercial LRS.)

> **Note**
>
> Pour plus d'informations sur les considérations relatives à la configuration des charges de travail d'impression par lots du mainframe, consultez la section Considérations de la section Informations supplémentaires de ce modèle.

Versions du produit

- Rocket Enterprise Server 6.0 (mise à jour du produit 7)
- LRS VPSX/MFI V1R3 ou supérieur

Architecture

Pile technologique source

- Système d'exploitation — IBM z/OS
- Langage de programmation — Langage orienté métier commun (COBOL), langage de contrôle des tâches (JCL) et système de contrôle des informations clients (CICS)
- Base de données — IBM DB2 pour z/OS et méthode d'accès au stockage virtuel (VSAM)
- Sécurité : Resource Access Control Facility (RACF), CA Top Secret pour z/OS et Access Control Facility 2 () ACF2
- Gestion de l'impression et de la sortie : produits d'impression IBM mainframe z/OS (IBM Tivoli Output Manager pour z/OS, LRS et CA View)

Pile technologique cible

- Système d'exploitation — Microsoft Windows Server exécuté sur Amazon EC2
- Calcul — Amazon EC2
- Langage de programmation : COBOL, JCL et CICS
- Base de données — Amazon RDS
- Sécurité — Microsoft AD géré par AWS
- Gestion de l'impression et de la sortie : solution d'impression LRS sur AWS
- Environnement d'exécution mainframe — Rocket Enterprise Server

Architecture source

Le schéma suivant montre une architecture d'état actuelle typique pour une charge de travail d'impression par lots sur un mainframe :

Le schéma suivant illustre le flux de travail suivant :

1. Les utilisateurs effectuent des transactions commerciales sur un système d'engagement (SoE) basé sur une application IBM CICS écrite en COBOL.
2. Le SoE invoque le service mainframe, qui enregistre les données des transactions commerciales dans une base de données system-of-records (SoR) telle qu'IBM DB2 for z/OS.
3. Le SoR conserve les données commerciales provenant du SoE.
4. Le planificateur de tâches par lots lance une tâche par lots pour générer une sortie d'impression.
5. Le traitement par lots extrait les données de la base de données, les met en forme en fonction des besoins commerciaux, puis génère des résultats commerciaux tels que des relevés de facturation, des cartes d'identité ou des relevés de prêt. Enfin, le traitement par lots achemine la sortie vers la gestion des sorties d'impression pour le traitement et la livraison des sorties, en fonction des exigences commerciales.
6. La gestion des sorties d'impression reçoit les résultats d'impression du traitement par lots, puis les transmet à une destination spécifiée, telle qu'un e-mail, un partage de fichiers utilisant un protocole FTP sécurisé, une imprimante physique utilisant des solutions d'impression LRS (comme illustré dans ce modèle) ou IBM Tivoli.

Architecture cible

Le schéma suivant montre l'architecture d'une charge de travail d'impression par lots sur mainframe déployée dans le cloud AWS :

Le schéma suivant illustre le flux de travail suivant :

1. Le planificateur de tâches par lots lance une tâche par lots pour créer des sorties d'impression, telles que des relevés de facturation, des cartes d'identité ou des relevés de prêt.
2. Le traitement par lots du mainframe (replatformé sur Amazon EC2) utilise le runtime Rocket Enterprise Server pour extraire les données de la base de données de l'application, appliquer une

logique métier aux données, les formater, puis les envoyer vers une destination d'impression à l'aide de Rocket Software Print Exit (documentation Micro Focus).

3. La base de données de l'application (un SoR qui s'exécute sur Amazon RDS) conserve les données pour l'impression.
4. L'agent de VPSX/MFI printing solution is deployed on Amazon EC2 and its operational data is stored in Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI uses the TCP/IP-based LRS/Queue transmission LRS permet de collecter les données d'impression via l'API JES Print Exit de Rocket Software et de les transmettre à une destination d'imprimante spécifiée.

> **Note**
>
> La solution cible ne nécessite généralement pas de modifications de l'application pour s'adapter aux langages de formatage du mainframe, tels qu'IBM Advanced Function Presentation (AFP) ou Xerox Line Condition Data Stream (LCDS). Pour plus d'informations sur l'utilisation de Rocket Software pour la migration et la modernisation des applications mainframe sur AWS, consultez le billet de blog Empowering Enterprise Mainframe Workloads on AWS with Micro Focus.

Architecture de l'infrastructure AWS

Le schéma suivant montre une architecture d'infrastructure AWS hautement disponible et sécurisée pour une charge de travail d'impression par lots sur mainframe :

Le schéma suivant illustre le flux de travail suivant :

1. Le planificateur de lots lance le processus de traitement par lots et est déployé sur Amazon EC2 dans plusieurs zones de disponibilité pour une haute disponibilité (HA).

   > **Note**
   >
   > Ce modèle ne couvre pas la mise en œuvre du planificateur de lots. Pour plus d'informations sur la mise en œuvre, consultez la documentation du fournisseur de logiciels pour votre planificateur.

2. Le traitement par lots du mainframe (écrit dans un langage de programmation tel que JCL ou COBOL) utilise la logique métier de base pour traiter et générer des documents imprimés, tels que

des relevés de facturation, des cartes d'identité et des relevés de prêt. La tâche est déployée sur Amazon EC2 dans deux zones de disponibilité pour HA et utilise Rocket Software Print Exit pour acheminer les résultats d'impression vers LRS VPSX/MFI pour l'impression par l'utilisateur final.

3. VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Rocket Software JES Print Exit programming interface. Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the spool file and dynamically build LRS/QueueCommandes LRS. Les commandes sont ensuite exécutées à l'aide d'une fonction intégrée standard de Rocket Software.

> **Note**
>
> Pour plus d'informations sur les données d'impression transmises de Rocket Software Print Exit aux mécanismes de traitement par lots du mainframe pris en LRS/Queue and LRS VPSX/MFI charge, consultez la section Capture des données d'impression dans la section Informations supplémentaires de ce modèle.

4.
> **Note**
>
> Un Network Load Balancer fournit un nom DNS pour intégrer Rocket Enterprise Server au LRS VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI et achemine le trafic vers les cibles enregistrées qui sont saines.

5.
> **Note**
>
> Le serveur d'impression LRS VPSX/MFI est déployé EC2 sur Amazon dans deux zones de disponibilité pour HA et utilise Amazon EBS comme magasin de données opérationnel. LRS VPSX/MFI supports both the active-active and active-passive service modes. This architecture uses multiple AZs in an active-passive pair as an active and hot standby. The Network Load Balancer performs a health check on LRS VPSX/MFI EC2 instances and routes traffic to hot standby instances in the other AZ if an active instance is in an unhealthy state. The print requests are persisted in the LRS Job Queue locally in each of the EC2 instances. In the event of recovery, a failed instance has to be restarted for the LRS services to resume processing the print request. : LRS VPSX/MFI peut également effectuer des contrôles de santé au niveau du parc d'imprimantes. Pour plus

d'informations, consultez la section Contrôles de santé du parc d'imprimantes dans la section Informations supplémentaires de ce modèle.

6. AWS Managed Microsoft AD s'intègre à LRS/DIS pour effectuer l'authentification et l'autorisation du flux de travail d'impression. Pour plus d'informations, voir Authentification et autorisation d'impression dans la section Informations supplémentaires de ce modèle.
7. LRS VPSX/MFI utilise Amazon EBS pour le stockage par blocs. Vous pouvez sauvegarder les données Amazon EBS des EC2 instances actives sur Amazon S3 sous forme de point-in-time snapshots et les restaurer sur des volumes EBS en veille. Pour automatiser la création, la conservation et la suppression des instantanés de volume Amazon EBS, vous pouvez utiliser Amazon Data Lifecycle Manager pour définir la fréquence des instantanés automatisés et les restaurer en fonction de vos exigences RTO/RPO.

Outils

Services AWS

- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances. EC2 Les volumes EBS se comportent comme des périphériques de stockage en mode bloc bruts non formatés. Vous pouvez monter ces volumes en tant qu'appareils sur vos instances.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que vous le souhaitez, et vous pouvez les étendre ou les intégrer.
- Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud AWS. Il fournit une capacité redimensionnable et rentable pour une base de données relationnelle et gère les tâches d'administration de base de données courantes.
- AWS Directory Service pour Microsoft Active Directory, également connu sous le nom d'AWS Managed Microsoft AD, permet à vos charges de travail sensibles aux annuaires et à vos ressources AWS d'utiliser Microsoft Active Directory dans le cloud AWS.

Autres outils

- LRS VPSX/MFI (Micro Focus Interface), co-développé par LRS et Rocket Software, capture le résultat d'une bobine JES de Rocket Enterprise Server et le transmet de manière fiable à une destination d'impression spécifiée.
- Le serveur LRS Directory Information Server (LRS/DIS) est utilisé pour l'authentification et l'autorisation pendant le flux de travail d'impression.
- TCP/IP-based LRS/Queue transmission agent is used by LRS VPSX/MFIpour collecter ou capturer des données d'impression via l'interface de programmation JES Print Exit de Rocket Software.
- Rocket Enterprise Server est un environnement de déploiement d'applications pour les applications mainframe. Il fournit l'environnement d'exécution pour les applications mainframe migrées ou créées à l'aide de n'importe quelle version de Rocket Software Enterprise Developer.

Épopées

Configuration du serveur Rocket Enterprise sur Amazon EC2 et déploiement d'une application batch pour mainframe

Tâche	Description	Compétences requises
Configurez Rocket Enterprise Server et déployez une application de démonstration.	Configurez Rocket Enterprise Server sur Amazon EC2, puis déployez l'application de BankDemo démonstration Rocket Software sur Amazon EC2. L' BankDemo application est une application batch sur ordinateur central qui crée puis lance une sortie d'impression.	Architecte du cloud

Configurer un serveur d'impression LRS sur Amazon EC2

Tâche	Description	Compétences requises
Obtenez une licence de produit LRS pour l'impression.	Pour obtenir une licence de produit LRS pour LRSVPSX/MFI, LRS/Queue, and LRS/DIS, contactez l'équipe de gestion des sorties LRS. Vous devez fournir les noms d'hôte des EC2 instances sur lesquelles les produits LRS seront installés.	Gagnez du plomb
Créez une instance Amazon EC2 Windows pour installer LRS VPSX/MFI.	Lancez une instance Amazon EC2 Windows en suivant les instructions de la section Lancer une EC2 instance Amazon dans la EC2 documentation Amazon. Votre instance doit répondre aux exigences matérielles et logicielles suivantes pour LRS VPSX/MFI : • Processeur : double cœur • RAM — 16 GO • Disque dur : 500 Go • EC2 Instance minimale : m5.xlarge • Système d'exploitation — Windows/Linux • Logiciel : Internet Information Service (IIS) ou Apache	Architecte du cloud

Tâche	Description	Compétences requises
	Note Les exigences matérielles et logiciell es ci-dessus sont destinées à un petit parc d'imprimantes (environ 500 à 1 000). Pour connaître toutes les exigences, consultez vos contacts LRS et AWS. Lorsque vous créez votre instance Windows, procédez comme suit : 1. Vérifiez que le nom EC2 d'hôte est le même que celui utilisé pour la licence du produit LRS. 2. Activez CGI dans Amazon en EC2 effectuant les opérations suivantes : a. Connectez-vous à votre EC2 instance en suivant les instructions de	

Tâche	Description	Compétences requises
Installez LRS VPSX/MFI sur l'instance. EC2	1. Connectez-vous à votre EC2 instance en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. 2. **Note** Ouvrez le lien vers la page de téléchargement du produit contenu dans l'e-mail LRS que vous devriez recevoir. : Les produits LRS sont distribués par transfert électroni que de fichiers (EFT). 3. Téléchargez LRS VPSX/MFI et décompressez le fichier (dossier par défaut :). `c:\LRS` 4. Lancez le programme d'installation du produit LRS depuis le dossier décompressé pour installer LRS VPSX/MFI. 5. Dans le menu Sélection ner les fonctionnalités, sélectionnez VPSX® Server (V1R3.022), puis choisisse	Architecte du cloud

Tâche	Description	Compétences requises
	z Suivant pour démarrer le processus d'installation. Vous recevrez un message de confirmation lorsque l'installation sera terminée.	
Installez LRS/Queue.	1. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans l'e-mail LRS que vous devriez recevoir, téléchargez LRS/Queue , puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS pour installer LRS/Queue.	Architecte du cloud

Tâche	Description	Compétences requises
Installez LRS/DIS.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans l'e-mail LRS que vous devriez recevoir, téléchargez LRS/DIS, puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS. 4. Dans le programme d'installation du produit LRS, développez LRS Misc Tools, sélectionnez LRS DIS, puis Next. 5. Suivez le reste des instructions du programme d'installation du produit LRS pour terminer le processus d'installation.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un groupe cible et enregistrez LRS EC2 VPSX/MFI comme cible.	Créez un groupe cible en suivant les instructions de la section Create a target group for your Network Load Balancer dans la documentation d'Elastic Load Balancing. Lorsque vous créez le groupe cible, procédez comme suit : 1. Sur la page Spécifier les détails du groupe, pour Choisir un type de cible, sélectionnez Instances. 2. Pour Protocole, choisissez TCP. 3. Pour Port, choisissez 5500. 4. Sur la page Enregistrer les cibles, dans la section Instances disponibles, sélectionnez les instances LRS EC2 VPSX/MFI.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un Network Load Balancer.	Suivez les instructions de Create a Network Load Balancer dans la documentation d'Elastic Load Balancing. Votre Network Load Balancer achemine le trafic de Rocket Enterprise Server vers LRS VPSX/MFI. EC2 Lorsque vous créez le Network Load Balancer, procédez comme suit sur la page Listeners and Routing : 1. Pour Protocol (Protocole), choisissez TCP. 2. Pour Port, choisissez 5500. 3. Pour Action par défaut, choisissez Transférer vers pour le groupe cible que vous avez créé précédemment.	Architecte du cloud

Intégrer le serveur Rocket Enterprise à LRS VPSX/MFI and LRS/Queue

Tâche	Description	Compétences requises
Configurez le serveur Rocket Enterprise pour l'intégration de LRS/Queue.	1. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon.	Architecte du cloud

Tâche	Description	Compétences requises
	2. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration de Rocket Enterprise Server. 3. Dans la barre de menu, choisissez NATIVE. 4. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO. 5. Depuis Général dans le volet de navigation de gauche, faites défiler la page vers le bas jusqu'à la section Additional pour configurer les variables d'environnement (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) afin qu'elles pointent vers LRSQ. 6. Pour LRSQ_ADDRESS, entrez l'adresse IP ou le nom DNS du Network Load Balancer que vous avez créé précédemment. 7. Pour LRSQ_PORT, entrez VPSX LRSQ Listener Port (5500). 8. Pour LRSQ_COMMAND, entrez l'emplacement du chemin de l'exécutable LRSQ.	

Tâche	Description	Compétences requises
	Note LRS prend actuellement en charge une limite maximale de 50 caractères pour les noms DNS, mais cette limite est susceptible de changer à l'avenir. Si votre nom DNS est supérieur à 50, vous pouvez utiliser l'adresse IP du Network Load Balancer comme alternative.	

Tâche	Description	Compétences requises
Configurez le serveur Rocket Enterprise pour l'intégration LRS VPSX/MFI.	1. Copiez le `VPSX_MFI_R2` dossier depuis le programme d'installation LRS VPSX/MFI vers l'emplacement du serveur Rocket Enterprise à l'adresse. `C\BANKDEMO\print` 2. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. 3. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration de Rocket Enterprise Server. 4. Dans la barre de menu, choisissez NATIVE. 5. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO. 6. Sous BANKDEMO, choisissez JES. 7. Sous JES Program Path, ajoutez le `DLL(VPSX_MFI_R2)` chemin depuis l'`C\BANKDEMO\print`emplacement.	Architecte du cloud

Configuration des imprimantes et des utilisateurs d'impression dans Rocket Enterprise Server et LRS VPSX/MFI

Tâche	Description	Compétences requises
Associez le module Rocket Software Print Exit au processus d'exécution du serveur d'impression par lots Rocket Enterprise Server.	1. Connectez-vous à votre EC2 instance Rocket Enterprise Server en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. 2. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration de Rocket Enterprise Server. 3. Dans la barre de menu, choisissez NATIVE. 4. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO. 5. Sous BANKDEMO, choisissez JES et faites défiler l'écran vers le bas jusqu'à Imprimantes. 6. Dans Imprimantes, associez le module Rocket Software Print Exit (LRSPRTE6 pour Batch) au processus d'exécution du serveur (SEP) de l'imprimante par lots Rocket Enterprise Server. Cela permet d'acheminer les	Architecte du cloud

Tâche	Description	Compétences requises
	sorties d'impression vers LRS VPSX/MFI. 7. Connectez-vous à l'interface utilisateur d'administration du serveur d'entreprise. Pour plus d'informations sur la configuration, consultez la section Utilisation de la sortie dans la documentation de Micro Focus.	

Tâche	Description	Compétences requises
Ajoutez une imprimante dans LRS VPSX/MFI.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Ouvrez l'interface Web VPSX depuis le menu Démarrer de Windows. 3. Dans le volet de navigation, sélectionnez Imprimantes. 4. Choisissez Ajouter, puis sélectionnez Ajouter une imprimante. 5. Sur la page Configuration de l'imprimante, dans Nom de l'imprimante, saisissez Local. 6. Pour VPSX ID, entrez. VPS1 7. Pour CommType, sélectionnez TCP/IP/LRSQ. 8. Pour Adresse hôte/IP, entrez l'adresse IP de l'imprimante physique que vous souhaitez ajouter. 9. Dans Appareil, entrez le nom de votre appareil. 10. Choisissez le pilote Windows ou le pilote Linux/Mac.	Architecte du cloud

Tâche	Description	Compétences requises
	11. Choisissez Ajouter.	

Tâche	Description	Compétences requises
Créez un utilisateur d'impression dans LRS VPSX/MFI.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Ouvrez l'interface Web VPSX depuis le menu Démarrer de Windows. 3. Dans le volet de navigation, choisissez Security, puis Users. 4. Dans la colonne Nom d'utilisateur, choisissez admin, puis Copier. 5. Dans la fenêtre Maintenance du profil utilisateur, pour Nom d'utilisateur, entrez un nom d'utilisateur (par exemple, PrintUser). 6. Dans Description, entrez une brève description (par exemple, Utilisateur pour le test d'impression). 7. Choisissez Mettre à jour. Cela crée un utilisateur d'impression (par exemple, PrintUser). 8. Dans le volet de navigation, sous Utilisateur, choisissez le nouvel utilisateur que vous avez créé.	Architecte du cloud

Tâche	Description	Compétences requises
	9. Dans le menu Commande, sélectionnez Sécurité. 10. Sur la page Règles de sécurité, choisissez toutes les options de sécurité de l'imprimante et de sécurité des tâches applicables, puis sélectionnez Enregistrer. 11. Pour ajouter votre nouvel utilisateur d'impression au groupe des administr ateurs, accédez au volet de navigation, choisissez Sécurité, puis sélectionnez Configurer. 12. Dans la fenêtre de configuration de la sécurité, ajoutez votre nouvel utilisateur d'impression dans la colonne Administr ateur.	

Configuration de l'authentification et de l'autorisation d'impression

Tâche	Description	Compétences requises
Créez un domaine Microsoft AD géré par AWS avec des utilisateurs et des groupes.	1. Créez un Active Directory sur AWS Managed Microsoft AD en suivant les instructions de la section Créer votre répertoire AWS Managed Microsoft AD dans la documentation AWS Directory Service.	Architecte du cloud

Tâche	Description	Compétences requises
	2. Déployez une EC2 instance (gestionnaire Active Directory) et installez les outils Active Directory pour gérer votre AWS Managed Microsoft AD en suivant les instructions de l'étape 3 : Déployer une EC2 instance pour gérer votre AWS Managed Microsoft AD dans la documentation AWS Directory Service. 3. **Note** Connectez-vous à votre EC2 instance en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. : Lorsque vous vous connectez à l' EC2 instance, entrez vos informations d'identification d'administrateur (pour le répertoire que vous avez créé à la première étape) dans la fenêtre de sécurité Windows.	

Tâche	Description	Compétences requises
	4. Dans le menu Démarrer de Windows, sous Outils d'administration Windows, sélectionnez Utilisateurs et ordinateurs Active Directory . 5. Créez un utilisateur d'impression dans le domaine Active Directory en suivant les étapes décrites dans la section Créer un utilisateur dans la documentation du service AWS Directory.	
Associez LRS VPSX/MFI EC2 à un domaine Microsoft AD géré par AWS.	Associez LRS VPSX/MFI EC2 à votre domaine Microsoft AD géré par AWS automatiquement (documentation du centre de connaissances AWS) ou manuellement (documentation AWS Directory Service).	Architecte du cloud

Tâche	Description	Compétences requises
Configurez et intégrez LRS/DIS à AWS Managed Microsoft AD.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, choisissez Security, puis Configure. 4. Sur la page Configuration de la sécurité, dans la section Paramètres de sécurité, pour Type de sécurité, sélectionnez Interne. 5. Entrez vos préférences pour les autres options dans la section Paramètres de sécurité. 6. Ouvrez le dossier LRS Output Management dans le menu Démarrer de Microsoft Windows, choisissez Server Start, puis Server Stop. 7. Connectez-vous à LRS VPSX/MFI à l'aide de votre nom d'utilisateur et de	Architecte du cloud

Tâche	Description	Compétences requises
	votre mot de passe Active Directory.	

Tester un flux de travail d'impression

Tâche	Description	Compétences requises
Lancez une demande d'impression par lots depuis l' BankDemo application Rocket Software.	1. Ouvrez l'émulateur de terminal 3270 dans votre instance Rocket Enterprise Server EC2 . 2. Connectez-vous à l' BankDemo application en exécutant la commande suivante : `connect 127.0.0.1:9278` 3. Sur l'interface de ligne de BankDemo commande, pour ID utilisateur, entrez B0001. Dans le champ Mot de passe, entrez une clé non vide. 4. Pour l'option Demander l'impression de relevés, entrez X sur la ligne vide. 5. Dans la section Envoyer l'instruction par, pour Mail, entrez Y, puis appuyez sur F10.	Ingénieur de test
Vérifiez la sortie d'impression dans LRS VPSX/MFI.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect	Ingénieur de test

Tâche	Description	Compétences requises
	to your instance dans la documentation Amazon. EC2 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, choisissez Imprimantes, puis choisissez Output Queue. 4. Dans la colonne Spool ID, choisissez l'ID de spool pour la demande dans la file d'attente de l'imprimante. 5. Dans l'onglet Actions, dans la colonne COMMANDE, choisissez Parcourir. Vous pouvez maintenant voir la sortie imprimée d'un relevé de compte avec des colonnes pour le numéro de compte. , Description, date, montant et solde. Pour un exemple, consultez la pièce jointe batch_print_output pour ce modèle.	

Ressources connexes

- Modernisation des sorties LRS (documentation LRS)
- Commandes ANSI et du chariot de machines (documentation IBM)

- Mots de commande des canaux (documentation IBM)
- Optimisation des charges de travail du mainframe d'entreprise sur AWS avec Micro Focus (blog du réseau de partenaires AWS)
- Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager (documentation AWS Prescriptive Guidance)
- Flux de données de présentation des fonctions avancées (AFP) (documentation IBM)
- Flux de données conditionné par ligne (LCDS) (documentation Compart)

Informations supplémentaires

Considérations

Au cours de votre processus de modernisation, vous pouvez envisager une grande variété de configurations pour les processus par lots du mainframe et les résultats qu'ils génèrent. La plate-forme centrale a été personnalisée par chaque client et fournisseur qui l'utilise avec des exigences particulières qui ont une incidence directe sur l'impression. Par exemple, votre plateforme actuelle peut intégrer l'IBM Advanced Function Presentation (AFP) ou le Xerox Line Condition Data Stream (LCDS) dans le flux de travail actuel. En outre, les caractères de commande du chariot central et les mots de commande des canaux peuvent affecter l'apparence de la page imprimée et nécessiter un traitement spécial. Dans le cadre du processus de planification de la modernisation, nous vous recommandons d'évaluer et de comprendre les configurations de votre environnement d'impression spécifique.

Capture de données d'impression

Rocket Software Print Exit transmet les informations nécessaires pour permettre à LRS VPSX/MFI de traiter efficacement le fichier spool. Les informations se composent de champs transmis dans les blocs de contrôle appropriés, tels que :

- NOM DU POSTE
- PROPRIÉTAIRE (IDENTIFIANT UTILISATEUR)
- DESTINATION
- FORMULAIRE
- NOM DE FICHIER
- ÉCRIVAIN

Le LRS VPSX/MFI prend en charge les mécanismes de traitement par lots du mainframe suivants pour capturer des données depuis Rocket Enterprise Server.

- Déclarations COBOL print/spool processing using standard z/OS JCL SYSOUT DD/OUTPUT BATCH
- Instructions BATCH COBOL print/spool processing using standard z/OS JCL CA-SPOOL SUBSYS DD
- IMS/COBOL print/spooltraitement à l'aide de l'interface CBLTDLI (pour une liste complète des méthodes prises en charge et des exemples de programmation, consultez la documentation LRS incluse dans la licence de votre produit.)

Contrôles de santé du parc d'imprimantes

Le LRS VPSX/MFI (LRS LoadX) peut effectuer des contrôles de santé approfondis, y compris la gestion des appareils et l'optimisation opérationnelle. La gestion des périphériques permet de détecter les défaillances d'une imprimante et d'acheminer la demande d'impression vers une imprimante saine. Pour plus d'informations sur les contrôles approfondis de l'état des flottes d'imprimantes, consultez la documentation LRS incluse dans la licence de votre produit.

Authentification et autorisation d'impression

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DISpeut également appliquer des contrôles de sécurité d'impression de niveau granulaire dans les cas d'utilisation suivants :

- Gérez les personnes autorisées à parcourir la tâche d'impression.
- Gérez le niveau de navigation des jobs des autres utilisateurs.
- Gérez les tâches opérationnelles. Par exemple, sécurité au niveau des commandes, telle que maintenir/relâcher, purger, modifier, copier et rediriger. La sécurité peut être configurée par l'ID utilisateur ou par le groupe (similaire au groupe AD ou au groupe LDAP).

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Modernisation du mainframe : DevOps activée AWS avec Rocket Software Enterprise Suite

Créée par Kevin Yung (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Les défis des clients

Organisations qui exécutent des applications de base sur du matériel mainframe rencontrent généralement quelques difficultés lorsque le matériel doit évoluer pour répondre aux exigences des innovations numériques. Ces défis incluent les contraintes suivantes.

- Les environnements de développement et de test du mainframe ne peuvent pas évoluer en raison de la rigidité des composants matériels du mainframe et du coût élevé des modifications.
- Le développement d'ordinateurs centraux fait face à des pénuries de compétences, car les nouveaux développeurs ne sont pas habitués aux outils de développement de mainframe traditionnels et ne s'y intéressent pas. Les technologies modernes telles que les conteneurs, les pipelines integration/continuous delivery (CI/CD (continus) et les frameworks de test modernes ne sont pas disponibles pour le développement de mainframes.

Résultats du modèle

Pour relever ces défis, Amazon Web Services (AWS) et Rocket Software Micro Focus, un partenaire AWS Partner Network (APN), ont collaboré pour créer ce modèle. La solution est conçue pour vous aider à atteindre les résultats suivants.

- Productivité améliorée des développeurs. Les développeurs peuvent recevoir de nouvelles instances de développement de mainframe en quelques minutes.
- Utilisation du AWS Cloud pour créer de nouveaux environnements de test de mainframe avec une capacité pratiquement illimitée.
- Provisionnement rapide de la nouvelle infrastructure CI/CD du mainframe. Le provisionnement AWS peut être effectué en une heure à l'aide de AWS CloudFormation et AWS Systems Manager.

- Utilisation native d' AWS DevOps outils pour le développement de mainframes, notamment, AWS CodeBuild, AWS CodeCommit AWS CodePipeline AWS CodeDeploy, et Amazon Elastic Container Registry (Amazon ECR).
- Transformez le développement en cascade traditionnel en développement agile dans les projets mainframe.

Résumé des technologies

Dans ce modèle, la pile cible contient les composants suivants.

Composants logiques	Solutions de mise en œuvre	Description
Référentiels de code source	AccuRev Serveur logiciel Rocket CodeCommit, Amazon ECR	Gestion du code source : la solution utilise deux types de code source : • Code source du mainframe , par exemple COBOL et JCL. • AWS modèles d'infrast ructure et scripts d'automat isation Les deux types de code source nécessitent un contrôle de version, mais ils sont gérés différemment SCMs. Le code source déployé sur le mainframe ou les serveurs Rocket Software Enterprise est géré dans Rocket Software Micro Focus AccuRev Server. AWS les modèles et les scripts d'automatisation sont gérés dans CodeCommit. Amazon

		ECR est utilisé pour les référentiels d'images Docker.
Instances de développeurs d'entreprise	Amazon Elastic Compute Cloud (Amazon EC2), développeur Rocket Software Enterprise pour Eclipse	Les développeurs de mainframe peuvent développer du code sur Amazon en EC2 utilisant Rocket Software Enterprise Developer for Eclipse. Ainsi, il n'est plus nécessaire de recourir au matériel du mainframe pour écrire et tester le code.
Gestion des licences de Rocket Software Enterprise Suite	License Manager de Rocket Software Enterprise Suite	Pour une gestion et une gouvernance centralisées des licences Rocket Software Enterprise Suite, la solution utilise Rocket Software Enterprise Suite License Manager pour héberger la licence requise.
Canalisations CI/CD	CodePipeline, CodeBuild, CodeDeploy, Rocket Software Enterprise Developer dans un conteneur, Rocket Software Enterprise Test Server dans un conteneur, Rocket Software Micro Focus Enterprise Server	Les équipes de développement de mainframe ont besoin de pipelines CI/CD pour effectuer la compilation du code, les tests d'intégration et les tests de régression. Dans AWS CodePipeline et CodeBuild peut fonctionner avec Rocket Software Enterprise Developer et Enterprise Test Server dans un conteneur de manière native.

Conditions préalables et limitations

Prérequis

Name (Nom)	Description
py3270	py3270 est une interface Python pour x3270, un émulateur de terminal IBM 3270. Il fournit une API à un sous-processus x3270 ou s3270.
x3270	x3270 est un émulateur de terminal IBM 3270 pour le système X Window et Windows. Cela peut être utilisé par le développeur pour des tests unitaires en local.
Bibliothèque Robot-Framework-Mainframe-3270	Mainframe3270 est une bibliothèque pour Robot Framework basée sur le projet py3270.
Logiciel Rocket Verastream	Rocket Software Verastream est une plateforme d'intégration qui permet de tester les actifs du mainframe de la même manière que les applications mobiles, les applications Web et les services Web SOA.
Programme d'installation et licence de Rocket Software Unified Functional Testing (UFT)	Rocket Software Unified Functional Testing est un logiciel qui fournit une automatisation des tests fonctionnels et de régression pour les applications et les environnements logiciels.
Programme d'installation et licence de Rocket Software Enterprise Server	Enterprise Server fournit l'environnement d'exécution pour les applications mainframe.
Programme d'installation et licence du serveur de test Rocket Software Enterprise	Rocket Software Enterprise Test Server est un environnement de test d'applications mainframe IBM.
Programme d' AccuRev installation et licence de Rocket Software pour le serveur, et programme d' AccuRev installation et	AccuRev fournit la gestion du code source (SCM). Le AccuRev système est conçu pour

licence Rocket Software Micro Focus pour les systèmes d'exploitation Windows et Linux	être utilisé par une équipe de personnes qui développent un ensemble de fichiers.
Rocket Software Enterprise Developer pour le programme d'installation, le correctif et la licence d'Eclipse	Enterprise Developer fournit aux développeurs de mainframe une plate-forme leur permettan t de développer et de gérer les principales applications en ligne et par lots du mainframe.

Limites

- La création d'une image Windows Docker n'est pas prise en charge dans CodeBuild. Ce problème signalé nécessite l'assistance des équipes Windows Kernel/HCS et Docker. La solution consiste à créer un runbook de génération d'images Docker à l'aide de Systems Manager. Ce modèle utilise la solution de contournement pour créer des images de conteneur Rocket Software Enterprise Developer for Eclipse et Rocket Software Micro Focus Enterprise Test Server Container.
- La connectivité au cloud privé virtuel (VPC) depuis n' CodeBuild est pas encore prise en charge sous Windows. Le modèle n'utilise donc pas Rocket Software License Manager pour gérer les licences dans les conteneurs OpenText Rocket Software Enterprise Developer et Rocket Software Enterprise Test Server.

Versions du produit

- Rocket Software Enterprise Developer 5.5 ou version ultérieure
- Rocket Software Enterprise Test Server 5.5 ou version ultérieure
- Rocket Software Enterprise Server 5.5 ou version ultérieure
- Rocket Software AccuRev 7.x ou version ultérieure
- Image de base Windows Docker pour Rocket Software Enterprise Developer et Enterprise Test Server : microsoft/dotnet-framework-4.7.2-runtime
- Image de base de Linux Docker pour le AccuRev client : amazonlinux:2

Architecture

Environnement mainframe

Dans le cadre du développement d'un mainframe classique, les développeurs doivent utiliser le matériel du mainframe pour développer et tester des programmes. Ils sont confrontés à des limites de

capacité, par exemple à un million d'instructions par seconde (MIPS) restreint pour l'environnement de développement/test, et ils doivent s'appuyer sur les outils disponibles sur les ordinateurs centraux.

Dans de nombreuses organisations, le développement des mainframes suit la méthodologie de développement en cascade, les équipes s'appuyant sur de longs cycles pour publier les modifications. Ces cycles de lancement sont généralement plus longs que ceux du développement de produits numériques.

Le schéma suivant montre plusieurs projets de mainframe partageant du matériel mainframe pour leur développement. Dans le domaine du matériel mainframe, il est coûteux d'étendre un environnement de développement et de test à un plus grand nombre de projets.

Architecture AWS

Ce modèle étend le développement du mainframe au AWS Cloud. Tout d'abord, il utilise AccuRev SCM pour héberger le code source du mainframe. AWS Il met ensuite le développeur d'entreprise et le serveur de test d'entreprise à disposition pour créer et tester le code du mainframe. AWS

Les sections suivantes décrivent les trois principaux composants du modèle.

1. SCM

Dans AWS, le modèle est utilisé AccuRev pour créer un ensemble d'espaces de travail SCM et de contrôle de version pour le code source du mainframe. Son architecture basée sur les flux permet le développement parallèle de mainframes pour plusieurs équipes. Pour fusionner une modification, utilisez AccuRev le concept de promotion. Pour ajouter cette modification à d'autres espaces de travail, AccuRev utilise le concept de mise à jour.

Au niveau du projet, chaque équipe peut créer un ou plusieurs flux AccuRev pour suivre les changements au niveau du projet. C'est ce que l'on appelle les flux de projets. Ces flux de projet sont hérités du même flux parent. Le flux parent est utilisé pour fusionner les modifications des différents flux de projet.

Chaque flux de projet peut promouvoir le code vers AccuRev, et un déclencheur de publication de promotion est configuré pour lancer le pipeline AWS CI/CD. La génération réussie d'une modification de flux de projet peut être promue vers son flux parent pour d'autres tests de régression.

Généralement, le flux parent est appelé flux d'intégration du système. Lorsqu'il y a une promotion d'un flux de projet vers un flux d'intégration du système, un déclencheur de post-promotion lance un autre pipeline CI/CD pour exécuter des tests de régression.

Outre le code mainframe, ce modèle inclut des AWS CloudFormation modèles, des documents Systems Manager Automation et des scripts. Conformément aux infrastructure-as-code meilleures pratiques, leur version est contrôlée dans. CodeCommit

Si vous devez resynchroniser le code du mainframe avec un environnement mainframe à des fins de déploiement, Rocket Software fournit la solution Enterprise Sync, qui synchronise le code du AccuRev SCM vers le SCM du mainframe.

2. Environnements de développement et de test

Dans une grande entreprise, il est difficile de faire évoluer plus d'une centaine, voire plus d'un millier de développeurs mainframe. Pour répondre à cette contrainte, le modèle utilise des instances Amazon EC2 Windows pour le développement. Sur les instances, les outils Enterprise Developer for Eclipse sont installés. Le développeur peut effectuer tous les tests de code du mainframe et le débogage localement sur l'instance.

AWS Systems Manager Les documents State Manager et Automation sont utilisés pour automatiser le provisionnement des instances de développement. Le délai moyen de création d'une instance de développeur est de 15 minutes. Les logiciels et configurations suivants sont préparés :

- AccuRev Client Windows pour extraire et valider le code source dans AccuRev
- Outil Enterprise Developers for Eclipse, pour écrire, tester et déboguer du code mainframe en local
- Frameworks de test open source Le framework de test de développement piloté par le comportement (BDD) en Python Behave, py3270, et l'émulateur x3270 pour créer des scripts pour tester des applications
- Un outil de développement Docker permettant de créer l'image Docker du serveur de test d'entreprise et de tester l'application dans le conteneur Docker du serveur de test d'entreprise

Au cours du cycle de développement, les développeurs utilisent l' EC2 instance pour développer et tester le code du mainframe localement. Lorsque les modifications locales sont testées avec succès, les développeurs les promeuvent sur le AccuRev serveur.

3. Canalisations CI/CD

Dans le modèle, les pipelines CI/CD sont utilisés pour les tests d'intégration et les tests de régression avant le déploiement dans l'environnement de production.

Comme expliqué dans la section SCM, AccuRev utilise deux types de flux : un flux de projet et un flux d'intégration. Chaque flux est connecté à des pipelines CI/CD. Pour effectuer l'intégration entre le AccuRev serveur et AWS CodePipeline, le modèle utilise un script de AccuRev post-promotion pour créer un événement permettant de lancer le CI/CD.

Par exemple, lorsqu'un développeur promeut une modification d'un flux de projet dans AccuRev, il lance un script de post-promotion à exécuter dans AccuRev Server. Le script télécharge ensuite les métadonnées de la modification dans un compartiment Amazon Simple Storage Service (Amazon S3) afin de créer un événement Amazon S3. Cet événement lancera l'exécution d'un pipeline CodePipeline configuré.

Le même mécanisme de déclenchement d'événements est utilisé pour le flux d'intégration et ses pipelines associés.

Dans le pipeline CI/CD, CodePipeline utilise CodeBuild le conteneur client AccuRev Linux pour extraire le code le plus récent des AccuRev flux. Ensuite, le pipeline commence CodeBuild à utiliser le conteneur Windows Enterprise Developer pour compiler le code source et à utiliser le conteneur Windows Enterprise Test Server CodeBuild pour tester les applications mainframe.

Le CI/CD pipelines are built using CloudFormation templates, and the blueprint will be used for new projects. By using the templates, it takes less than an hour for a project to create a new CI/CD pipeline entre AWS.

Pour étendre les capacités de test de votre mainframe AWS, le modèle intègre la suite de DevOps tests Rocket Software, Verastream et le serveur UFT. En utilisant les DevOps outils modernes, vous pouvez exécuter autant de tests AWS que vous le souhaitez.

Un exemple d'environnement de développement mainframe avec Rocket Software activé AWS est illustré dans le schéma suivant.

Pile technologique cible

Cette section examine de plus près l'architecture de chaque composant du modèle.

1. Référentiel de code source — AccuRev SCM

AccuRev SCM est configuré pour gérer les versions du code source du mainframe. Pour une haute disponibilité, AccuRev prend en charge les modes principal et réplica. Les opérateurs peuvent basculer vers la réplique lorsqu'ils effectuent des opérations de maintenance sur le nœud principal.

Pour accélérer la réponse du pipeline CI/CD, le modèle utilise Amazon CloudWatch Events pour détecter les modifications du code source et lancer le démarrage du pipeline.

1. Le pipeline est configuré pour utiliser une source Amazon S3.
2. Une règle d' CloudWatch événements est configurée pour capturer les événements S3 à partir d'un compartiment S3 source.
3. La règle CloudWatch Events définit une cible pour le pipeline.
4. AccuRev SCM est configuré pour exécuter un script de post-promotion localement une fois la promotion terminée.
5. AccuRev SCM génère un fichier XML contenant les métadonnées de la promotion, et le script télécharge le fichier XML dans le compartiment S3 source.
6. Après le téléchargement, le compartiment S3 source envoie des événements conformes à la règle CloudWatch Events, et la règle CloudWatch Events lance l'exécution du pipeline.

Lorsque le pipeline s'exécute, il lance un CodeBuild projet visant à utiliser un conteneur client AccuRev Linux pour extraire le dernier code du mainframe à partir d'un flux associé AccuRev .

Le schéma suivant montre une configuration AccuRev de serveur.

2. Modèle de développeur d'entreprise

Le modèle utilise des EC2 modèles Amazon pour simplifier la création de l'instance de développeur. En utilisant State Manager, il peut appliquer les paramètres logiciels et de licence aux EC2 instances de manière cohérente.

Le EC2 modèle Amazon intègre ses paramètres de contexte VPC et ses paramètres d'instance par défaut, et il répond aux exigences de balisage de l'entreprise. À l'aide d'un modèle, une équipe peut créer ses propres nouvelles instances de développement.

Lorsqu'une instance de développeur démarre, en l'associant à des balises, Systems Manager utilise State Manager pour appliquer l'automatisation. L'automatisation comprend les étapes générales suivantes.

1. Installez le logiciel Enterprise Developer et installez les correctifs.

2. Installez le AccuRev client pour Windows.
3. Installez le script préconfiguré permettant aux développeurs de rejoindre le AccuRev stream. Initialisez les espaces de travail Eclipse.
4. Installez des outils de développement, notamment x3270, py3270 et Docker.
5. Configurez les paramètres de licence pour qu'ils pointent vers un équilibreur de charge License Manager.

Le schéma suivant montre une instance de développeur d'entreprise créée par le EC2 modèle Amazon, avec le logiciel et la configuration appliqués à l'instance par State Manager. Les instances de développeurs d'entreprise se connectent AWS License Manager pour activer leur licence.

3. Canalisations CI/CD

Comme expliqué dans la section sur AWS l'architecture, dans le modèle, il existe des CI/CD pipelines and system integration pipelines. Each mainframe project team creates a pipeline or multiple CI/CD pipelines for building the programs that they are developing in a project. These project CI/CD pipelines au niveau du projet qui extraient le code source d'un flux associé AccuRev .

Dans une équipe de projet, les développeurs font la promotion de leur code dans le AccuRev flux associé. La promotion lance ensuite le pipeline du projet pour créer le code et exécuter des tests d'intégration.

Chaque pipeline CI/CD de projet utilise des CodeBuild projets dotés de l'outil Enterprise Developer Amazon ECR image et de l'outil Enterprise Test Server Amazon ECR image.

CodePipeline et CodeBuild sont utilisés pour créer les pipelines CI/CD. Parce que CodeBuild , sans frais ni engagements initiaux, vous ne payez que pour ce que vous utilisez. CodePipeline Par rapport au matériel mainframe, la AWS solution réduit considérablement les délais de mise en service du matériel et réduit le coût de votre environnement de test.

Dans le développement moderne, plusieurs méthodologies de test sont utilisées. Par exemple, le développement piloté par les tests (TDD), le BDD et le Robot Framework. Avec ce modèle, les développeurs peuvent utiliser ces outils modernes pour tester le mainframe. Par exemple, en utilisant x3270, py3270 et l'outil de test Behave python, vous pouvez définir le comportement d'une application en ligne. Vous pouvez également utiliser le framework robot build mainframe 3270 dans ces pipelines CI/CD.

Le schéma suivant montre le pipeline CI/CD Team Stream.

Le schéma suivant montre le rapport de test CI/CD du projet produit par CodePipeline Mainframe3270 Robot Framework.

Le schéma suivant montre le rapport de test CI/CD du projet produit par CodePipeline in Py3270 et Behave BDD.

Une fois les tests réussis au niveau du projet, le code testé est manuellement promu dans le flux d'intégration dans AccuRev SCM. Vous pouvez automatiser cette étape une fois que les équipes auront confiance dans la couverture des tests de leur pipeline de projets.

Lorsque le code est promu, le pipeline CI/CD d'intégration du système extrait le code fusionné et effectue des tests de régression. Le code fusionné est promu à partir de tous les flux de projets parallèles.

En fonction de la finesse requise pour l'environnement de test, les clients peuvent disposer d'un plus grand nombre de pipelines CI/CD d'intégration système dans un environnement différent, par exemple UAT ou pré-production.

Dans le modèle, les outils utilisés dans le pipeline d'intégration du système sont Enterprise Test Server, UFT Server et Verastream. Tous ces outils peuvent être déployés dans le conteneur Docker et utilisés avec CodeBuild.

Après avoir testé avec succès les programmes du mainframe, l'artefact est stocké, avec contrôle de version, dans un compartiment S3.

Le schéma suivant montre un pipeline CI/CD d'intégration du système.

Une fois que l'artefact a été testé avec succès dans les pipelines CI/CD d'intégration du système, il peut être promu pour un déploiement en production.

Si vous devez redéployer le code source sur le mainframe, Rocket Software propose la solution Enterprise Sync pour synchroniser le code source depuis Mainframe AccuRev Endeavour.

Le schéma suivant montre un pipeline CI/CD de production déployant l'artefact sur des serveurs d'entreprise. Dans cet exemple, CodeDeploy orchestre le déploiement de l'artefact mainframe testé dans Enterprise Server.

Outre la présentation de l'architecture du pipeline CI/CD, consultez le billet de AWS DevOps blog Automatisez des milliers de tests de mainframe AWS avec la suite Micro Focus Enterprise pour plus d'informations sur le test d'applications mainframe dans et. CodeBuild CodePipeline (Micro Focus s'appelle désormais Rocket Software.) Consultez le billet de blog pour connaître les meilleures pratiques et les détails relatifs à la réalisation de tests sur mainframe sur AWS.

Outils

AWS outils d'automatisation

- AWS CloudFormation
- CloudWatch Événements Amazon
- AWS CodeBuild
- AWS CodeDeploy
- AWS CodePipeline
- Amazon ECR
- Amazon S3
- AWS Secrets Manager
- AWS Systems Manager

Outils Rocket Software

- Développeur Rocket Enterprise pour Eclipse
- Serveur de test Rocket Enterprise
- Rocket Enterprise Server (déploiement en production)
- Logiciel Rocket AccuRev
- License Manager de Rocket Software Enterprise Suite
- Intégrateur hôte Verastream de Rocket Software
- Logiciel Rocket UFT One

Autres outils

- x3270
- py3270
- Bibliothèque Robot-Framework-Mainframe-3270

Épopées

Création de l' AccuRev infrastructure SCM

Tâche	Description	Compétences requises
Déployez un serveur AccuRev SCM principal à l'aide CloudFormation de.		AWS CloudFormation
Créez l'utilisateur AccuRev administrateur.	Connectez-vous au serveur AccuRev SCM et exécutez la commande CLI pour créer un utilisateur administrateur.	AccuRev Administrateur du serveur SCM
Créez des AccuRev streams.	Créez des AccuRev flux qui héritent des flux supérieur s dans l'ordre : production, intégration du système, flux d'équipe.	AccuRev Administrateur SCM
Créez les comptes de AccuRev connexion des développeurs.	Utilisez les commandes de la CLI AccuRev SCM pour créer des comptes de connexion AccuRev utilisateur pour les développeurs de mainframe.	AccuRev Administrateur SCM

Créez le modèle de EC2 lancement Amazon pour les développeurs d'entreprise

Tâche	Description	Compétences requises
Déployez le modèle de EC2 lancement Amazon en utilisant CloudFormation.	CloudFormation À utiliser pour déployer un modèle de EC2 lancement Amazon pour les instances Enterpris e Developer. Le modèle inclut un document Systems Manager Automation pour l'instance Rocket Enterprise Developer.	AWS CloudFormation
Créez l'instance Enterprise Developer à partir du EC2 modèle Amazon.		Connexion à la console AWS et compétences de développe ur de mainframe

Création de l'image Docker de l'outil Enterprise Developer

Tâche	Description	Compétences requises
Créez l'image Docker de l'outil Enterprise Developer.	Utilisez la commande Docker et l'outil de développement d'entreprise Dockerfile pour créer l'image Docker.	Docker
Créez le référentiel Docker dans Amazon ECR.	Sur la console Amazon ECR, créez le référentiel pour l'image Docker du développe ur d'entreprise.	Amazon ECR
Transférez l'image Docker de l'outil Enterprise Developer sur Amazon ECR.	Exécutez la commande Docker push pour envoyer l'image Docker de l'outil Enterprise Developer afin de	Docker

Tâche	Description	Compétences requises
	l'enregistrer dans le référentiel Docker d'Amazon ECR.	

Création de l'image Docker du serveur de test d'entreprise

Tâche	Description	Compétences requises
Créez l'image Docker du serveur de test d'entreprise.	Utilisez la commande Docker et le fichier Dockerfile du serveur de test d'entreprise pour créer l'image Docker.	Docker
Créez le référentiel Docker dans Amazon ECR.	Sur la console Amazon ECR, créez le référentiel Amazon ECR pour l'image Docker du serveur de test d'entreprise.	Amazon ECR
Transférez l'image Docker du serveur de test d'entreprise vers Amazon ECR.	Exécutez la commande Docker push pour envoyer et enregistrer l'image Docker du serveur de test d'entreprise dans Amazon ECR.	Docker

Création du pipeline CI/CD Team Stream

Tâche	Description	Compétences requises
Créez le CodeCommit référentiel.	Sur la CodeCommit console, créez un référentiel Git pour l'infrastructure et le CloudFormation code.	AWS CodeCommit
Téléchargez le CloudFormation modèle et le code	Exécutez la commande Git push pour télécharger le CloudFormation modèle et le	Git

Tâche	Description	Compétences requises
d'automatisation dans le CodeCommit référentiel.	code d'automatisation dans le référentiel.	
Déployez le pipeline CI/CD Team Stream en utilisant. CloudFormation	Utilisez le CloudFormation modèle préparé pour déployer un pipeline CI/CD Team Stream.	AWS CloudFormation

Création du pipeline CI/CD d'intégration du système

Tâche	Description	Compétences requises
Créez l'image UFT Docker.	Utilisez la commande Docker et le Dockerfile UFT pour créer l'image Docker.	Docker
Créez le référentiel Docker dans Amazon ECR pour l'image UFT.	Sur la console Amazon ECR, créez le référentiel Docker pour l'image UFT.	Amazon ECR
Transférez l'image UFT Docker vers Amazon ECR.	Exécutez la commande Docker push pour envoyer et enregistrer l'image Docker du serveur de test d'entreprise dans Amazon ECR.	Docker
Créez l'image Docker de Verastream.	Utilisez la commande Docker et le Dockerfile Verastream pour créer l'image Docker.	Docker
Créez le référentiel Docker dans Amazon ECR pour l'image Verastream.	Sur la console Amazon ECR, créez le référentiel Docker pour l'image Verastream.	Amazon ECR

Tâche	Description	Compétences requises
Déployez le pipeline CI/CD d'intégration du système en utilisant. CloudFormation	Utilisez le CloudFormation modèle préparé pour déployer un pipeline CI/CD d'intégration du système.	AWS CloudFormation

Création d'un pipeline CI/CD de déploiement en production

Tâche	Description	Compétences requises
Déployez Enterprise Server à l'aide du AWS Quick Start.	Pour déployer un serveur d'entreprise à l'aide de CloudFormation, lancez le serveur d'entreprise sur AWS Quick Start.	AWS CloudFormation
Déployez un pipeline CI/CD de déploiement en production.	Sur la CloudFormation console, utilisez le CloudForm ation modèle pour déployer un pipeline CI/CD de déploiement de production.	AWS CloudFormation

Ressources connexes

Références

- AWS DevOps Blog - Automatisez des milliers de tests de mainframe AWS avec la suite Micro Focus Enterprise (Micro Focus s'appelle désormais Rocket Software).
- Dépôt py3270/py3270 GitHub
- Référentiel Altran-PT-GDC/Robot-Framework-Mainframe-3270-Library GitHub
- Bienvenue chez Behave !
- Blog des partenaires APN - Tag : Micro Focus (Micro Focus est désormais Rocket Software.)
- Lancement d'une instance à partir d'un modèle de lancement

AWS Marketplace

- Logiciel Rocket UFT One

AWS Quick Start

- Serveur Rocket Enterprise activé AWS

Modernisez les charges de travail d'impression en ligne du mainframe sur AWS à l'aide de Micro Focus Enterprise Server et de LRS VPSX/MFI

Créée par Shubham Roy (AWS), Abraham Rondon (Micro Focus), Guy Tucker (Levi, Ray and Shoup Inc) et Kevin Yung (AWS)

Récapitulatif

Ce modèle vous montre comment moderniser les charges de travail d'impression en ligne critiques de votre mainframe sur le cloud Amazon Web Services (AWS) en utilisant Micro Focus Enterprise Server comme environnement d'exécution pour une application mainframe modernisée et LRS VPSX/MFI (Micro Focus Interface) comme serveur d'impression. Le modèle est basé sur l'approche de modernisation du mainframe replateforme. Dans cette approche, vous migrez votre application en ligne de mainframe vers Amazon Elastic Compute Cloud (Amazon EC2) et vous migrez votre base de données mainframe, telle qu'IBM DB2 pour z/OS, vers Amazon Relational Database Service (Amazon RDS). L'authentification et l'autorisation pour le flux de travail d'impression modernisé sont effectuées par AWS Directory Service pour Microsoft Active Directory, également connu sous le nom d'AWS Managed Microsoft AD. Le serveur d'informations d'annuaire LRS (LRS/DIS) est intégré à AWS Managed Microsoft AD pour l'authentification et l'autorisation du flux de travail d'impression. En modernisant vos charges de travail d'impression en ligne, vous pouvez réduire les coûts d'infrastructure informatique, atténuer la dette technique liée à la maintenance des systèmes existants, supprimer les silos de données, accroître l'agilité et l'efficacité grâce à un DevOps modèle et tirer parti des ressources à la demande et de l'automatisation dans le cloud AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Charge de travail d'impression ou de gestion des sorties en ligne sur ordinateur central
- Connaissances de base sur la façon de reconstruire et de fournir une application mainframe qui s'exécute sur Micro Focus Enterprise Server (pour plus d'informations, consultez la fiche technique du serveur Enterprise dans la documentation Micro Focus.)
- Connaissances de base des solutions et des concepts d'impression cloud LRS (pour plus d'informations, voir Modernisation des sorties dans la documentation LRS.)
- Logiciel et licence Micro Focus Enterprise Server (pour plus d'informations, contactez le service commercial de Micro Focus.)

- VPSX/MFI, LRS/Queue, and LRS/DISLogiciels et licences LRS (Pour plus d'informations, contactez le service commercial LRS.)

> **Note**
>
> Pour plus d'informations sur les considérations relatives à la configuration des charges de travail d'impression en ligne du mainframe, consultez la section Considérations de la section Informations supplémentaires de ce modèle.

Versions du produit

- Micro Focus Enterprise Server 8.0 ou version ultérieure
- LRS VPSX/MFI V1R3 ou version ultérieure

Architecture

Pile technologique source

- Système d'exploitation — IBM z/OS
- Langage de programmation — Langage orienté métier commun (COBOL) et système de contrôle des informations clients (CICS)
- Base de données — IBM DB2 pour z/OS Système de gestion de l'information (IMS) IBM pour z/OS et méthode d'accès au stockage virtuel (VSAM)
- Sécurité : Resource Access Control Facility (RACF), CA Top Secret pour z/OS et Access Control Facility 2 () ACF2
- Gestion de l'impression et de la sortie : produits d'impression IBM mainframe z/OS (IBM Infoprint Server pour z/OS, LRS et CA View)

Pile technologique cible

- Système d'exploitation — Microsoft Windows Server exécuté sur Amazon EC2
- Calcul — Amazon EC2
- Langage de programmation — COBOL et CICS
- Base de données — Amazon RDS

- Sécurité — Microsoft AD géré par AWS
- Gestion de l'impression et de la sortie : solution d'impression LRS sur AWS
- Environnement d'exécution du mainframe — Micro Focus Enterprise Server

Architecture de la source

Le schéma suivant montre une architecture d'état actuelle typique pour une charge de travail d'impression en ligne sur un mainframe.

Le schéma suivant illustre le flux de travail suivant :

1. Les utilisateurs effectuent des transactions commerciales sur un système d'engagement (SoE) basé sur une application IBM CICS écrite en COBOL.
2. Le SoE invoque le service mainframe, qui enregistre les données des transactions commerciales dans une base de données system-of-records (SoR) telle qu'IBM DB2 for z/OS.
3. Le SoR conserve les données commerciales provenant du SoE.
4. Un utilisateur lance une demande pour générer une sortie d'impression à partir du CICS SoE, qui lance une application de transaction d'impression pour traiter la demande d'impression.
5. L'application de transaction d'impression (telle qu'un programme CICS et COBOL) extrait les données de la base de données, les met en forme en fonction des exigences commerciales et génère des résultats commerciaux (données d'impression) tels que des relevés de facturation, des cartes d'identité ou des relevés de prêt. L'application envoie ensuite une demande d'impression à l'aide de la méthode d'accès aux télécommunications virtuelles (VTAM). Un serveur d'impression z/OS (tel qu'IBM Infoprint Server) utilise un composant VTAM NetSpool ou un composant similaire pour intercepter les demandes d'impression, puis crée des ensembles de données de sortie d'impression sur le spool JES en utilisant les paramètres de sortie JES. Les paramètres de sortie JES spécifient les informations de routage que le serveur d'impression utilise pour transmettre la sortie à une imprimante réseau spécifique. Le terme VTAM fait référence au serveur de communication z/OS et à l'élément de services SNA (System Network Architecture) de z/OS.
6. Le composant de transmission de sortie d'impression transmet les ensembles de données d'impression de sortie de la bobine JES à des imprimantes ou à des serveurs d'impression distants, tels que LRS (comme illustré dans ce modèle), IBM Infoprint Server ou des destinations de courrier électronique.

Architecture cible

Le schéma suivant montre l'architecture d'une charge de travail d'impression en ligne sur mainframe déployée dans le cloud AWS :

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur lance une demande d'impression depuis une interface utilisateur en ligne (CICS) pour créer des documents imprimés, tels que des relevés de facturation, des cartes d'identité ou des relevés de prêt.
2. L'application en ligne du mainframe (replatformée sur Amazon EC2) utilise le moteur d'exécution Micro Focus Enterprise Server pour extraire les données de la base de données de l'application, appliquer une logique métier aux données, les formater, puis les envoyer vers une destination d'impression à l'aide de Micro Focus CICS Print Exit (DFHUPRNT).
3. La base de données de l'application (un SoR qui s'exécute sur Amazon RDS) conserve les données pour l'impression.
4. Le nom de la VPSX/MFI printing solution is deployed on Amazon EC2, and its operational data is stored in Amazon Elastic Block Store (Amazon EBS). LRS VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect print data through the Micro Focus CICS Print Exit API (DFHUPRNT) and deliver the data to a specified printer destination. The original TERMID (TERM) that’s used in the modernized CICS application is used as the VPSX/MFI file d'attente LRS.

> **Note**
>
> La solution cible ne nécessite généralement pas de modifications de l'application pour s'adapter aux langages de formatage du mainframe, tels qu'IBM Advanced Function Presentation (AFP) ou Xerox Line Condition Data Stream (LCDS). Pour plus d'informations sur l'utilisation de Micro Focus pour la migration et la modernisation des applications mainframe sur AWS, consultez la section Empowering Enterprise Mainframe Workloads on AWS with Micro Focus dans la documentation AWS.

Architecture de l'infrastructure AWS

Le schéma suivant montre une architecture d'infrastructure AWS hautement disponible et sécurisée pour une charge de travail d'impression en ligne sur mainframe :

Le schéma suivant illustre le flux de travail suivant :

1. L'application en ligne pour ordinateur central (écrite dans un langage de programmation tel que CICS ou COBOL) utilise la logique métier de base pour traiter et générer des documents imprimés, tels que des relevés de facturation, des cartes d'identité et des relevés de prêt. L'application en ligne est déployée sur Amazon EC2 dans deux zones de disponibilité (AZ) pour une haute disponibilité (HA) et utilise Micro Focus CICS Print Exit pour acheminer les résultats d'impression vers LRS VPSX/MFI pour l'impression par l'utilisateur final.
2. VPSX/MFI uses a TCP/IP-based LRS/Queue transmission agent to collect or capture print data from the Micro Focus online Print Exit programming interface. Online Print Exit passes the necessary information to enable LRS VPSX/MFI to effectively process the print file and dynamically build LRS/QueueCommandes LRS.

   > **Note**
   >
   > Pour plus d'informations sur les différentes méthodes de programmation d'applications CICS pour l'impression et sur la manière dont elles sont prises en charge dans le serveur Micro Focus Enterprise et le LRS VPSX/MFI, voir Capture des données d'impression dans la section Informations supplémentaires de ce modèle.

3.
   > **Note**
   >
   > Un Network Load Balancer fournit un nom DNS pour intégrer Micro Focus Enterprise Server au LRS VPSX/MFI. : LRS VPSX/MFI supports a Layer 4 load balancer. The Network Load Balancer also does a basic health check on LRS VPSX/MFI et achemine le trafic vers les cibles enregistrées qui sont saines.

4. Le serveur d'impression LRS VPSX/MFI est déployé EC2 sur Amazon dans deux zones de disponibilité pour HA et utilise Amazon EBS comme magasin de données opérationnel. VPSX/MFI supports both the active-active and active-passive service modes. This architecture uses multiple Availability Zones in an active-passive pair as an active and hot standby. The Network Load Balancer performs a health check on LRS VPSX/MFI EC2 Instances LRS et achemine le trafic vers des instances en veille active situées dans une autre zone de disponibilité si l'état d'une instance active est défaillant. Les demandes d'impression sont conservées dans la file d'attente des tâches LRS localement dans chacune des EC2 instances. En cas de restauration, une instance défaillante doit être redémarrée pour que les services LRS reprennent le traitement de la demande d'impression.

> **Note**
>
> Le LRS VPSX/MFI peut également effectuer des contrôles de santé au niveau du parc d'imprimantes. Pour plus d'informations, consultez la section Contrôles de santé du parc d'imprimantes dans la section Informations supplémentaires de ce modèle.

5. AWS Managed Microsoft AD s'intègre à LRS/DIS pour effectuer l'authentification et l'autorisation du flux de travail d'impression. Pour plus d'informations, voir Authentification et autorisation d'impression dans la section Informations supplémentaires de ce modèle.
6. LRS VPSX/MFI utilise Amazon EBS pour le stockage par blocs. Vous pouvez sauvegarder les données Amazon EBS des EC2 instances actives sur Amazon S3 sous forme de point-in-time snapshots et les restaurer sur des volumes EBS en veille. Pour automatiser la création, la conservation et la suppression des instantanés de volume Amazon EBS, vous pouvez utiliser Amazon Data Lifecycle Manager pour définir la fréquence des instantanés automatisés et les restaurer en fonction de vos exigences RTO/RPO.

Outils

Services AWS

- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon. EC2 Les volumes EBS se comportent comme des périphériques de stockage en mode bloc bruts non formatés. Vous pouvez monter ces volumes en tant qu'appareils sur vos instances.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- AWS Directory Service pour Microsoft Active Directory (AD), également connu sous le nom d'AWS Managed Microsoft Active Directory, permet à vos charges de travail sensibles aux annuaires et à vos ressources AWS d'utiliser Active Directory géré dans AWS.

Autres outils

- L'interface LRS VPSX/MFI (Micro Focus Interface), développée conjointement par LRS et Micro Focus, capture le résultat d'une bobine JES du serveur Micro Focus Enterprise et le transmet de manière fiable à une destination d'impression spécifiée.
- Le serveur LRS Directory Information Server (LRS/DIS) est utilisé pour l'authentification et l'autorisation pendant le flux de travail d'impression.
- LRS/Queue is a TCP/IP-based LRS/Queue transmission agent, used by LRS VPSX/MFI, pour collecter ou capturer des données d'impression via l'interface de programmation en ligne Print Exit de Micro Focus.
- Micro Focus Enterprise Server est un environnement de déploiement d'applications pour les applications mainframe. Il fournit l'environnement d'exécution pour les applications mainframe migrées ou créées à l'aide de n'importe quelle version de Micro Focus Enterprise Developer.

Épopées

Configuration de Micro Focus Enterprise Server sur Amazon EC2 et déploiement d'une application en ligne pour mainframe

Tâche	Description	Compétences requises
Configurez Micro Focus Enterprise Server et déployez une application de démonstration en ligne.	Configurez Micro Focus Enterprise Server sur Amazon EC2, puis déployez l'application Micro Focus Account Demo (ACCT Demo) sur Amazon EC2 en suivant les instructions du didacticiel : Support CICS figurant dans la documentation Micro Focus. L'application ACCT Demo est une application en ligne pour ordinateur central (CICS) qui crée puis lance une sortie d'impression.	Architecte du cloud

Configurer un serveur d'impression LRS sur Amazon EC2

Tâche	Description	Compétences requises
Obtenez une licence de produit LRS pour l'impression.	Pour obtenir une licence de produit LRS pour LRSVPSX/MFI, LRS/Queue, and LRS/DIS, contactez l'équipe de gestion des sorties LRS. Vous devez fournir les noms d'hôte des EC2 instances sur lesquelles les produits LRS seront installés.	Gagnez du plomb
Créez une instance Amazon EC2 Windows pour installer LRS VPSX/MFI.	Lancez une instance Amazon EC2 Windows en suivant les instructions de l'étape 1 : Lancer une instance dans la EC2 documentation Amazon. Votre instance doit répondre aux exigences matérielles et logicielles suivantes pour LRS VPSX/MFI : • Processeur : double cœur • RAM — 16 GO • Disque dur : 500 Go • EC2 Instance minimale : m5.xlarge • Système d'exploitation — Windows/Linux • Logiciel : Internet Information Service (IIS) ou Apache	Architecte du cloud

Tâche	Description	Compétences requises
	Note Les exigences matérielles et logiciell es ci-dessus sont destinées à un petit parc d'imprimantes (environ 500 à 1 000). Pour connaître toutes les exigences, consultez vos contacts LRS et AWS. Lorsque vous créez votre instance Windows, procédez comme suit : 1. Vérifiez que le nom EC2 d'hôte est le même que celui utilisé pour la licence du produit LRS. 2. Activez CGI dans Amazon en EC2 effectuant les opérations suivantes : a. Connectez-vous à votre EC2 instance en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. b. Dans le menu Démarrer de Windows, recherchez	

Tâche	Description	Compétences requises
	et ouvrez le Gestionnaire de serveur. c. Dans le Gestionnaire de serveur, choisissez Tableau de bord, Démarrage rapide, Ajouter des rôles et des fonctionnalités. Choisissez ensuite Rôles de serveur. d. Dans Rôles de serveur, choisissez WebServer (IIS), puis choisissez Développement d'applications. e. Dans Développement d'applications, cochez la case CGI. f. Suivez les instructions de l'assistant d'ajout de rôles et de fonctionnalités du Gestionnaire de serveurs Windows pour installer CGI. g. Ouvrez le port 5500 dans le pare-feu Windows de l' EC2 instance pour la communication LRS/Queue.	

Tâche	Description	Compétences requises
Installez LRS VPSX/MFI sur l'instance. EC2	1. Connectez-vous à votre EC2 instance en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. 2. **Note** Ouvrez le lien vers la page de téléchargement du produit contenu dans l'e-mail LRS que vous devriez recevoir. : Les produits LRS sont distribués par transfert électroni que de fichiers (EFT). 3. Téléchargez LRS VPSX/MFI et décompressez le fichier (dossier par défaut :). `c:\LRS` 4. Lancez le programme d'installation du produit LRS depuis le dossier décompressé pour installer LRS VPSX/MFI. 5. Dans le menu Sélection ner les fonctionnalités, sélectionnez VPSX® Server (V1R3.022), puis choisisse	Architecte du cloud

Tâche	Description	Compétences requises
	z Suivant pour démarrer le processus d'installation. Vous recevrez un message de confirmation lorsque l'installation sera terminée.	
Installez LRS/Queue.	1. Connectez-vous à votre EC2 instance Micro Focus Enterprise Server en suivant les instructions de l'étape 2 : Connexion à votre instance dans la EC2 documentation Amazon. 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans l'e-mail LRS que vous devriez recevoir, téléchargez LRS/Queue , puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS pour installer LRS/Queue.	Architecte du cloud

Tâche	Description	Compétences requises
Installez LRS/DIS.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Ouvrez le lien vers la page de téléchargement du produit LRS figurant dans l'e-mail LRS que vous devriez recevoir, téléchargez LRS/DIS, puis décompressez le fichier. 3. Accédez à l'emplacement où vous avez téléchargé les fichiers, puis lancez le programme d'installation du produit LRS. 4. Dans le programme d'installation du produit LRS, développez LRS Misc Tools, sélectionnez LRS DIS, puis Next. 5. Suivez le reste des instructions du programme d'installation du produit LRS pour terminer le processus d'installation.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un groupe cible et enregistrez LRS EC2 VPSX/MFI comme cible.	Créez un groupe cible en suivant les instructions de la section Create a target group for your Network Load Balancer dans la documentation d'Elastic Load Balancing. Lorsque vous créez le groupe cible, procédez comme suit : 1. Sur la page Spécifier les détails du groupe, pour Choisir un type de cible, sélectionnez Instances. 2. Pour Protocole, choisissez TCP. 3. Pour Port, choisissez 5500. 4. Sur la page Enregistrer les cibles, dans la section Instances disponibles, sélectionnez les instances LRS EC2 VPSX/MFI.	Architecte du cloud

Tâche	Description	Compétences requises
Créez un Network Load Balancer.	Suivez les instructions de Create a Network Load Balancer dans la documentation d'Elastic Load Balancing. Votre Network Load Balancer achemine le trafic de Micro Focus Enterprise Server vers LRS VPSX/MFI. EC2 Lorsque vous créez le Network Load Balancer, procédez comme suit sur la page Listeners and Routing : 1. Pour Protocol (Protocole), choisissez TCP. 2. Pour Port, choisissez 5500. 3. Pour Action par défaut, choisissez Transférer vers pour le groupe cible que vous avez créé précédemment.	Architecte du cloud

Intégrer Micro Focus Enterprise Server à LRS VPSX/MFI and LRS/Queue

Tâche	Description	Compétences requises
Configurez Micro Focus Enterprise Server pour l'intégration de LRS/Queue.	1. Connectez-vous à votre EC2 instance Micro Focus Enterprise Server en suivant les instructions de l'étape 2 : Connexion à votre instance dans la EC2 documentation Amazon.	Architecte du cloud

Tâche	Description	Compétences requises
	2. Dans le menu Démarrer de Windows, ouvrez l'interface utilisateur d'administration de Micro Focus Enterprise Server. 3. Dans la barre de menu, choisissez NATIVE. 4. Dans le volet de navigation, choisissez Directory Server, puis BANKDEMO ou la région de votre serveur d'entreprise. 5. Depuis Général dans le volet de navigation de gauche, faites défiler la page vers le bas jusqu'à la section Additional pour configurer les variables d'environnement (LRSQ_ADDRESS, LRSQ_PORT, LRSQ_COMMAND) afin qu'elles pointent vers LRSQ. 6. Pour LRSQ_ADDRESS, entrez l'adresse IP ou le nom DNS du Network Load Balancer que vous avez créé précédemment. 7. Pour LRSQ_PORT, entrez VPSX LRSQ Listener Port (5500). 8. Pour LRSQ_COMMAND, entrez l'emplacement du	

Tâche	Description	Compétences requises
	chemin de l'exécutable LRSQ. 9. **Note** LRS prend actuellement en charge une limite maximale de 50 caractères pour les noms DNS, mais cette limite est susceptible de changer à l'avenir. Si votre nom DNS est supérieur à 50, vous pouvez utiliser l'adresse IP du Network Load Balancer comme alternative.	

Tâche	Description	Compétences requises
Rendez CICS Print Exit (DFHUPRNT) disponible pour l'initialisation de Micro Focus Enterprise Server.	1. Connectez-vous à votre EC2 instance Micro Focus Enterprise Server en suivant les instructions de l'étape 2 : Connexion à votre instance dans la EC2 documentation Amazon. 2. **Note** Copiez CICS Print Exit (DFHUPRNT) depuis le dossier exécutable LRS VPSX/MFI (nomméVPSX_MFI_R2) vers l'emplacement de l'instance Micro Focus Enterprise Server. EC2 Pour les systèmes 32 bits, l'emplacement estC:\Program Files (x86)\Micro Focus\Enterprise Server\bin . Pour les systèmes 64 bits, l'emplacement estC:\Program Files (x86)\Micro Focus\Enterprise	Architecte du cloud

Tâche	Description	Compétences requises
	`Server\bin64 .` : le `DFHUPRNT_64.dll` fichier doit être renommé `DFHUPRNT.dll` lorsqu'il est copié. Vérifiez que Micro Focus Enterprise Server a détecté CICS Print Exit (DFHUPRNT) 1. Arrêtez et démarrez Micro Focus Enterprise Server. 2. Dans le panneau d'administration de Micro Focus Enterprise Server, ouvrez Monitor, Logs, Console logs. 3. Consultez les journaux de la console pour voir s'afficher le message suivant : « L'utilisateur de l'imprimante 3270 quitte DFHUPRNT installé avec succès ».	

Tâche	Description	Compétences requises
Définissez l'ID du terminal de l'imprimante CICS (TERMIDs) en tant que Micro Focus Enterprise Server.	Activer l'impression 3270 dans Micro Focus Enterprise Server 1. Dans le panneau d'administration de Micro Focus Enterprise Server, ouvrez CICS, Resources, By Group. 2. Dans le panneau de navigation de gauche, choisissez SIT (Table d'initialisation du système), puis BNKCICV. 3. Dans la section Général, faites défiler l'écran jusqu'à 3270, puis cochez la case Imprimer 3270. Définissez le terminal de l'imprimante CICS dans Micro Focus Enterprise Server 1. Dans le panneau d'administration de Micro Focus Enterprise Server, ouvrez CICS, Resources, By Type. 2. Dans le panneau de navigation de gauche, choisissez Terme, puis Nouveau. Le formulaire Créer une ressource de terminal s'ouvre. 3. Dans Nom, entrez le nom de la file d'impression LRS.	Architecte du cloud

Tâche	Description	Compétences requises
	(Remarque : ce modèle utilise « P275 » comme identifiant de terminal de l'imprimante CICS et comme file d'impression LRS VPSX.) 4. Dans le champ Groupe, saisissez BANKTERM. 5. Dans le champ Installation automatique — Modèle, entrez NON. 6. Pour Identifiants de terminal - Type de terminal, entrez DFHPRT32. 7. Dans le champ Nom du réseau, entrez VTAMP275. 8. Pour l'utilisation du terminal, cochez la case En service. 9. Faites défiler la page en haut de la page, puis sélectionnez Enregistrer. 10. Choisissez Installer. Un message contextuel affiche un message d'installation réussie.	

Configuration des imprimantes et des utilisateurs d'impression dans Micro Focus Enterprise Server et LRS VPSX/MFI

Tâche	Description	Compétences requises
Créez une file d'impression dans le LRS VPSX.	1. Connectez-vous à votre EC2 instance LRS VPSX/	Architecte du cloud

Tâche	Description	Compétences requises
	MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Ouvrez l'interface Web VPSX depuis le menu Démarrer de Windows. 3. Dans le volet de navigation, sélectionnez Imprimantes. 4. Choisissez Ajouter, puis sélectionnez Ajouter une imprimante. 5. Sur la page Configuration de l'imprimante, dans Nom de l'imprimante, entrez P275. 6. Pour VPSX ID, entrez. VPS1 7. Pour CommType, sélectionnez TCP/IP/LRSQ. 8. Pour Adresse hôte/IP, entrez l'adresse IP de l'imprimante physique que vous souhaitez ajouter. 9. Dans Appareil, entrez le nom de votre appareil. 10. Choisissez le pilote Windows ou le pilote Linux/Mac. 11. Choisissez Ajouter.	

Tâche	Description	Compétences requises
	Note La file d'impression doit être équivalente à l'impression TERMIDs créée dans Micro Focus Enterprise Server.	

Tâche	Description	Compétences requises
Créez un utilisateur d'impression dans LRS VPSX/MFI.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Ouvrez l'interface Web VPSX depuis le menu Démarrer de Windows. 3. Dans le volet de navigation, choisissez Security, puis Users. 4. Dans la colonne Nom d'utilisateur, choisissez admin, puis Copier. 5. Dans la fenêtre Maintenance du profil utilisateur, pour Nom d'utilisateur, entrez un nom d'utilisateur (par exemple, PrintUser). 6. Dans Description, entrez une brève description (par exemple, Utilisateur pour le test d'impression). 7. Choisissez Mettre à jour. Cela crée un utilisateur d'impression (par exemple, PrintUser). 8. Dans le volet de navigation, sous Utilisateur, choisissez le nouvel utilisateur que vous avez créé.	Architecte du cloud

Tâche	Description	Compétences requises
	9. Dans le menu Commande, sélectionnez Sécurité. 10. Sur la page Règles de sécurité, choisissez toutes les options de sécurité de l'imprimante et de sécurité des tâches applicables, puis sélectionnez Enregistrer. 11. Pour ajouter votre nouvel utilisateur d'impression au groupe des administr ateurs, accédez au volet de navigation, choisissez Sécurité, puis sélectionnez Configurer. 12. Dans la fenêtre de configuration de la sécurité, ajoutez votre nouvel utilisateur d'impression dans la colonne Administr ateur.	

Configuration de l'authentification et de l'autorisation d'impression

Tâche	Description	Compétences requises
Créez un domaine Microsoft AD géré par AWS avec des utilisateurs et des groupes.	1. Créez un Active Directory sur AWS Managed Microsoft AD en suivant les instructions de la section Créer votre répertoire AWS Managed Microsoft AD dans la documentation AWS Directory Service.	Architecte du cloud

Tâche	Description	Compétences requises
	2. Déployez une EC2 instance (gestionnaire Active Directory) et installez les outils Active Directory pour gérer votre AWS Managed Microsoft AD en suivant les instructions de l'étape 3 : Déployer une EC2 instance pour gérer votre AWS Managed Microsoft AD dans la documentation AWS Directory Service. 3. **Note** Connectez-vous à votre EC2 instance en suivant les instructions de l'étape 2 : Se connecter à votre instance dans la EC2 documentation Amazon. : Lorsque vous vous connectez à l' EC2 instance, entrez vos informations d'identification d'administrateur (pour le répertoire que vous avez créé à la première étape) dans la fenêtre de sécurité Windows.	

Tâche	Description	Compétences requises
	4. Dans le menu Démarrer de Windows, sous Outils d'administration Windows, sélectionnez Utilisateurs et ordinateurs Active Directory . 5. Créez un utilisateur d'impression dans le domaine Active Directory en suivant les étapes décrites dans la section Créer un utilisateur dans la documentation du service AWS Directory.	
Associez LRS VPSX/MFI EC2 à un domaine Microsoft AD géré par AWS.	Associez LRS VPSX/MFI EC2 à votre domaine Microsoft AD géré par AWS automatiquement (documentation du centre de connaissances AWS) ou manuellement (documentation AWS Directory Service).	Architecte du cloud

Tâche	Description	Compétences requises
Configurez et intégrez LRS/DIS à AWS Managed Microsoft AD.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, choisissez Security, puis Configure. 4. Sur la page Configuration de la sécurité, dans la section Paramètres de sécurité, pour Type de sécurité, sélectionnez Interne. 5. Entrez vos préférences pour les autres options dans la section Paramètres de sécurité. 6. Ouvrez le dossier LRS Output Management dans le menu Démarrer de Microsoft Windows, choisissez Server Start, puis Server Stop. 7. Connectez-vous à LRS VPSX/MFI à l'aide de votre nom d'utilisateur et de	Architecte du cloud

Tâche	Description	Compétences requises
	votre mot de passe Active Directory.	

Testez un flux d'impression en ligne

Tâche	Description	Compétences requises
Lancez une demande d'impression en ligne à partir de l'application Micro Focus ACCT Demo.	1. **Note** Ouvrez l'émulateur de terminal TN3270 dans votre EC2 instance Micro Focus Enterprise Server. (: Ce modèle utilise des émulateurs de terminal 3270.) 2. Connectez-vous à l'émulateur de terminal TN3270 (Rumba). Pour l'adresse du nom d'hôte, utilisez 127.0.0.1. Pour le port Telnet, utilisez 9270. 3. Une fois connecté à l'écran 3270, appuyez sur CTL +SHIFT+Z pour effacer l'écran. 4. Pour démarrer l'application ACCT Demo, en écran clair, entrez ACCT. Cela ouvre l'écran principal de l'application ACCT Demo Online	Architecte du cloud

Tâche	Description	Compétences requises
	(CICS). Remarque : L'écran principal inclut des options de menu telles que le fichier de compte, la recherche par nom, la saisie, le type de demande, le compte et l'imprimante. 5. Pour soumettre une demande d'impression à partir de l'application ACCT Demo Online (CICS), entrez P dans le champ du type de demande, 11111 dans le champ du compte et P275 dans le champ de l'imprima nte. Assurez-vous de définir la valeur dans le champ de l'imprimante sur la valeur de l'ID du terminal de l'imprima nte CICS. 6. Appuyez sur Entrée. Le message « Demande d'impression planifiée » apparaît en bas de l'écran. Cela confirme qu'une demande d'impression en ligne a été générée à partir de l'application ACCT Demo et envoyée à LRS VPS/MFI pour le traitement de l'impression.	

Tâche	Description	Compétences requises
Vérifiez la sortie d'impression dans LRS VPSX/MFI.	1. Connectez-vous à votre EC2 instance LRS VPSX/MFI en suivant les instructions de l'étape 2 : Connect to your instance dans la documentation Amazon. EC2 2. Dans le menu Démarrer de Windows, ouvrez l'interface Web VPSX. 3. Dans le volet de navigation, choisissez Imprimantes, puis choisissez Output Queue. Recherchez la file d'impression P275 que vous avez créée précédemment pour l'impression en ligne. 4. Pour la file d'impression (P275), dans la colonne ID de bobine, choisissez l'ID de bobine pour la demande dans la file d'impression. 5. Dans l'onglet Actions, dans la colonne COMMANDE, choisissez Parcourir. Vous pouvez maintenant voir la sortie imprimée d'un relevé de compte avec des colonnes pour le numéro de compte, le nom de famille, le prénom, l'adresse, le téléphone, le	Ingénieur de test

Tâche	Description	Compétences requises
	numéro de téléphone. Cartes émises, date d'émission, montant et solde. Pour un exemple, consultez la pièce jointe online_print_output pour ce modèle.	

Ressources connexes

- Modernisation des sorties LRS (documentation LRS)
- Concepts de réseau VTAM (documentation IBM)
- Résumé des types d'unités logiques (LU) (documentation IBM)
- Commandes ANSI et du chariot de machines (documentation IBM)
- Optimisation des charges de travail du mainframe d'entreprise sur AWS avec Micro Focus (blog du réseau de partenaires AWS)
- Créez un PAC de serveur Micro Focus Enterprise avec Amazon EC2 Auto Scaling et Systems Manager (documentation AWS Prescriptive Guidance)
- Flux de données de présentation des fonctions avancées (AFP) (documentation IBM)
- Flux de données conditionné par ligne (LCDS) (documentation Compart)

Informations supplémentaires

Considérations

Au cours de votre processus de modernisation, vous pouvez envisager une grande variété de configurations pour les processus en ligne du mainframe et les résultats qu'ils génèrent. La plate-forme centrale a été personnalisée par chaque client et fournisseur qui l'utilise avec des exigences particulières qui ont une incidence directe sur l'impression. Par exemple, votre plateforme actuelle peut intégrer l'IBM Advanced Function Presentation (AFP) ou le Xerox Line Condition Data Stream (LCDS) dans le flux de travail actuel. En outre, les caractères de commande du chariot central et les mots de commande des canaux peuvent affecter l'apparence de la page imprimée et nécessiter un traitement spécial. Dans le cadre du processus de planification de la modernisation, nous vous

recommandons d'évaluer et de comprendre les configurations de votre environnement d'impression spécifique.

Capture de données d'impression

Cette section résume les méthodes de programmation d'applications CICS que vous pouvez utiliser dans un environnement mainframe IBM pour l'impression. Serveur d'VPSX/MFI components provide techniques to allow the same application programs to create data in the same way. The following table describes how each application programming method is supported in a modernized CICS application running in AWS and Micro Focus Enterprise Server with an LRS VPSX/MFIimpression LRS.

Méthode	Description	Support de la méthode dans un environnement modernisé
EXEC CICS ENVOIE DU TEXTE.. ou EXEC CICS SEND MAP.	Ces méthodes CICS et VTAM sont chargées de créer et de fournir des flux de données d'impression 3270/SCS à LUTYPE0 et aux périphéri ques d'impression. LUTYPE1 LUTYPE3	Une interface de programme d'application (API) Micro Focus Online Print Exit (DFHUPRNT) permet de traiter les données d'impress ion par des flux de données VPSX/MFI when 3270/SCS d'impression créés à l'aide de l'une ou l'autre de ces méthodes.
EXEC CICS ENVOIE DU TEXTE.. ou EXEC CICS SEND MAP. (avec un logiciel IBM mainframe tiers)	Les méthodes CICS et VTAM sont chargées de créer et de fournir des flux de données d'impression 3270/SCS à LUTYPE0 et aux périphéri ques d'impression. LUTYPE1 LUTYPE3 Des logiciels tiers interceptent les données d'impression, les convertis sent en données de format d'impression standard avec un caractère de contrôle	Une API Micro Focus Online Print Exit (DFHUPRNT) permet de traiter les données d'impression par des flux de données VPSX/MFI when 3270/SCS d'impression créés à l'aide de l'une ou l'autre de ces méthodes.

	ASA/MCH et placent les données sur la bobine JES pour qu'elles soient traitées par des systèmes d'impress ion basés sur des ordinateurs centraux utilisant JES.	
EXEC CICS SPOOLOPEN	Cette méthode est utilisée par les programmes d'applica tion CICS pour écrire des données directement dans le spool JES. Les données sont ensuite disponibles pour être traitées par des systèmes d'impression basés sur des ordinateurs centraux qui utilisent JES.	Micro Focus Enterprise Server envoie les données vers le spool Enterprise Server où elles peuvent être traitées par le VPSX/MFI Batch Print Exit LRSPRTE6 () qui envoie les données vers VPSX.
DRS/API	Une interface de programma tion fournie par LRS est utilisée pour écrire les données d'impression dans JES.	Le VPSX/MFI fournit une interface de remplacement qui transmet les données d'impression directement au VPSX.

Contrôles de santé du parc d'imprimantes

Le LRS VPSX/MFI (LRS LoadX) peut effectuer des contrôles de santé approfondis, y compris la gestion des appareils et l'optimisation opérationnelle. La gestion des périphériques permet de détecter les défaillances d'une imprimante et d'acheminer la demande d'impression vers une imprimante saine. Pour plus d'informations sur les contrôles approfondis de l'état des flottes d'imprimantes, consultez la documentation LRS incluse dans la licence de votre produit.

Authentification et autorisation d'impression

LRS/DIS enables LRS applications to authenticate user IDs and passwords by using Microsoft Active Directory or an LDAP server. In addition to basic print authorization, LRS/DISpeut également appliquer des contrôles de sécurité d'impression de niveau granulaire dans les cas d'utilisation suivants :

- Gérez les personnes autorisées à parcourir la tâche d'impression.
- Gérez le niveau de navigation des offres d'emploi des autres utilisateurs.
- Gérez les tâches opérationnelles. Par exemple, la sécurité au niveau de la commande, telle que la maintenance/libération, la purge, la modification, la copie et le reroutage. La sécurité peut être configurée par l'ID utilisateur ou par le groupe (similaire au groupe AD ou au groupe LDAP).

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Déplacez les fichiers du mainframe directement vers Amazon S3 à l'aide de Transfer Family

Créée par Luis Gustavo Dantas (AWS)

Récapitulatif

Dans le cadre du processus de modernisation, vous pouvez relever le défi du transfert de fichiers entre vos serveurs sur site et le cloud Amazon Web Services (AWS). Le transfert de données depuis des mainframes peut représenter un défi de taille, car les mainframes ne peuvent généralement pas accéder aux magasins de données modernes tels qu'Amazon Simple Storage Service (Amazon S3), Amazon Elastic Block Store (Amazon EBS) ou Amazon Elastic File System (Amazon EFS).

De nombreux clients utilisent des ressources intermédiaires, telles que des serveurs Linux, Unix ou Windows sur site, pour transférer des fichiers vers le cloud AWS. Vous pouvez éviter cette méthode indirecte en utilisant AWS Transfer Family avec le protocole SFTP (Secure Shell) pour charger les fichiers du mainframe directement sur Amazon S3.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cloud privé virtuel (VPC) doté d'un sous-réseau accessible par votre ancienne plateforme
- Un point de terminaison Transfer Family pour votre VPC
- Fichiers VSAM (Mainframe Virtual Storage Access Method) convertis en fichiers séquentiels de longueur fixe (documentation IBM)

Limites

- Le SFTP transfère les fichiers en mode binaire par défaut, ce qui signifie que les fichiers sont chargés sur Amazon S3 avec le codage EBCDIC préservé. Si votre fichier ne contient pas de données binaires ou compressées, vous pouvez utiliser la sous-commande sftp ascii (documentation IBM) pour convertir vos fichiers en texte pendant le transfert.
- Vous devez déballer les fichiers du mainframe (AWS Prescriptive Guidance) contenant du contenu compressé et binaire pour pouvoir utiliser ces fichiers dans votre environnement cible.
- La taille des objets Amazon S3 peut varier d'un minimum de 0 octet à un maximum de 5 To. Pour plus d'informations sur les fonctionnalités d'Amazon S3, consultez Amazon S3 FAQs.

Architecture

Pile technologique source

- Langage de contrôle des tâches (JCL)
- Shell z/OS Unix et ISPF
- SFTP
- VSAM et fichiers plats

Pile technologique cible

- Transfer Family
- Amazon S3
- Amazon Virtual Private Cloud (Amazon VPC)

Architecture cible

Le schéma suivant montre une architecture de référence permettant d'utiliser Transfer Family with SFTP pour télécharger des fichiers du mainframe directement dans un compartiment S3.

Le schéma suivant illustre le flux de travail suivant :

1. Vous utilisez une tâche JCL pour transférer les fichiers de votre mainframe de l'ancien mainframe vers le cloud AWS via Direct Connect.
2. Direct Connect permet à votre trafic réseau de rester sur le réseau mondial AWS et de contourner l'Internet public. Direct Connect améliore également la vitesse du réseau, en commençant à 50 Mbits/s et en augmentant jusqu'à 100 Gbit/s.
3. Le point de terminaison VPC permet d'établir des connexions entre les ressources de votre VPC et les services pris en charge sans utiliser l'Internet public. Access to Transfer Family et Amazon S3 assure une haute disponibilité grâce aux interfaces réseau élastiques situées dans deux sous-réseaux privés et des zones de disponibilité.
4. Transfer Family authentifie les utilisateurs et utilise le protocole SFTP pour recevoir vos fichiers depuis l'environnement existant et les déplacer vers un compartiment S3.

Automatisation et évolutivité

Une fois le service Transfer Family en place, vous pouvez transférer un nombre illimité de fichiers du mainframe vers Amazon S3 en utilisant une tâche JCL comme client SFTP. Vous pouvez également automatiser le transfert de fichiers en utilisant un planificateur de tâches par lots du mainframe pour exécuter les tâches SFTP lorsque vous êtes prêt à transférer les fichiers du mainframe.

Outils

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.
- AWS Transfer Family vous permet de dimensionner en toute sécurité vos transferts de business-to-business fichiers récurrents vers Amazon S3 et Amazon EFS en utilisant les protocoles SFTP, FTPS et FTP.

Épopées

Création du compartiment S3 et de la politique d'accès

Tâche	Description	Compétences requises
Créez le compartiment S3.	Créez un compartiment S3 pour héberger les fichiers que vous transférez depuis votre environnement existant.	AWS général
Créez le rôle et la politique IAM.	Transfer Family utilise votre rôle AWS Identity and Access Management (IAM) pour accorder l'accès au compartiment S3 que vous avez créé précédemment. Créez un rôle IAM qui inclut la politique IAM suivante :	AWS général

Tâche	Description	Compétences requises
	{ "Version": "2012-10-17", "Statement": [{ "Sid": "UserFolderListing", "Action": ["s3:ListBucket", "s3:GetBucketLocat ion"], "Effect": "Allow", "Resource": ["arn:aws:s3:::<your- bucket-name>"] }, { "Sid": "HomeDirObjectAcce ss", "Effect": "Allow", "Action": ["s3:PutObject", "s3:GetObjectAcl", "s3:GetObject", "s3:DeleteObjectVe rsion", "s3:DeleteObject",	

Tâche	Description	Compétences requises

	<pre>"s3:PutObjectAcl",
	
	"s3:GetObjectVersion"
	],
	"Resource":
	"arn:aws:s3:::<your-
	bucket-name>/*"
	}
	]
	}</pre>
	Note
	Vous devez choisir le cas d'utilisation du transfert lorsque vous créez le rôle IAM.	

Définissez le service de transfert

Tâche	Description	Compétences requises
Créez le serveur SFTP.	1. Connectez-vous à la console de gestion AWS, ouvrez la console Transfer Family, puis choisissez Create server. 2. Choisissez uniquement le protocole SFTP (SSH File Transfer Protocol) - transfert de fichiers via le protocole Secure Shell, puis choisissez Next.	AWS général

Tâche	Description	Compétences requises
	3. Pour le fournisseur d'identité, choisissez Service géré, puis cliquez sur Suivant. 4. Pour le type de point de terminaison, choisissez VPC hébergé. 5. Pour Access, choisissez Internal. 6. Pour VPC, choisissez votre VPC. 7. Dans la section Zones de disponibilité, choisissez vos zones de disponibilité et vos sous-réseaux. 8. Dans la section Groupes de sécurité, choisissez votre groupe de sécurité, puis cliquez sur Suivant. 9. Pour Domain, choisissez Amazon S3, puis Next. 10. Conservez les options par défaut sur la page Configurer les informations supplémentaires, puis choisissez Suivant. 11. Choisissez Créer un serveur. **Note** Pour plus d'informations sur la configuration d'un serveur	

Tâche	Description	Compétences requises
	SFTP, consultez Create an SFTP enabled server (AWS Transfer Family User Guide).	
Obtenez l'adresse du serveur.	1. Ouvrez la console Transfer Family et choisissez votre ID de serveur dans la colonne Server ID. 2. Dans la section Détails du point de terminaison, pour le type de point de terminaison, choisissez l'ID du point de terminais on. Cela vous amène à la console Amazon VPC. 3. Dans l'onglet Détails de la console Amazon VPC, recherchez les noms DNS à côté des noms DNS.	AWS général
Créez la paire de clés du client SFTP.	Créez une paire de clés SSH pour Microsoft Windows ou macOS/Linux/UNIX.	AWS, SSH en général

Tâche	Description	Compétences requises
Créez l'utilisateur SFTP.	1. Ouvrez la console Transfer Family, choisissez Servers dans le volet de navigation, puis sélectionnez votre serveur. 2. Dans la colonne ID du serveur, choisissez l'ID du serveur pour votre serveur, puis choisissez Ajouter un utilisateur. 3. Dans Nom d'utilisateur, entrez un nom d'utilisateur correspondant au nom d'utilisateur de votre paire de clés SSH. 4. Pour Rôle, choisissez le rôle IAM que vous avez créé précédemment. 5. Pour le répertoire personnel, choisissez le compartiment S3 que vous avez créé précédemment. 6. Pour les clés publiques SSH, entrez la paire de clés que vous avez créée précédemment. 7. Choisissez Ajouter.	AWS général

Transférer le fichier du mainframe

Tâche	Description	Compétences requises

Envoyez la clé privée SSH au mainframe.	Utilisez SFTP ou SCP pour envoyer la clé privée SSH à l'environnement existant.
	
	Exemple SFTP :
	
	`sftp [USERNAME@mainframeIP]`
	`[password]`
	`cd [/u/USERNAME]`
	`put [your-key-pair-file]`
	
	Exemple de SCP :
	
	`scp [your-key-pair-file] [USERNAME@MainframeIP]:/[u/USERNAME]`
	
	Enregistrez ensuite la clé SSH dans le système de fichiers z/OS Unix sous le nom d'utilisateur qui exécutera ultérieurement le traitement par lots de transfert de fichiers (par exemple,). `/u/CONTROLM`
	
	Note
	Pour plus d'informations sur le shell z/OS Unix, voir Présentat
		Ordinateur central, shell z/OS Unix, FTP, SCP

Tâche	Description	Compétences requises
	ion du shell z/OS (documentation IBM).	

Tâche	Description	Compétences requises

Créez le client SFTP JCL.	Les mainframes n'ayant pas de client SFTP natif, vous devez utiliser l'utilitaire BPXBATCH pour exécuter le client SFTP depuis le shell z/OS Unix.
	
	Dans l'éditeur ISPF, créez le client SFTP JCL. Par exemple :
	
	`//JOBNAM JOB ...`
	`//************`
	`******************`
	`******************`
	`******************`
	`****`
	`//SFTP EXEC PGM=BPXBA`
	`TCH,REGION=0M`
	`//STDPARM DD *`
	`SH cp "//'MAINF`
	`RAME.FILE.NAME'"`
	` filename.txt;`
	`echo 'put filename.txt'`
	` > uplcmd;`
	`sftp -b uplcmd -i`
	` ssh_private_key_fi`
	`le ssh_username@<tran`
	`sfer service ip or`
	` DNS>;`
	`//SYSPRINT DD SYSOUT=*`
	`//STDOUT DD SYSOUT=*`
	`//STDENV DD *`
	`//STDERR DD SYSOUT=*`
	
	Note
	Pour plus d'informations sur l'exécuti
		JCL, mainframe, shell z/OS Unix

Tâche	Description	Compétences requises
	on d'une commande dans le shell z/OS Unix, consultez l'utilitaire BPXBATCH (documentation IBM). Pour plus d'informations sur la création ou la modification de tâches JCL dans z/OS, consultez Qu'est-ce que l'ISPF ? et l'éditeur ISPF (documentation IBM).	
Exécutez le client SFTP JCL.	1. Dans l'éditeur ISPF, entrez SUB, puis appuyez sur la touche ENTER une fois la tâche JCL créée. 2. Surveillez l'activité des tâches de transfert de fichiers par lots du mainframe dans SDSF. **Note** Pour plus d'informations sur la façon de vérifier l'activité des tâches par lots, consultez le guide de l'utilisateur z/OS SDSF (documentation IBM).	Ordinateur central, JCL, ISPF

Tâche	Description	Compétences requises
Validez le transfert de fichiers.	1. Connectez-vous à la console de gestion AWS, ouvrez la console Amazon S3, puis choisissez Buckets dans le volet de navigation. 2. Choisissez le bucket associé à votre Transfer Family. 3. Dans la section Objets de l'onglet Objets, recherchez le fichier que vous avez transféré depuis le mainframe.	AWS général
Automatisez le client SFTP JCL.	Utilisez le planificateur de tâches pour déclencher automatiquement le client SFTP JCL. **Note** Vous pouvez utiliser des planificateurs de tâches mainframe, tels que BMC Control-M ou CA Workload Automation, pour automatiser les tâches par lots pour les transferts de fichiers en fonction du temps et d'autres dépendances entre les tâches par lots.	Planificateur de tâches

Ressources connexes

- Comment fonctionne AWS Transfer Family
- Modernisation du mainframe avec AWS

Sécurisez et rationalisez l'accès des utilisateurs dans une base de données de fédération DB2 sur AWS en utilisant des contextes fiables

Créée par Sai Parthasaradhi (AWS)

Récapitulatif

De nombreuses entreprises migrent leurs anciennes charges de travail mainframe vers Amazon Web Services (AWS). Cette migration inclut le transfert des bases de données IBM Db2 for z/OS vers Db2 pour Linux, Unix et Windows (LUW) sur Amazon Elastic Compute Cloud (Amazon). EC2 Lors d'une migration progressive d'un environnement sur site vers AWS, les utilisateurs peuvent avoir besoin d'accéder aux données dans IBM Db2 z/OS et dans Db2 LUW sur Amazon EC2 jusqu'à ce que toutes les applications et bases de données soient entièrement migrées vers Db2 LUW. Dans de tels scénarios d'accès aux données à distance, l'authentification des utilisateurs peut s'avérer difficile car les différentes plateformes utilisent des mécanismes d'authentification différents.

Ce modèle explique comment configurer un serveur de fédération sur Db2 pour LUW avec Db2 pour z/OS comme base de données distante. Le modèle utilise un contexte fiable pour propager l'identité d'un utilisateur de Db2 LUW à Db2 z/OS sans se réauthentifier sur la base de données distante. Pour plus d'informations sur les contextes sécurisés, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance Db2 exécutée sur une instance Amazon EC2
- Une base de données Db2 pour z/OS distante exécutée sur site
- Le réseau sur site connecté à AWS via le Site-to-SiteVPN AWS ou AWS Direct Connect

Architecture

Architecture cible

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le cloud AWS. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Site-to-SiteLe VPN AWS vous aide à faire passer le trafic entre les instances que vous lancez sur AWS et votre propre réseau distant.

Autres outils

- db2cli est la commande d'interface de ligne de commande (CLI) interactive de DB2.

Épopées

Activer la fédération sur la base de données DB2 LUW exécutée sur AWS

Tâche	Description	Compétences requises
Activez la fédération sur la base de données DB2 LUW.	Pour activer la fédération sur DB2 LUW, exécutez la commande suivante. `update dbm cfg using federated YES`	DBA
Redémarrez la base de données.	Pour redémarrer la base de données, exécutez la commande suivante. `db2stop force; db2start;`	DBA

Cataloguer la base de données distante

Tâche	Description	Compétences requises
Cataloguez le sous-système Db2 z/OS distant.	Pour cataloguer la base de données distante Db2 z/OS	DBA

Tâche	Description	Compétences requises
	sur Db2 LUW exécutée sur AWS, utilisez l'exemple de commande suivant. `catalog TCPIP NODE tcpnode REMOTE mainframehost SERVER mainframeport`	
Cataloguez la base de données distante.	Pour cataloguer la base de données distante, utilisez l'exemple de commande suivant. `catalog db dbnam1 as ndbnam1 at node tcpnode`	DBA

Création de la définition du serveur distant

Tâche	Description	Compétences requises
Collectez les informations d'identification utilisateur pour la base de données distante Db2 z/OS.	Avant de passer aux étapes suivantes, collectez les informations suivantes : • Nom du sous-système Db2 z/OS : nom de Db2 z/OS catalogué sur LUW à partir de l'étape précédente (par exemple,) `ndbnam1` • Version Db2 z/OS : version du sous-système Db2 z/OS (par exemple,) 12 • ID utilisateur Db2 z/OS : utilisateur disposant du	DBA

Tâche	Description	Compétences requises
	privilège BIND, nécessaire pour créer uniquement la définition du serveur (par exemple,) `dbuser1` • Mot de passe Db2 z/OS : mot de passe pour `dbuser1` (par exemple,) `dbpasswd` • Utilisateur proxy Db2 z/OS : ID de l'utilisateur du proxy, qui sera utilisé pour établir une connexion sécurisée (par exemple,) `zproxy` • Mot de passe du proxy Db2 z/OS : mot de passe de l'`zproxy`utilisateur (par exemple,) `zproxy`	
Créez le wrapper DRDA.	Pour créer le wrapper DRDA, exécutez la commande suivante. `CREATE WRAPPER DRDA;`	DBA

Tâche	Description	Compétences requises
Créez la définition du serveur.	Pour créer la définition du serveur, exécutez l'exemple de commande suivant. `CREATE SERVER ndbserver TYPE DB2/ZOS VERSION 12 WRAPPER DRDA AUTHORIZATION "dbuser1" PASSWORD "dbpasswd " OPTIONS ( DBNAME 'ndbnam1',FED_PROXY_USER 'ZPROXY' );` Dans cette définition, `FED_PROXY_USER` indique l'utilisateur proxy qui sera utilisé pour établir des connexions fiables à la base de données Db2 z/OS. L'ID utilisateur et le mot de passe d'autorisation ne sont requis que pour créer l'objet serveur distant dans la base de données DB2 LUW. Ils ne seront pas utilisés ultérieur ement pendant l'exécution.	DBA

Création de mappages d'utilisateurs

Tâche	Description	Compétences requises
Créez un mappage utilisateur pour l'utilisateur proxy.	Pour créer un mappage utilisateur pour un utilisateur proxy, exécutez la commande suivante.	DBA

Tâche	Description	Compétences requises
	`CREATE USER MAPPING FOR ZPROXY SERVER ndbserver OPTIONS (REMOTE_AUTHID 'ZPROXY', REMOTE_PASSWORD 'zproxy');`	

Tâche	Description	Compétences requises
Créez des mappages d'utilisateurs pour chaque utilisateur sur DB2 LUW.	Créez des mappages d'utilisateurs pour tous les utilisateurs de la base de données DB2 LUW sur AWS qui ont besoin d'accéder aux données distantes via l'utilisateur proxy. Pour créer les mappages d'utilisateurs, exécutez la commande suivante. `CREATE USER MAPPING FOR PERSON1 SERVER ndbserver OPTIONS (REMOTE_AUTHID 'USERZID', USE_TRUSTED_CONTEXT 'Y');` L'instruction indique qu'un utilisateur de DB2 LUW (PERS0N1) peut établir une connexion sécurisée avec la base de données distante Db2 z/OS (). `USE_TRUSTED_CONTEXT 'Y'` Une fois la connexion établie via l'utilisateur proxy, celui-ci peut accéder aux données à l'aide de l'ID utilisateur Db2 z/OS ()`REMOTE_AUTHID 'USERZID'` .	DBA

Création de l'objet de contexte sécurisé

Tâche	Description	Compétences requises
Créez l'objet de contexte sécurisé.	Pour créer l'objet de contexte sécurisé sur la base de données distante Db2 z/OS, utilisez l'exemple de commande suivant. `CREATE TRUSTED CONTEXT CTX_LUW_ZOS BASED UPON CONNECTIO N USING SYSTEM AUTHID ZPROXY ATTRIBUTES ( ADDRESS '10.10.10.10' ) NO DEFAULT ROLE ENABLE WITH USE FOR PUBLIC WITHOUT AUTHENTIC ATION;` Dans cette définition, `CTX_LUW_ZOS` il s'agit d'un nom arbitraire pour l'objet de contexte sécurisé. L'objet contient l'ID utilisateur du proxy et l'adresse IP du serveur d'où doit provenir la connexion sécurisée. Dans cet exemple, le serveur est la base de données DB2 LUW sur AWS. Vous pouvez utiliser le nom de domaine au lieu de l'adresse IP. La clause `WITH USE FOR PUBLIC WITHOUT AUTHENTICATION` indique	DBA

Tâche	Description	Compétences requises
	que le changement d'ID utilisateur sur une connexion sécurisée est autorisé pour chaque ID utilisateur. Il n'est pas nécessaire de fournir un mot de passe.	

Ressources connexes

- Installation de contrôle d'accès aux ressources IBM (RACF)
- Fédération IBM DB2 LUW
- Contextes fiables

Informations supplémentaires

Contextes fiables DB2

Un contexte sécurisé est un objet de base de données DB2 qui définit une relation de confiance entre un serveur fédéré et un serveur de base de données distant. Pour définir une relation de confiance, le contexte de confiance spécifie les attributs de confiance. Il existe trois types d'attributs de confiance :

- ID d'autorisation système à l'origine de la demande initiale de connexion à la base de données
- L'adresse IP ou le nom de domaine à partir duquel la connexion est établie
- Paramètre de chiffrement pour les communications de données entre le serveur de base de données et le client de base de données

Une connexion sécurisée est établie lorsque tous les attributs d'une demande de connexion correspondent aux attributs spécifiés dans un objet de contexte sécurisé défini sur le serveur. Il existe deux types de connexions fiables : les connexions implicites et les connexions explicites. Une fois qu'une connexion sécurisée implicite est établie, un utilisateur hérite d'un rôle auquel il n'a pas accès en dehors du cadre de cette définition de connexion sécurisée. Une fois qu'une connexion sécurisée explicite est établie, les utilisateurs peuvent être connectés à la même connexion physique, avec ou sans authentification. En outre, les utilisateurs de DB2 peuvent se voir attribuer des rôles qui

spécifient des privilèges à utiliser uniquement dans le cadre de la connexion sécurisée. Ce modèle utilise une connexion sécurisée explicite.

Contexte fiable dans ce modèle

Une fois le schéma terminé, PERSON1 sur Db2, LUW accède aux données distantes depuis Db2 z/OS en utilisant un contexte sécurisé fédéré. La connexion pour PERSON1 est établie via un utilisateur proxy si la connexion provient de l'adresse IP ou du nom de domaine spécifié dans la définition du contexte sécurisé. Une fois la connexion établie, PERSON1 l'ID utilisateur Db2 z/OS correspondant est changé sans nouvelle authentification, et l'utilisateur peut accéder aux données ou aux objets en fonction des privilèges Db2 configurés pour cet utilisateur.

Avantages des contextes fiables fédérés

- Cette approche maintient le principe du moindre privilège en éliminant l'utilisation d'un identifiant d'utilisateur ou d'un identifiant d'application commun qui nécessiterait un surensemble de tous les privilèges requis par tous les utilisateurs.
- L'identité réelle de l'utilisateur qui effectue la transaction à la fois sur la base de données fédérée et distante est toujours connue et peut être auditée.
- Les performances s'améliorent car la connexion physique est réutilisée entre les utilisateurs sans que le serveur fédéré n'ait besoin de s'authentifier à nouveau.

Transférez des données Db2 z/OS à grande échelle vers Amazon S3 dans des fichiers CSV

Créée par Bruno Sahinoglu (AWS), Ivan Schuster (AWS) et Abhijit Kshirsagar (AWS)

Récapitulatif

Un ordinateur central est toujours un système d'enregistrement dans de nombreuses entreprises, contenant une énorme quantité de données, y compris des entités de données de base contenant des enregistrements des transactions commerciales actuelles et historiques. Il est souvent cloisonné et n'est pas facilement accessible par les systèmes distribués au sein d'une même entreprise. Avec l'émergence de la technologie cloud et la démocratisation des mégadonnées, les entreprises souhaitent utiliser les informations cachées dans les données du mainframe pour développer de nouvelles capacités commerciales.

Dans ce but, les entreprises cherchent à ouvrir les données Db2 de leur mainframe à leur environnement cloud Amazon Web Services (AWS). Les raisons commerciales sont multiples et les méthodes de transfert varient d'un cas à l'autre. Il se peut que vous préfériez connecter votre application directement au mainframe ou que vous préfériez répliquer vos données en temps quasi réel. Si le cas d'utilisation consiste à alimenter un entrepôt de données ou un lac de données, il n'est plus nécessaire de disposer d'une up-to-date copie et la procédure décrite dans ce modèle peut suffire, en particulier si vous souhaitez éviter les coûts de licence de produits tiers. Un autre cas d'utilisation peut être le transfert de données sur le mainframe pour un projet de migration. Dans un scénario de migration, les données sont nécessaires pour effectuer les tests d'équivalence fonctionnelle. L'approche décrite dans cet article est un moyen rentable de transférer les données DB2 vers l'environnement cloud AWS.

Amazon Simple Storage Service (Amazon S3) étant l'un des services AWS les plus intégrés, vous pouvez accéder aux données à partir de là et recueillir des informations directement en utilisant d'autres services AWS tels qu'Amazon Athena, les fonctions AWS Lambda ou Amazon. QuickSight Vous pouvez également charger les données sur Amazon Aurora ou Amazon DynamoDB à l'aide d'AWS Glue ou d'AWS Database Migration Service (AWS DMS). Dans cet objectif, il décrit comment décharger les données Db2 dans des fichiers CSV au format ASCII sur le mainframe et transférer les fichiers vers Amazon S3.

À cette fin, des scripts mainframe ont été développés pour aider à générer des langages de contrôle des tâches (JCLs) permettant de décharger et de transférer autant de tables DB2 que nécessaire.

Conditions préalables et limitations

Prérequis

- Utilisateur du système d'exploitation IBM z/OS autorisé à exécuter des scripts Restructured Extended Executor (REXX) et JCL.
- Accès aux services système z/OS Unix (USS) pour générer des clés privées et publiques SSH (Secure Shell).
- Un compartiment S3 inscriptible. Pour plus d'informations, consultez Créer votre premier compartiment S3 dans la documentation Amazon S3.
- Un serveur compatible avec le protocole SFTP (AWS Transfer Family SSH File Transfer Protocol) utilisant Service géré en tant que fournisseur d'identité et Amazon S3 en tant que service de stockage AWS. Pour plus d'informations, consultez la section Créer un serveur compatible SFTP dans la documentation AWS Transfer Family.

Limites

- Cette approche n'est pas adaptée à la synchronisation des données en temps quasi réel ou en temps réel.
- Les données ne peuvent être déplacées que de Db2 z/OS vers Amazon S3, et non l'inverse.

Architecture

Pile technologique source

- Mainframe exécutant Db2 sous z/OS

Pile technologique cible

- AWS Transfer Family
- Amazon S3
- Amazon Athena
- Amazon QuickSight
- AWS Glue
- Amazon Relational Database Service (Amazon RDS)

- Amazon Aurora
- Amazon Redshift

Architecture source et cible

Le schéma suivant montre le processus de génération, d'extraction et de transfert de données Db2 z/OS au format ASCII CSV vers un compartiment S3.

1. Une liste de tables est sélectionnée pour la migration des données à partir du catalogue DB2.
2. La liste est utilisée pour générer des tâches de déchargement avec les colonnes numériques et de données au format externe.
3. Les données sont ensuite transférées vers Amazon S3 à l'aide d'AWS Transfer Family.
4. Une tâche d'extraction, de transformation et de chargement (ETL) AWS Glue peut transformer les données et les charger dans un bucket traité au format spécifié, ou AWS Glue peut introduire les données directement dans la base de données.
5. Amazon Athena et Amazon QuickSight peuvent être utilisés pour interroger et afficher les données afin de générer des analyses.

Le schéma suivant montre le déroulement logique de l'ensemble du processus.

1. Le premier JCL, appelé TABNAME, utilisera l'utilitaire Db2 DSNTIAUL pour extraire et générer la liste des tables que vous comptez décharger de Db2. Pour choisir vos tables, vous devez adapter manuellement l'entrée SQL pour sélectionner et ajouter des critères de filtre afin d'inclure un ou plusieurs schémas DB2.
2. Le second JCL, appelé REXXEXEC, utilisera le squelette JCL et le programme REXX fournis pour traiter la liste des tables créée par le JCL TABNAME et générer un JCL par nom de table. Chaque JCL contiendra une étape pour décharger la table et une autre pour envoyer le fichier au compartiment S3 à l'aide du protocole SFTP.
3. La dernière étape consiste à exécuter la JCL pour décharger la table et à transférer le fichier vers AWS. L'ensemble du processus peut être automatisé à l'aide d'un planificateur sur site ou sur AWS.

Outils

Services AWS

- Amazon Athena est un service de requêtes interactif qui vous permet d'analyser les données directement dans Amazon Simple Storage Service (Amazon S3) à l'aide du langage SQL standard.
- Amazon Aurora est un moteur de base de données relationnelle entièrement géré conçu pour le cloud et compatible avec MySQL et PostgreSQL.
- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- Amazon QuickSight est un service de business intelligence (BI) à l'échelle du cloud qui vous permet de visualiser, d'analyser et de rapporter vos données dans un tableau de bord unique.
- Amazon Redshift est un service d'entrepôt de données géré à l'échelle du pétaoctet dans le cloud AWS.
- Amazon Relational Database Service (Amazon RDS) vous aide à configurer, exploiter et dimensionner une base de données relationnelle dans le cloud AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Transfer Family est un service de transfert sécurisé qui vous permet de transférer des fichiers vers et depuis les services de stockage AWS.

Outils pour ordinateurs centraux

- Le protocole SFTP (SSH File Transfer Protocol) est un protocole de transfert de fichiers sécurisé qui permet la connexion à distance et le transfert de fichiers entre serveurs. SSH assure la sécurité en chiffrant tout le trafic.
- DSNTIAUL est un exemple de programme fourni par IBM pour le déchargement de données.
- DSNUTILB est un programme d'utilitaires par lots fourni par IBM pour décharger des données avec différentes options de DSNTIAUL.
- z/OS OpenSSH est un port du logiciel open source SSH exécuté sur le service système Unix sous le système d'exploitation IBM z/OS. SSH est un programme de connexion sécurisé et crypté entre deux ordinateurs fonctionnant sur un réseau TCP/IP. Il fournit plusieurs utilitaires, dont ssh-keygen.
- Le script REXX (Restructured Extended Executor) est utilisé pour automatiser la génération de JCL avec les étapes Db2 Unload et SFTP.

Code

Le code de ce modèle est disponible dans le dépôt GitHub unloaddb2.

Bonnes pratiques

Lors du premier déchargement, les données générées JCLs doivent décharger l'intégralité des données de la table.

Après le premier déchargement complet, effectuez des déchargements incrémentiels pour améliorer les performances et réaliser des économies. Mettez à jour la requête SQL dans le modèle de deck JCL pour tenir compte des modifications apportées au processus de déchargement.

Vous pouvez convertir le schéma manuellement ou en utilisant un script sur Lambda avec le Db2 SYSPUNCH en entrée. Pour un processus industriel, AWS Schema Conversion Tool (SCT) est l'option préférée.

Enfin, utilisez un planificateur basé sur le mainframe ou un planificateur sur AWS avec un agent sur le mainframe pour gérer et automatiser l'ensemble du processus.

Épopées

Configuration du compartiment S3

Tâche	Description	Compétences requises
Créez le compartiment S3.	Pour obtenir des instructions, consultez la section Création de votre premier compartiment S3.	AWS général

Configuration du serveur Transfer Family

Tâche	Description	Compétences requises
Créez un serveur compatible SFTP.	Pour ouvrir et créer un serveur SFTP sur la console AWS Transfer Family, procédez comme suit :	AWS général

Tâche	Description	Compétences requises
	1. Sur la page Choisir des protocoles, cochez la case SFTP (protocole de transfert de fichiers SSH) — transfert de fichiers via Secure Shell. 2. Pour le fournisseur d'identité, choisissez Service géré. 3. Pour le point de terminaison, choisissez Accessible au public. 4. Pour le domaine, choisissez Amazon S3. 5. Sur la page Configurer les détails supplémentaires, conservez les paramètres par défaut. 6. Créez le serveur.	
Créez un rôle IAM pour Transfer Family.	Pour créer un rôle AWS Identity and Access Management (IAM) permettant à Transfer Family d'accéder à Amazon S3, suivez les instructions de la section Création d'un rôle et d'une politique IAM.	Administrateur AWS
Ajoutez un utilisateur géré par le service Amazon S3.	Pour ajouter l'utilisateur géré par le service Amazon S3, suivez les instructions de la documentation AWS et utilisez l'ID utilisateur de votre mainframe.	AWS général

Sécuriser le protocole de communication

Tâche	Description	Compétences requises
Créez la clé SSH.	Dans l'environnement USS de votre mainframe, exécutez la commande suivante. `ssh-keygen -t rsa` **Note** Lorsque vous êtes invité à saisir un mot de passe, gardez-le vide.	Développeur mainframe

Attribuez les niveaux d'autorisation appropriés au dossier SSH et aux fichiers clés.	Par défaut, les clés publiques et privées sont stockées dans le répertoire des utilisateurs/u/`home/username/.ssh` .
	Vous devez donner l'autorisation 644 aux fichiers clés et 700 au dossier.
	`chmod 644 .ssh/id_rsa`
	`chmod 700 .ssh`
		Développeur mainframe

Copiez le contenu de la clé publique sur votre utilisateur géré par le service Amazon S3.	Pour copier le contenu de la clé publique générée par USS, ouvrez la console AWS Transfer Family. 1. Dans le volet de navigation, choisissez Servers (Serveurs).	Développeur mainframe

Tâche	Description	Compétences requises
	2. Choisissez l'identifiant dans la colonne ID du serveur pour voir les détails du serveur 3. Sous Utilisateurs, choisissez un nom d'utilisateur pour voir les détails de l'utilisateur 4. Sous Clés publiques SSH, choisissez Ajouter une clé publique SSH pour ajouter la clé publique à un utilisateur. Pour la clé publique SSH, entrez votre clé publique. Votre clé est validée par le service avant que vous puissiez ajouter votre nouvel utilisateur. 5. Sélectionnez Ajouter une clé.	

Générez le JCLs

Tâche	Description	Compétences requises
Générez la liste des tables DB2 intégrées au champ d'application.	Fournissez du code SQL d'entrée pour créer une liste des tables concernées par la migration des données. Cette étape vous oblige à spécifier des critères de sélection pour interroger la table de catalogue DB2 SYSIBM.SYSTABLES à l'aide	Développeur mainframe

Tâche	Description	Compétences requises
	d'une clause SQL where. Les filtres peuvent être personnalisés pour inclure un schéma spécifique ou des noms de table commençant par un préfixe particulier ou basés sur un horodatage pour un déchargement incrémentiel. La sortie est capturée dans un jeu de données séquentiel physique (PS) sur le mainframe. Cet ensemble de données servira d'entrée pour la prochaine phase de génération de JCL. Avant d'utiliser le JCL TABNAME (vous pouvez le renommer si nécessaire), apportez les modifications suivantes : 1. <Jobcard>Remplacez-le par une classe de travail et un utilisateur autorisé à exécuter les utilitaires DB2. 2. Remplacez < HLQ1 > ou personnalisez les noms des jeux de données en sortie pour qu'ils répondent aux normes de votre site. 3. Mettez à jour la pile STEPLIB de PDSEs (ensemble de données partitionné étendu)	

Tâche	Description	Compétences requises

	conformément aux normes de votre site. L'exemple de ce modèle utilise les valeurs par défaut d'IBM.
	4. Remplacez le nom PLAN et LIB par les valeurs spécifiques à votre installation.
	5. Remplacez <Schema>et <Prefix>par vos critères de sélection pour le catalogue Db2.
	6. Enregistrez le JCL obtenu dans une bibliothèque PDS (ensemble de données partitionné).
	7. Soumettez le JCL.
	
	Tâche d'extraction de listes de tables DB2
	
	`<Jobcard>`
	`//*`
	`//* UNLOAD ALL THE TABLE NAMES FOR A PARTICULAR SCHEMA`
	`//*`
	`//STEP01 EXEC PGM=IEFBR14`
	`//*`
	`//DD1 DD DISP=(MOD,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(1000,(1,1)),`
	`// DSN=<HLQ1>.DSN81210.TABLIST`	

Tâche	Description	Compétences requises

	`//*`
	`//DD2 DD DISP=(MOD`
	`,DELETE,DELETE),`
	`// UNIT=SYSDA,`
	`// SPACE=(1000,`
	`(1,1)),`
	`// DSN=<HLQ1`
	`>.DSN81210.SYSPUNCH`
	`//*`
	`//UNLOAD EXEC PGM=IKJEF`
	`T01,DYNAMNBR=20`
	`//SYSTSPRT DD`
	` SYSOUT=*`
	`//STEPLIB DD`
	` DISP=SHR,DSN=DSNC1`
	`0.DBCG.SDSNEXIT`
	`// DD DISP=SHR,`
	`DSN=DSNC10.SDSNLOAD`
	`// DD DISP=SHR,`
	`DSN=CEE.SCEERUN`
	`// DD DISP=SHR,`
	`DSN=DSNC10.DBCG.RU`
	`NLIB.LOAD`
	`//SYSTSIN DD *`
	`  DSN SYSTEM(DBCG)`
	`  RUN PROGRAM(D`
	`SNTIAUL) PLAN(DSNT`
	`IB12) PARMS('SQL') -`
	`  LIB('DSNC`
	`10.DBCG.RUNLIB.LOAD')`
	`  END`
	`//SYSPRINT DD SYSOUT=*`
	`//*`
	`//SYSUDUMP DD SYSOUT=*`
	`//*`
	`//SYSREC00 DD DISP=(NEW`
	`,CATLG,DELETE),`
	`// UNIT=SYSD`
	`A,SPACE=(32760,(10`
	`00,500)),`
	`// DSN=<HLQ1`
	`>.DSN81210.TABLIST`	

Tâche	Description	Compétences requises

	`//*`
	`//SYSPUNCH DD DISP=(NEW`
	`,CATLG,DELETE),`
	`//  UNIT=SYSD`
	`A,SPACE=(32760,(10`
	`00,500)),`
	`//  VOL=SER=S`
	`CR03,RECFM=FB,LREC`
	`L=120,BLKSIZE=12`
	`//  DSN=<HLQ1`
	`>.DSN81210.SYSPUNCH`
	`//*`
	`//SYSIN  DD *`
	`  SELECT CHAR(CREA`
	`TOR), CHAR(NAME)`
	`  FROM SYSIBM.SY`
	`STABLES`
	`  WHERE OWNER =`
	`'<Schema>'`
	`  AND NAME LIKE`
	`'<Prefix>%'`
	`  AND TYPE = 'T';`
	`/*`	

Tâche	Description	Compétences requises
Modifiez les modèles JCL.	Les modèles JCL fournis avec ce modèle contiennent une carte de travail générique et des noms de bibliothèques. Cependant, la plupart des sites mainframe auront leurs propres normes de dénominat ion pour les noms de jeux de données, les noms de bibliothèques et les fiches de travail. Par exemple, une classe de travail spécifiqu e peut être requise pour exécuter des tâches DB2. Le sous-système Job Entry implémente JES2 et JES3 peut imposer des modificat ions supplémentaires. Les bibliothèques de chargemen t standard peuvent avoir un premier qualificatif différent de celui SYS1 qui est celui par défaut d'IBM. Par conséquen t, personnalisez les modèles pour tenir compte des normes spécifiques à votre site avant de les exécuter. Apportez les modifications suivantes dans le squelette JCL UNLDSKEL : 1. Modifiez la carte de travail avec une classe de travail	Développeur mainframe

Tâche	Description	Compétences requises
	et un utilisateur autorisés à exécuter les utilitaires DB2. 2. Personnalisez les noms des jeux de données en sortie pour répondre aux normes de votre site. 3. Mettez à jour la pile STEPLIB PDSEs conformément aux normes de votre site. L'exemple de ce modèle utilise les valeurs par défaut d'IBM. 4. <DSN>Remplacez-le par le nom de votre sous-système DB2 et l'ID de corrélation. 5. Enregistrez le JCL obtenu dans une bibliothèque PDS faisant partie de votre pile ISPSLIB, qui est la bibliothèque de modèles de squelette standard pour ISPF. Déchargement et squelette JCL SFTP `//&USRPFX.U JOB (DB2UNLOAD),'JOB', CLASS=A,MSGCLASS=A, //  TIME=1440 ,NOTIFY=&USRPFX //* DELETE DATASETS //STEP01  EXEC PGM=IEFBR14`	

Tâche	Description	Compétences requises
	`//DD01 DD DISP=(MOD ,DELETE,DELETE), // UNIT=SYSD A, // SPACE=(TR K,(1,1)), // DSN=&USRPFX..DB2.P UNCH.&JOBNAME //DD02 DD DISP=(MOD ,DELETE,DELETE), // UNIT=SYSD A, // SPACE=(TR K,(1,1)), // DSN=&USRPFX..DB2.U NLOAD.&JOBNAME //* //* RUNNING DB2 EXTRACTION BATCH JOB FOR AWS DEMO //* //UNLD01 EXEC PGM=DSNUTILB,REGIO N=0M, // PARM='<DSN>,UNLOAD' //STEPLIB DD DISP=SHR,DSN=DSNC1 0.DBCG.SDSNEXIT // DD DISP=SHR, DSN=DSNC10.SDSNLOAD //SYSPRINT DD SYSOUT=* //UTPRINT DD SYSOUT=* //SYSOUT DD SYSOUT=* //SYSPUN01 DD DISP=(NEW,CATLG,DE LETE), // SPACE=(CY L,(1,1),RLSE), // DSN=&USRPFX..DB2.P UNCH.&JOBNAME`	

Tâche	Description	Compétences requises

	//SYSREC01 DD
	 DISP=(NEW,CATLG,DE
	LETE),
	// SPACE=(CY
	L,(10,50),RLSE),
	// DSN=&USRPFX..DB2.U
	NLOAD.&JOBNAME
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD *
	  UNLOAD
	  DELIMITED COLDEL ','
	  FROM TABLE &TABNAME
	  UNLDDN SYSREC01
	  PUNCHDDN SYSPUN01
	  SHRLEVEL CHANGE
	 ISOLATION UR;
	 /*
	//*
	//* FTP TO AMAZON S3
	 BACKED FTP SERVER IF
	 UNLOAD WAS SUCCESSFUL
	//*
	//SFTP EXEC PGM=BPXBA
	TCH,COND=(4,LE),RE
	GION=0M
	//STDPARM DD *
	 SH cp "//'&USRP
	FX..DB2.UNLOAD.&JO
	BNAME'"
	  &TABNAME..csv;
	 echo "ascii
	 " >> uplcmd;
	 echo "PUT &TABNAME.
	.csv " >>>> uplcmd;
	 sftp -b uplcmd -i .ssh/
	id_rsa &FTPUSER.
	@&FTPSITE;
	 rm &TABNAME..csv;
	 //SYSPRINT DD SYSOUT=*
	 //STDOUT DD SYSOUT=*
	 //STDENV DD *	

Tâche	Description	Compétences requises
	`//STDERR DD SYSOUT=*`	

Tâche	Description	Compétences requises
Générez le JCL Mass Unload.	Cette étape implique l'exécuti on d'un script REXX dans un environnement ISPF à l'aide de JCL. Fournissez la liste des tables incluses créées lors de la première étape en tant qu'entrée pour la génération massive de JCL par rapport au `TABLIST DD` nom. La JCL générera une nouvelle JCL par nom de table dans un ensemble de données partitionné spécifié par l'utilisateur et indiqué par rapport au nom. `ISPFILE DD` Allouez cette bibliothèque au préalable. Chaque nouvelle JCL comportera deux étapes : une étape pour décharger la table Db2 dans un fichier, et une étape pour envoyer le fichier dans le compartiment S3. Apportez les modificat ions suivantes dans le JCL REXXEXEC (vous pouvez changer le nom) : 1. `Job card user ID`Remplacez-le par un ID utilisateur du mainframe autorisé à décharger les tables. `SYSPROCISPPLIB`Remplacez	Développeur mainframe

Tâche	Description	Compétences requises
	-les, ISPSLIBISPMLIB, et ISPTLIB <HLQ1> valorisez -les ou personnalisez- les DSN pour répondre aux normes de votre site. Pour connaître les valeurs spécifiques à votre installat ion, utilisez la commande. TSO ISRDDN 2. <MFUSER>Remplacez-le par un ID utilisateur doté de privilèges d'exécution de tâches dans votre installat ion. 3. <FTPUSER> Remplacez- le par un ID utilisateur doté des privilèges USS et FTP dans votre installation. Il est supposé que cet ID utilisate ur et ses clés de sécurité SSH sont en place dans le répertoire des services Unix Systems approprié sur le mainframe. 4. <AWS TransferFamily IP>Remplacez-le par l'adresse IP ou le nom de domaine AWS Transfer Family. Cette adresse sera utilisée pour l'étape SFTP. 5. Soumettez le JCL après avoir appliqué l'héberge ment standard du site et mis à jour le programme	

Tâche	Description	Compétences requises

	REXX comme décrit ci-dessous.
	
	Tâche de génération de JCL en masse
	
	`//RUNREXX JOB (CREATEJCL),'RUNS ISPF TABLIST', CLASS=A,MSGCLASS=A,`
	
	`//  TIME=1440 ,NOTIFY=&SYSUID`
	`//* Most of the values required can be updated to your site specific`
	`//* values using the command 'TSO ISRDDN' in your ISPF session.`
	`//* Update all the lines tagged with //update marker to desired`
	`//* site specific values.`
	`//ISPF EXEC PGM=IKJEFT01,REGION=2048K,DYNAMNBR=25`
	`//SYSPROC DD DISP=SHR,DSN=USER.Z23D.CLIST`
	`//SYSEXEC DD DISP=SHR,DSN=<HLQ1>.TEST.REXXLIB`
	`//ISPPLIB DD DISP=SHR,DSN=ISP.SISPPENU`
	`//ISPSLIB DD DISP=SHR,DSN=ISP.SISPSENU`	

Tâche	Description	Compétences requises

	`//  DD`
	` DISP=SHR,DSN=<HLQ1`
	`>.TEST.ISPSLIB`
	`//ISPMLIB  DD`
	` DSN=ISP.SISPMENU,D`
	`ISP=SHR`
	`//ISPTLIB  DD`
	` DDNAME=ISPTABL`
	`//  DD DSN=ISP.S`
	`ISPTENU,DISP=SHR`
	`//ISPTABL  DD`
	` LIKE=ISP.SISPTENU,`
	`UNIT=VIO`
	`//ISPPROF  DD`
	` LIKE=ISP.SISPTENU,`
	`UNIT=VIO`
	`//ISPLOG  DD`
	` SYSOUT=*,RECFM=VA,`
	`LRECL=125`
	`//SYSPRINT  DD SYSOUT=*`
	`//SYSTSPRT  DD`
	` SYSOUT=*`
	`//SYSUDUMP  DD`
	` SYSOUT=*`
	`//SYSDBOUT  DD`
	` SYSOUT=*`
	`//SYSTSPRT  DD`
	` SYSOUT=*`
	`//SYSUDUMP  DD`
	` SYSOUT=*`
	`//SYSDBOUT  DD`
	` SYSOUT=*`
	`//SYSHELP  DD`
	` DSN=SYS1.HELP,DISP`
	`=SHR`
	`//SYSOUT  DD SYSOUT=*`
	`//* Input list of`
	` tablenames`
	`//TABLIST  DD`
	` DISP=SHR,DSN=<HLQ1`
	`>.DSN81210.TABLIST`
	`//* Output pds`	

Tâche	Description	Compétences requises

	`//ISPFILE DD DISP=SHR,DSN=<HLQ1>.TEST.JOBGEN`
	`//SYSTSIN DD *`
	`ISPSTART CMD(ZSTEPS <MFUSER> <FTPUSER> <AWS TransferFamily IP>)`
	`/*`
	
	Avant d'utiliser le script REXX, apportez les modifications suivantes :
	
	1. Enregistrez le script REXX dans une bibliothè que PDS définie sous la `SYSEXEC` pile dans le JCL REXXEXEC édité à l'étape précédente avec ZSTEPS comme nom de membre. Si vous souhaitez le renommer, vous devez mettre à jour la JCL en fonction de vos besoins.
	2. Ce script utilise l'option trace pour imprimer des informations supplémen taires en cas d'erreur. Vous pouvez à la place ajouter un code de gestion des `EXECIO` erreurs après les `TSO` instructions,, et supprimer la ligne de trace. `ISPEXEC`
	3. Ce script génère des noms de membres en utilisant la	

Tâche	Description	Compétences requises
	convention de L0Dnnnnn dénomination, qui peut prendre en charge jusqu'à 100 000 membres. Si vous avez plus de 100 000 tables, utilisez un préfixe plus court et ajustez les nombres dans le `tempjob` relevé. Script STEPS REX `/*REXX - - -

Tâche	Description	Compétences requises

	<pre>tempjob= "LOD" !! RIGHT("0000" !! i, 5) jobname=tempjob Say tempjob ADDRESS ISPEXEC "FTOPEN " ADDRESS ISPEXEC "FTINCL UNLDSKEL" /* member will be saved in ISPDSN library allocated in JCL */ ADDRESS ISPEXEC "FTCLOSE NAME("tem pjob")" END
	
	ADDRESS TSO "FREE F(TABLIST) " ADDRESS TSO "FREE F(ISPFILE) "
	
	exit 0</pre>	

Exécutez le JCLs

Tâche	Description	Compétences requises
Effectuez l'étape de déchargement de DB2.	Après la génération de JCL, vous aurez JCLs autant de tables à décharger. Cette histoire utilise un exemple généré par JCL pour expliquer la structure et les étapes les plus importantes. Aucune action de votre part n'est nécessaire. Les	Développeur mainframe, Ingénieur système

Tâche	Description	Compétences requises
	informations suivantes sont fournies à titre de référence uniquement. Si votre intention est de soumettre JCLs ce que vous avez généré à l'étape précédente, passez à la section Soumettre la LODnnnnn JCLs tâche. Lorsque vous déchargez des données Db2 à l'aide d'une JCL avec l'utilita ire DSNUTILB Db2 fourni par IBM, vous devez vous assurer que les données déchargées ne contiennent pas de données numérique s compressées. Pour ce faire, utilisez le paramètre DSNUTILB`DELIMITED` . Le `DELIMITED` paramètre permet de décharger les données au format CSV en ajoutant un caractère comme délimiteur et des guillemet s doubles pour le champ de texte, en supprimant le rembourrage dans la colonne VARCHAR et en convertissant tous les champs numérique s en FORMAT EXTERNE, y compris les champs DATE. L'exemple suivant montre à quoi ressemble l'étape de	

Tâche	Description	Compétences requises
	déchargement dans le JCL généré, en utilisant la virgule comme séparateur. `UNLOAD DELIMITED COLDEL ',' FROM TABLE SCHEMA_NAME.TBNAME UNLDDN SYSREC01 PUNCHDDN SYSPUN01 SHRLEVEL CHANGE ISOLATION UR;`	

Tâche	Description	Compétences requises
Effectuez l'étape SFTP.	Pour utiliser le protocole SFTP depuis une JCL, utilisez l'utilitaire BPXBATCH. L'utilitaire SFTP ne peut pas accéder directement aux ensembles de données MVS. Vous pouvez utiliser la commande copy (`cp`) pour copier le fichier `&USRPFX..DB2.UNLOAD.&JOBNAME` séquentiel dans le répertoire USS, où il se trouve. `&TABNAME..csv` Exécutez la `sftp` commande à l'aide de la clé privée (`id_rsa`) et de l'ID utilisateur RACF comme nom d'utilisateur pour vous connecter à l'adresse IP AWS Transfer Family. `SH cp "//'&USRPFX..DB2.UNLOAD.&JOBNAME'" &TABNAME..csv; echo "ascii " >> uplcmd; echo "PUT &TABNAME..csv " >>>> uplcmd; sftp -b uplcmd -i .ssh/id_rsa &FTPUSER.@&FTP_TF_SITE; rm &TABNAME..csv;`	Développeur mainframe, Ingénieur système

Tâche	Description	Compétences requises
Soumettez le LODnnnnn JCLs.	La JCL précédente générait toutes les tables LODnnnnn JCL qui devaient être déchargées, transformées en CSV et transférées dans le compartiment S3. Exécutez la `submit` commande sur tous ceux JCLs qui ont été générés.	Développeur mainframe, Ingénieur système

Ressources connexes

Pour plus d'informations sur les différents outils et solutions utilisés dans ce document, consultez les rubriques suivantes :

- Guide de l'utilisateur de z/OS OpenSSH
- Db2 z/OS — Exemples d'instructions de contrôle UNLOAD
- Db2 z/OS — Déchargement de fichiers délimités
- Transfer Family — Création d'un serveur compatible SFTP
- Transfer Family — Travailler avec des utilisateurs gérés par des services

Informations supplémentaires

Une fois que vous avez enregistré vos données DB2 sur Amazon S3, vous disposez de nombreuses méthodes pour développer de nouvelles connaissances. Amazon S3 s'intégrant aux services d'analyse de données AWS, vous pouvez librement consommer ou exposer ces données du côté distribué. Par exemple, vous pouvez effectuer les opérations suivantes :

- Créez un lac de données sur Amazon S3 et extrayez des informations précieuses à l'aide query-in-place d'outils d'analyse et d'apprentissage automatique sans déplacer les données.
- Lancez une fonction Lambda en configurant un flux de travail de traitement après le téléchargement intégré à AWS Transfer Family.

- Développez de nouveaux microservices pour accéder aux données dans Amazon S3 ou dans une base de données entièrement gérée à l'aide d'AWS Glue, un service d'intégration de données sans serveur qui facilite la découverte, la préparation et la combinaison de données à des fins d'analyse, d'apprentissage automatique et de développement d'applications.

Dans le cas d'une migration, étant donné que vous pouvez transférer toutes les données du mainframe vers S3, vous pouvez effectuer les opérations suivantes :

- Supprimez l'infrastructure physique et créez une stratégie d'archivage des données rentable avec Amazon S3 Glacier et S3 Glacier Deep Archive.
- Développez des solutions de sauvegarde et de restauration évolutives, durables et sécurisées avec Amazon S3 et d'autres services AWS, tels que S3 Glacier et Amazon Elastic File System (Amazon EFS), afin d'augmenter ou de remplacer les fonctionnalités sur site existantes.

Plus de modèles

- Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform
- Répliquez des bases de données mainframe sur AWS à l'aide de Precisely Connect

Gestion

Rubriques

- Gestion des coûts
- Calcul haute performance
- Cloud hybride
- Gestion et gouvernance
- Messagerie et communications

Gestion des coûts

Rubriques

- Créez des rapports détaillés sur les coûts et l'utilisation des tâches AWS Glue à l'aide d'AWS Cost Explorer
- Créez des rapports détaillés sur les coûts et l'utilisation des clusters Amazon EMR à l'aide d'AWS Cost Explorer
- Plus de modèles

Créez des rapports détaillés sur les coûts et l'utilisation des tâches AWS Glue à l'aide d'AWS Cost Explorer

Créée par Parijat Bhide (AWS) et Aromal Raj Jayarajan (AWS)

Récapitulatif

Ce modèle montre comment suivre les coûts d'utilisation des tâches d'intégration de données AWS Glue en configurant des balises de répartition des coûts définies par l'utilisateur. Vous pouvez utiliser ces balises pour créer des rapports détaillés sur les coûts et l'utilisation dans AWS Cost Explorer pour des tâches à plusieurs dimensions. Par exemple, vous pouvez suivre les coûts d'utilisation au niveau de l'équipe, du projet ou du centre de coûts.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une ou plusieurs tâches AWS Glue pour lesquelles des balises définies par l'utilisateur sont activées

Architecture

Pile technologique cible

- AWS Glue
- AWS Cost Explorer

Le schéma suivant montre comment appliquer des balises pour suivre les coûts d'utilisation des tâches AWS Glue.

Le schéma suivant illustre le flux de travail suivant :

1. Un ingénieur de données ou un administrateur AWS crée des balises de répartition des coûts définies par l'utilisateur pour les tâches AWS Glue.
2. Un administrateur AWS active les balises.

3. Les balises transmettent les métadonnées à AWS Cost Explorer.

Outils

- AWS Glue est un service d'extraction, de transformation et de chargement (ETL) entièrement géré. Il vous aide à classer, nettoyer, enrichir et déplacer les données de manière fiable entre les magasins de données et les flux de données.
- AWS Cost Explorer vous permet de visualiser et d'analyser vos coûts et votre utilisation d'AWS.

Épopées

Créez et activez des balises pour vos tâches AWS Glue

Tâche	Description	Compétences requises
Créez des balises de répartition des coûts définies par l'utilisateur pour vos tâches AWS Glue.	Pour ajouter des balises à une tâche AWS Glue existante 1. Connectez-vous à la console de gestion AWS, puis ouvrez la console AWS Glue. 2. Dans le volet de navigation de gauche, sous ETL, sélectionnez Jobs. 3. Dans la section Vos tâches, choisissez le nom de la tâche que vous balisez. 4. Sélectionnez l'onglet Job details (Détails de la tâche). Développez ensuite la section Propriétés avancées. 5. Pour Tags, choisissez Ajouter un nouveau tag.	Ingénieur de données

Tâche	Description	Compétences requises
	6. Pour Key, saisissez le nom de votre tag. 7. (Facultatif) Dans Valeur, entrez la valeur que vous souhaitez associer à la clé. 8. (Facultatif) Répétez les étapes 5 à 7 pour chaque balise que vous souhaitez créer pour la tâche. 9. Choisissez Enregistrer. Pour ajouter des balises à une nouvelle tâche AWS Glue 1. Créez une nouvelle tâche AWS Glue en fonction des exigences de votre cas d'utilisation. Pour obtenir des instructions, consultez la section Travailler avec des tâches sur la console AWS Glue dans le manuel du développeur AWS Glue. 2. Lorsque vous configure z les paramètres relatifs aux détails de la tâche, suivez les étapes 4 à 9 de la section Pour ajouter des balises à une tâche AWS Glue existante de cette tâche.	

Tâche	Description	Compétences requises
	Note Pour plus d'informations, consultez les balises AWS dans AWS Glue dans le manuel AWS Glue Developer Guide.	
Activez les balises de répartition des coûts définies par l'utilisateur.	Suivez les instructions de la section Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de l'utilisateur d'AWS Billing.	Administrateur AWS

Créez des rapports sur les coûts et l'utilisation de vos tâches AWS Glue

Tâche	Description	Compétences requises
Créez des rapports sur les coûts et l'utilisation de vos tâches AWS Glue à l'aide de filtres de balises dans AWS Cost Explorer.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Cost Management. 2. Dans le volet de navigation de gauche, choisissez Rapports. 3. Choisissez Créer un nouveau rapport. 4. Pour Sélectionner un type de rapport, sélectionnez Coût et utilisation	AWS général, administrateur AWS

Tâche	Description	Compétences requises
	(recommandé). Choisissez ensuite Create Report. 5. Pour les filtres, sélectionnez Service. La liste déroulante Service apparaît. 6. Cochez les cases situées à côté de Glue. Choisissez ensuite Appliquer les filtres. 7. Pour les filtres, choisissez Tag. La liste déroulante Tag apparaît. 8. Choisissez l'équipe. Cochez ensuite les cases à côté des équipes auxquelles vous avez attribué des tags. Excluez toutes les équipes auxquelles vous n'avez pas attribué de tags. Choisissez ensuite Appliquer les filtres. 9. En haut du graphique, choisissez Tag. Choisisse z ensuite les balises pour les tâches AWS Glue pour lesquelles vous souhaitez créer un rapport. 10. En haut du graphique, choisissez la liste déroulant e des 3 derniers mois et choisissez la période que vous souhaitez couvrir dans le rapport. Choisisse z ensuite le menu déroulant Mensuel et choisisse z la manière dont vous	

Tâche	Description	Compétences requises
	souhaitez que les éléments du rapport soient agrégés en fonction de la période. 11. Choisissez Save as (Enregistrer sous). Entrez ensuite le titre de votre rapport. 12. Choisissez Enregistrer le rapport. Pour plus d'informations, consultez la section Exploration de vos données à l'aide de Cost Explorer dans le guide de l'utilisateur d'AWS Cost Management.	

Créez des rapports détaillés sur les coûts et l'utilisation des clusters Amazon EMR à l'aide d'AWS Cost Explorer

Créée par Parijat Bhide (AWS) et Aromal Raj Jayarajan (AWS)

Récapitulatif

Ce modèle montre comment suivre les coûts d'utilisation des clusters Amazon EMR en configurant des balises de répartition des coûts définies par l'utilisateur. Vous pouvez utiliser ces balises pour créer des rapports détaillés sur les coûts et l'utilisation dans AWS Cost Explorer pour les clusters à plusieurs dimensions. Par exemple, vous pouvez suivre les coûts d'utilisation au niveau de l'équipe, du projet ou du centre de coûts.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un ou plusieurs clusters EMR dont les balises définies par l'utilisateur sont activées

Architecture

Pile technologique cible

- Amazon EMR
- AWS Cost Explorer

Architecture cible

Le schéma suivant montre comment appliquer des balises pour suivre les coûts d'utilisation de clusters Amazon EMR spécifiques.

Le schéma suivant illustre le flux de travail suivant :

1. Un ingénieur de données ou un administrateur AWS crée des balises de répartition des coûts définies par l'utilisateur pour les clusters Amazon EMR.
2. Un administrateur AWS active les balises.
3. Les balises transmettent les métadonnées à AWS Cost Explorer.

Outils

Outils

- Amazon EMR est une plate-forme de cluster gérée qui simplifie l'exécution de frameworks de mégadonnées sur AWS afin de traiter et d'analyser de grandes quantités de données.
- AWS Cost Explorer vous permet de visualiser et d'analyser vos coûts et votre utilisation d'AWS.

Épopées

Créez et activez des balises pour vos clusters Amazon EMR

Tâche	Description	Compétences requises
Créez des balises de répartition des coûts définies par l'utilisateur pour vos clusters Amazon EMR.	Pour ajouter des balises à un cluster Amazon EMR existant Suivez les instructions de la section Ajouter des balises à un cluster existant dans le guide de gestion Amazon EMR. Pour ajouter des balises à un nouveau cluster Amazon EMR Suivez les instructions de la section Ajouter des balises à un nouveau cluster dans le guide de gestion Amazon EMR. Pour plus d'informations sur la configuration d'un cluster Amazon EMR, consultez la section Planifier et configurer des clusters dans le guide de gestion Amazon EMR.	Ingénieur de données

Tâche	Description	Compétences requises
Activez les balises de répartition des coûts définies par l'utilisateur.	Suivez les instructions de la section Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de l'utilisateur d'AWS Billing.	Administrateur AWS

Créez des rapports de coûts et d'utilisation pour vos clusters Amazon EMR

Tâche	Description	Compétences requises
Créez des rapports sur les coûts et l'utilisation de vos clusters Amazon EMR à l'aide de filtres de balises dans AWS Cost Explorer.	1. Connectez-vous à l'AWS Management Console et ouvrez la console AWS Cost Management. 2. Dans le volet de navigation de gauche, choisissez Rapports. 3. Choisissez Créer un nouveau rapport. 4. Pour Sélectionner un type de rapport, sélectionnez Coût et utilisation (recommandé). Choisissez ensuite Create Report. 5. Pour les filtres, sélectionnez Service. La liste déroulante Service apparaît. 6. Cochez les cases situées à côté de EMR (Elastic MapReduce) et EC2-Instances (Elastic Compute Cloud — Compute).	AWS général, administrateur AWS

Tâche	Description	Compétences requises
	Choisissez ensuite Appliquer les filtres. 7. Pour les filtres, choisissez Tag. La liste déroulante Tag apparaît. 8. Choisissez l'équipe. Cochez ensuite les cases à côté des équipes auxquelles vous avez attribué des tags. Excluez toutes les équipes auxquelles vous n'avez pas attribué de tags. Choisissez ensuite Appliquer les filtres. 9. En haut du graphique, choisissez Tag. Choisissez ensuite les balises pour les clusters Amazon EMR pour lesquels vous souhaitez créer un rapport. 10. En haut du graphique, choisissez la liste déroulante des 3 derniers mois et choisissez la période que vous souhaitez couvrir dans le rapport. Choisissez ensuite le menu déroulant Mensuel et choisissez la manière dont vous souhaitez que les éléments du rapport soient agrégés en fonction de la période. 11. Choisissez Save as (Enregistrer sous). Entrez	

Tâche	Description	Compétences requises
	ensuite le titre de votre rapport. 12. Choisissez Enregistrer le rapport. Pour plus d'informations, consultez la section Exploration de vos données à l'aide de Cost Explorer dans le guide de l'utilisateur d'AWS Cost Management.	

Plus de modèles

- Automatisez AWS les opérations d'infrastructure en utilisant Amazon Bedrock
- Inventaire automatique AWS des ressources sur plusieurs comptes et régions
- Automatisez la création de ressources AppStream 2.0 à l'aide d'AWS CloudFormation
- Archivez automatiquement les éléments sur Amazon S3 à l'aide de DynamoDB TTL
- Arrêtez et démarrez automatiquement une instance de base de données Amazon RDS à l'aide de AWS Systems Manager Maintenance Windows
- Créez des rapports détaillés sur les coûts et l'utilisation pour Amazon RDS et Amazon Aurora
- Supprimez les volumes Amazon EBS inutilisés en utilisant AWS Config et AWS Systems Manager
- Estimation des coûts de stockage pour une table Amazon DynamoDB
- Estimation du coût d'une table DynamoDB pour une capacité à la demande
- Configurez le dimensionnement automatique piloté par les événements dans Amazon EKS à l'aide d'Amazon EKS Pod Identity et KEDA
- Coordonnez la dépendance des ressources et l'exécution des tâches à l'aide de la structure AWS Fargate WaitCondition hook

Calcul haute performance

Rubriques

- Déployez un système de fichiers Lustre pour un traitement des données performant à l'aide de Terraform et DRA
- Configurer un tableau de bord de surveillance Grafana pour AWS ParallelCluster
- Configurez une infrastructure de bureau virtuel à scalabilité automatique à l'aide de NICE EnginFrame et de NICE DCV Session Manager

Déployez un système de fichiers Lustre pour un traitement des données performant à l'aide de Terraform et DRA

Créée par Arun Bagal (AWS) et Ishwar Chauthaiwale (AWS)

Récapitulatif

Ce modèle déploie automatiquement un système de fichiers Lustre AWS et l'intègre à Amazon Elastic Compute Cloud (Amazon EC2) et Amazon Simple Storage Service (Amazon S3).

Cette solution vous permet de configurer rapidement un environnement de calcul haute performance (HPC) avec stockage intégré, ressources de calcul et accès aux données Amazon S3. Il combine les capacités de stockage de Lustre aux options de calcul flexibles proposées par Amazon EC2 et au stockage d'objets évolutif d'Amazon S3, afin que vous puissiez gérer les charges de travail gourmandes en données dans les domaines de l'apprentissage automatique, du HPC et de l'analyse des mégadonnées.

Le modèle utilise un module HashiCorp Terraform et Amazon FSx for Lustre pour rationaliser le processus suivant :

- Approvisionnement d'un système de fichiers Lustre
- Établissement d'une association de référentiel de données (DRA) entre FSx for Lustre et un compartiment S3 afin de relier le système de fichiers Lustre aux objets Amazon S3
- Création d'une EC2 instance
- Montage du système de fichiers Lustre avec le DRA lié à Amazon S3 sur l'instance EC2

Les avantages de cette solution incluent :

- Conception modulaire. Vous pouvez facilement gérer et mettre à jour les différents composants de cette solution.
- Scalabilité. Vous pouvez rapidement déployer des environnements cohérents entre Comptes AWS nos régions.
- Flexibilité. Vous pouvez personnaliser le déploiement en fonction de vos besoins spécifiques.
- Les meilleures pratiques. Ce modèle utilise des modules préconfigurés qui suivent les AWS meilleures pratiques.

Pour plus d'informations sur les systèmes de fichiers Lustre, consultez le site Web de Lustre.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Une politique de moindre privilège AWS Identity and Access Management (IAM) (voir les instructions)

Limites

FSx for Lustre limite le système de fichiers Lustre à une seule zone de disponibilité, ce qui peut poser problème si vous avez des exigences de haute disponibilité. En cas de défaillance de la zone de disponibilité contenant le système de fichiers, l'accès au système de fichiers est perdu jusqu'à la restauration. Pour atteindre une haute disponibilité, vous pouvez utiliser DRA pour relier le système de fichiers Lustre à Amazon S3 et transférer des données entre les zones de disponibilité.

Versions du produit

- Terraform version 1.9.3 ou ultérieure
- HashiCorp AWS Provider version 4.0.0 ou ultérieure

Architecture

Le schéma suivant montre l'architecture FSx de Lustre et la complémentarité Services AWS de AWS Cloud.

L'architecture inclut les éléments suivants :

- Un compartiment S3 est utilisé comme emplacement de stockage durable, évolutif et rentable pour les données. L'intégration entre FSx for Lustre et Amazon S3 fournit un système de fichiers performant qui est parfaitement lié à Amazon S3.
- FSx for Lustre exécute et gère le système de fichiers Lustre.
- Amazon CloudWatch Logs collecte et surveille les données des journaux à partir du système de fichiers. Ces journaux fournissent des informations sur les performances, l'état et l'activité de votre système de fichiers Lustre.
- Amazon EC2 est utilisé pour accéder aux systèmes de fichiers Lustre à l'aide du client Lustre open source. EC2 les instances peuvent accéder aux systèmes de fichiers depuis d'autres zones de

disponibilité au sein du même cloud privé virtuel (VPC). La configuration réseau permet l'accès à travers les sous-réseaux du VPC. Une fois le système de fichiers Lustre monté sur l'instance, vous pouvez utiliser ses fichiers et ses répertoires comme vous le feriez avec un système de fichiers local.

- AWS Key Management Service (AWS KMS) améliore la sécurité du système de fichiers en cryptant les données au repos.

Automatisation et évolutivité

Terraform facilite le déploiement, la gestion et le dimensionnement de vos systèmes de fichiers Lustre dans plusieurs environnements. Dans FSx Lustre, la taille d'un seul système de fichiers étant limitée, vous devrez peut-être effectuer une mise à l'échelle horizontale en créant plusieurs systèmes de fichiers. Vous pouvez utiliser Terraform pour provisionner plusieurs systèmes de fichiers Lustre en fonction de vos besoins en matière de charge de travail.

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon FSx for Lustre permet de lancer, d'exécuter et de faire évoluer facilement et à moindre coût un système de fichiers Lustre à hautes performances.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel Provision FSx for GitHub Lustre à l'aide de Terraform.

Bonnes pratiques

- Les variables suivantes définissent le système de fichiers Lustre. Assurez-vous de les configurer correctement en fonction de votre environnement, comme indiqué dans la section Epics.
  - `storage_capacity`— La capacité de stockage du système de fichiers Lustre, en GiBs. Le paramètre minimum et par défaut est de 1200 GiB.
  - `deployment_type`— Type de déploiement du système de fichiers Lustre. Pour une explication des deux options, `PERSISTENT_1` et `PERSISTENT_2` (par défaut), consultez la documentation de FSx for Lustre.
  - `per_unit_storage_throughput`— Le débit de lecture et d'écriture, en secondes MBs par TiB.
  - `subnet_id`— L'ID du sous-réseau privé dans lequel vous souhaitez déployer FSx Lustre.
  - `vpc_id`— L'ID de votre cloud privé virtuel sur AWS lequel vous souhaitez déployer FSx Lustre.
  - `data_repository_path`— Le chemin d'accès au compartiment S3 qui sera lié au système de fichiers Lustre.
  - `iam_instance_profile`— Le profil d'instance IAM à utiliser pour lancer l' EC2 instance.
  - `kms_key_id`— Le nom de ressource Amazon (ARN) de la AWS KMS clé qui sera utilisée pour le chiffrement des données.
- Garantissez un accès réseau et un positionnement appropriés au sein du VPC en utilisant les variables `security_group` et`vpc_id`.
- Exécutez la `terraform plan` commande comme décrit dans la section Epics pour prévisualiser et vérifier les modifications avant de les appliquer. Cela permet de détecter les problèmes potentiels et de garantir que vous êtes au courant de ce qui sera déployé.
- Utilisez la `terraform validate` commande décrite dans la section Epics pour vérifier les erreurs de syntaxe et vérifier que votre configuration est correcte.

Épopées

Configuration de votre environnement

Tâche	Description	Compétences requises
Installez Terraform.	Pour installer Terraform sur votre machine locale,	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	suivez les instructions de la documentation Terraform.	
Configurez les AWS informations d'identification.	Pour configurer le profil AWS Command Line Interface (AWS CLI) du compte, suivez les instructions de la AWS documentation.	AWS DevOps, DevOps ingénieur
Clonez le GitHub dépôt.	Pour cloner le GitHub dépôt, exécutez la commande suivante : `git clone https://github.com/aws-samples/provision-fsx-lustre-with-terraform.git`	AWS DevOps, DevOps ingénieur

Configuration et déploiement FSx pour Lustre

Tâche	Description	Compétences requises
Mettez à jour la configuration de déploiement.	1. Dans le référentiel cloné de votre machine locale, accédez au `fsx_deployment` répertoire : `cd fsx_deployment` 2. Ouvrez le `terraform.tfvars` fichier et mettez à jour les valeurs des variables suivantes : • `vpc_id`	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises
	• `subnet_id` • `data_repository_path` • `iam_instance_profile` • `kms_key_id` Pour une description de ces variables, consultez la section Bonnes pratiques. 3. Dans le même répertoire, ouvrez le `locals.tf` fichier et mettez à jour les plages CIDR pour les variables du groupe `fsx_egress` de sécurité `fsx_inress` et. 4. Si nécessaire, ouvrez le `variables.tf` fichier et mettez à jour les valeurs par défaut de ces variables : • `storage_capacity` • `deployment_type` • `per_unit_storage_throughput` Pour une description de ces variables, consultez la section Bonnes pratiques.	

Tâche	Description	Compétences requises
Initialisez l'environnement Terraform.	Pour initialiser votre environnement afin d'exécuter le `fsx_deployment` module Terraform, exécutez : `terraform init`	AWS DevOps, DevOps ingénieur
Validez la syntaxe Terraform.	Pour vérifier les erreurs de syntaxe et vérifier que votre configuration est correcte, exécutez : `terraform validate`	AWS DevOps, DevOps ingénieur
Validez la configuration Terraform.	Pour créer un plan d'exécution Terraform et prévisualiser le déploiement, exécutez : `terraform plan -var-file terraform.tfvars`	AWS DevOps, DevOps ingénieur
Déployez le module Terraform .	Pour déployer les ressources FSx for Lustre, exécutez : `terraform apply -var-file terraform.tfvars`	AWS DevOps, DevOps ingénieur

Nettoyer les AWS ressources

Tâche	Description	Compétences requises
Supprimez AWS des ressources.	Une fois que vous avez fini d'utiliser votre environnement FSx for Lustre, vous pouvez	AWS DevOps, DevOps ingénieur

Tâche	Description	Compétences requises

	supprimer les AWS ressources déployées par Terraform pour éviter d'encourir des frais inutiles. Le module Terraform fourni dans le référentiel de code automatise ce nettoyage.
	1. Dans votre dépôt local, accédez au `fsx_deployment` répertoire :
	`cd fsx_deployment`
	2. Exécutez la commande :
	`terraform destroy -var-file terraform.tfvars`	

Résolution des problèmes

Problème	Solution
FSx pour Lustre renvoie des erreurs.	Pour obtenir de l'aide concernant FSx les problèmes liés à Lustre, consultez la section Résolution des problèmes liés à Amazon FSx for Lustre dans la FSx documentation relative à Lustre.

Ressources connexes

- Création d'Amazon FSx pour Lustre à l'aide de Terraform (référence du AWS fournisseur dans la documentation Terraform)
- Commencer à utiliser Amazon FSx pour Lustre (FSx pour la documentation Lustre)

- AWS articles de blog sur Amazon FSx pour Lustre

Configurer un tableau de bord de surveillance Grafana pour AWS ParallelCluster

Créée par Dario La Porta (AWS) et William Lu (AWS)

Récapitulatif

AWS vous ParallelCluster aide à déployer et à gérer des clusters de calcul haute performance (HPC). Il prend en charge les planificateurs de tâches open source AWS Batch et Slurm. Bien qu'AWS ParallelCluster soit intégré à Amazon CloudWatch pour la journalisation et les métriques, il ne fournit pas de tableau de bord de surveillance pour la charge de travail.

Le tableau de bord Grafana pour AWS ParallelCluster (GitHub) est un tableau de bord de surveillance pour AWS. ParallelCluster Il fournit des informations sur le planificateur de tâches et des mesures de surveillance détaillées au niveau du système d'exploitation (OS). Pour plus d'informations sur les tableaux de bord inclus dans cette solution, consultez la section Exemples de tableaux de bord dans le GitHub référentiel. Ces indicateurs vous aident à mieux comprendre la charge de travail HPC et ses performances. Cependant, le code du tableau de bord n'est pas mis à jour pour les dernières versions d'AWS ParallelCluster ni pour les packages open source utilisés dans la solution. Ce modèle améliore la solution pour offrir les avantages suivants :

- Compatible avec AWS ParallelCluster v3
- Utilise la dernière version des packages open source, notamment Prometheus, Grafana, Prometheus Slurm Exporter et NVIDIA DCGM-Exporter
- Augmente le nombre de cœurs de processeur utilisés par GPUs les tâches Slurm
- Ajoute un tableau de bord de suivi des tâches
- Améliore le tableau de bord de surveillance des nœuds GPU pour les nœuds dotés de 4 ou 8 unités de traitement graphique (GPUs)

Cette version de la solution améliorée a été mise en œuvre et vérifiée dans l'environnement de production HPC d'un client AWS.

Conditions préalables et limitations

Prérequis

- ParallelCluster CLI AWS, installée et configurée.

- Configuration réseau prise en charge pour AWS ParallelCluster. Ce modèle utilise l'AWS ParallelCluster en utilisant une configuration de deux sous-réseaux, qui nécessite un sous-réseau public, un sous-réseau privé, une passerelle Internet et une passerelle NAT.
- Tous les nœuds ParallelCluster du cluster AWS doivent disposer d'un accès à Internet. Cela est nécessaire pour que les scripts d'installation puissent télécharger le logiciel open source et les images Docker.
- Une paire de clés dans Amazon Elastic Compute Cloud (Amazon EC2). Les ressources dotées de cette paire de clés ont un accès Secure Shell (SSH) au nœud principal.

Limites

- Ce modèle est conçu pour prendre en charge Ubuntu 20.04 LTS. Si vous utilisez une autre version d'Ubuntu ou si vous utilisez Amazon Linux ou CentOS, vous devez modifier les scripts fournis avec cette solution. Ces modifications ne sont pas incluses dans ce modèle.

Versions du produit

- Ubuntu 20.04 LTS
- ParallelCluster 3. X

Considérations relatives à la facturation et aux coûts

- La solution déployée selon ce modèle n'est pas couverte par le niveau gratuit. Des frais s'appliquent pour Amazon EC2, Amazon FSx for Lustre, la passerelle NAT d'Amazon VPC et Amazon Route 53.

Architecture

Architecture cible

Le schéma suivant montre comment un utilisateur peut accéder au tableau de bord de surveillance d'AWS ParallelCluster sur le nœud principal. Le nœud principal exécute NICE DCV, Prometheus, Grafana, Prometheus Slurm Exporter, Prometheus Node Exporter et NGINX Open Source. Les nœuds de calcul exécutent Prometheus Node Exporter, et ils exécutent également NVIDIA DCGM-Exporter si le nœud contient. GPUs Le nœud principal récupère les informations des nœuds de calcul et affiche ces données dans le tableau de bord Grafana.

Dans la plupart des cas, le nœud principal n'est pas très chargé car le planificateur de tâches ne nécessite pas une quantité importante de processeur ou de mémoire. Les utilisateurs accèdent au tableau de bord sur le nœud principal en utilisant le protocole SSL sur le port 443.

Tous les spectateurs autorisés peuvent consulter les tableaux de bord de surveillance de manière anonyme. Seul l'administrateur de Grafana peut modifier les tableaux de bord. Vous configurez un mot de passe pour l'administrateur Grafana dans le `aws-parallelcluster-monitoring/docker-compose/docker-compose.head.yml` fichier.

Outils

Services AWS

- NICE DCV est un protocole d'affichage à distance hautes performances qui vous permet de diffuser des postes de travail distants et des applications depuis n'importe quel cloud ou centre de données vers n'importe quel appareil, dans des conditions de réseau variables.
- AWS vous ParallelCluster aide à déployer et à gérer des clusters de calcul haute performance (HPC). Il prend en charge les planificateurs de tâches open source AWS Batch et Slurm.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini.

Autres outils

- Docker est un ensemble de produits de plateforme en tant que service (PaaS) qui utilisent la virtualisation au niveau du système d'exploitation pour fournir des logiciels dans des conteneurs.
- Grafana est un logiciel open source qui vous permet d'interroger, de visualiser, d'alerter et d'explorer les métriques, les journaux et les traces.
- NGINX Open Source est un serveur Web open source et un proxy inverse.
- NVIDIA Data Center GPU Manager (DCGM) est une suite d'outils permettant de gérer et de surveiller les unités de traitement graphique des centres de données NVIDIA (GPUs) dans des environnements de clusters. Dans ce modèle, vous utilisez DCGM-Exporter, qui vous permet d'exporter les métriques du GPU depuis Prometheus.

- Prometheus est une boîte à outils open source de surveillance des systèmes qui collecte et stocke ses métriques sous forme de séries chronologiques associées à des paires clé-valeur, appelées étiquettes. Dans ce modèle, vous utilisez également Prometheus Slurm Exporter pour collecter et exporter des métriques, et vous utilisez Prometheus Node Exporter pour exporter des métriques depuis les nœuds de calcul.
- Ubuntu est un système d'exploitation open source basé sur Linux conçu pour les serveurs d'entreprise, les ordinateurs de bureau, les environnements cloud et l'IoT.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub pcluster-monitoring-dashboardréférentiel.

Épopées

Créez les ressources nécessaires

Tâche	Description	Compétences requises
Créez un compartiment S3.	Créez un compartiment Amazon S3. Vous utilisez ce compartiment pour stocker les scripts de configuration. Pour obtenir des instructions, consultez la section Création d'un compartiment dans la documentation Amazon S3.	AWS général
Pour cloner le référentiel.	Clonez le GitHub pcluster-monitoring-dashboarddépôt en exécutant la commande suivante. `git clone https://github.com/aws-samples/parallelcluster-monitoring-dashboard.git`	DevOps ingénieur

Tâche	Description	Compétences requises
Créez un mot de passe administrateur.	1. Choisissez le `aws-parallelcluster-monitoring` dossier, puis ouvrez le `docker-compose` fichier docker-compose.head.yml. 2. Dans la `GF_SECURITY_ADMIN_PASSWORD` variable, remplacez-le `Grafana4PC!` par le mot de passe de votre choix. Il s'agit du mot de passe administratif que vous utilisez pour gérer le compte Grafana. 3. Enregistrez et fermez le fichier docker-compose.head.yml.	Scriptage de scripts Linux Shell
Copiez les fichiers requis dans le compartiment S3.	Copiez le script post_install.sh et le aws-parallelcluster-monitoringdossier dans le compartiment S3 que vous avez créé. Pour obtenir des instructions, consultez la section Chargement d'objets dans la documentation Amazon S3.	AWS général

Tâche	Description	Compétences requises
Configurez un groupe de sécurité supplémentaire pour le nœud principal.	1. Créez un groupe de sécurité pour le nœud principal. Ce groupe de sécurité autorisera le trafic entrant vers les tableaux de bord de surveillance du nœud principal. Pour obtenir des instructions, consultez la section Créer un groupe de sécurité dans la documentation Amazon VPC. 2. Ajoutez une règle entrante au groupe de sécurité. Pour obtenir des instructions, consultez la section Ajouter des règles à un groupe de sécurité dans la documentation Amazon VPC. Utilisez les paramètres suivants pour la règle : • Type : HTTPS • Protocole — TCP • Portée de ports : 443 • Source — Entrez votre adresse IP • Description — Autoriser les utilisateurs à accéder au tableau de bord de surveillance	Administrateur AWS

Tâche	Description	Compétences requises
Configurez une politique IAM pour le nœud principal.	Créez une politique basée sur l'identité pour le nœud principal. Cette politique permet au nœud de récupérer des données métriques auprès d'Amazon CloudWatch. Le GitHub dépôt contient un exemple de politique. Pour obtenir des instructions, consultez la section Création de politiques IAM dans la documentation AWS Identity and Access Management (IAM).	Administrateur AWS

Tâche	Description	Compétences requises
Configurez une politique IAM pour les nœuds de calcul.	Créez une politique basée sur l'identité pour les nœuds de calcul. Cette politique permet au nœud de créer les balises contenant l'ID de la tâche et le propriétaire de la tâche. Le GitHub dépôt contient un exemple de politique. Pour obtenir des instructions, consultez la section Création de politiques IAM dans la documentation IAM. Si vous utilisez le fichier d'exemple fourni, remplacez les valeurs suivantes : • <REGION>— La région AWS où le cluster est hébergé • <ACCOUNT_ID>— L'identifiant du compte AWS	Administrateur AWS

Créer le cluster

Tâche	Description	Compétences requises
Modifiez le fichier de modèle de cluster fourni.	Créez le ParallelCluster cluster AWS. Utilisez le fichier modèle CloudFormation AWS cluster.yaml fourni comme point de départ pour créer le cluster. Remplacez les valeurs	Administrateur AWS

Tâche	Description	Compétences requises
	suivantes dans le modèle fourni : • <REGION>— La région AWS dans laquelle le cluster est hébergé. • <HEADNODE_SUBNET> — Le sous-réseau public du VPC. • <ADDITIONAL_HEAD_NODE_SG>— Le nom du groupe de sécurité que vous avez créé pour le nœud principal. • <KEY_NAME>— Entrez le nom d'une paire de EC2 clés Amazon existante. Les ressources dotées de cette paire de clés ont un accès Secure Shell (SSH) au nœud principal. • <ALLOWED_IPS>- — Entrez la plage d'adresses IP au format CIDR autorisée à établir des connexions SSH avec le nœud principal. • <ADDITIONAL_HEAD_NODE_POLICY>— Entrez le nom de la politique IAM que vous avez créée pour le nœud principal. • <BUCKET_NAME>— Entrez le nom du compartiment S3 que vous avez créé.	

Tâche	Description	Compétences requises
	• <COMPUTE_SUBNET>— Entrez le nom du sous-rése au privé dans le VPC. • <ADDITIONAL_COMPUTE_NODE_POLICY>— Entrez le nom de la politique IAM que vous avez créée pour le nœud de calcul.	
Créez le cluster .	Dans la ParallelCluster CLI AWS, entrez la commande suivante. Cela permet de déployer le CloudFormation modèle et de créer le cluster. Pour plus d'informations sur cette commande, consultez pcluster create-cluster dans la documentation AWS. ParallelCluster `pcluster create-cluster -n <cluster_name> -c cluster.yaml`	Administrateur AWS
Surveillez la création du cluster.	Entrez la commande suivante pour surveiller la création du cluster. Pour plus d'informations sur cette commande, consultez pcluster describe-cluster dans la documentation AWS. ParallelCluster `pcluster describe-cluster -n <cluster_name>`	Administrateur AWS

Utilisation des tableaux de bord Grafana

Tâche	Description	Compétences requises
Accès au portail Grafana.	1. Entrez la commande suivante pour récupérer l'adresse IP publique du nœud principal. `pcluster describe-cluster -n <cluster_name> --query headNode.publicIpAddress` 2. Dans un navigateur Web, accédez à l'URL suivante pour accéder au tableau de bord Grafana. https ://<head_node_public_ip_address> 3. Sur la page d'accueil de Grafana, choisissez l'icône du tableau de bord à 4 carrés dans le menu de gauche, puis choisissez Général. Cela affiche une liste des tableaux de bord configurés. Les tableaux de bord suivants sont disponibles dans Grafana : • Coût du cluster : contient des informations sur le coût du cluster • Journaux du cluster : contient des informati	Administrateur AWS

Tâche	Description	Compétences requises
	ons sur les journaux du cluster • Détails des nœuds de calcul : contient des informations sur les statistiques d'utilisation des nœuds de calcul • Liste des nœuds de calcul : contient la liste des nœuds de calcul du cluster • Nœuds GPU : contient des informations sur les statistiques d'utilisation des nœuds GPU • Détails des tâches : contient des informati ons sur l'utilisation des ressources des tâches • Détails du nœud principal : contient des informati ons sur les statistiques d'utilisation du nœud principal • ParallelCluster Résumé : contient des informations sur l'utilisation du cluster	

Nettoyez la solution pour ne plus encourir de coûts associés

Tâche	Description	Compétences requises
Supprimez le cluster.	Entrez la commande suivante pour supprimer le cluster. Pour plus d'informations sur cette commande, consultez pcluster delete-cluster dans la documentation AWS. ParallelCluster `pcluster delete-cluster -n <cluster_name>`	Administrateur AWS
Supprimez les politiques IAM.	Supprimez les politiques que vous avez créées pour le nœud principal et le nœud de calcul. Pour plus d'informations sur la suppression de politiques, consultez la section Suppression de politiques IAM dans la documentation IAM.	Administrateur AWS
Supprimez le groupe de sécurité et la règle.	Supprimez le groupe de sécurité que vous avez créé pour le nœud principal. Pour plus d'informations, consultez Supprimer les règles du groupe de sécurité et Supprimer un groupe de sécurité dans la documentation Amazon VPC.	Administrateur AWS
Supprimez le compartiment S3.	Supprimez le compartiment S3 que vous avez créé pour stocker les scripts de	AWS général

Tâche	Description	Compétences requises
	configuration. Pour plus d'informations, consultez Supprimer un compartiment dans la documentation Amazon S3.	

Résolution des problèmes

Problème	Solution
Le nœud principal n'est pas accessible dans le navigateur.	Vérifiez le groupe de sécurité et confirmez que le port entrant 443 est ouvert.
Grafana ne s'ouvre pas.	Sur le nœud principal, vérifiez le journal du conteneur pour`docker logs Grafana`.
Certaines mesures ne contiennent aucune donnée.	Sur le nœud principal, vérifiez les journaux de tous les conteneurs.

Ressources connexes

Documentation AWS

- Politiques IAM pour Amazon EC2

Autres ressources AWS

- AWS ParallelCluster
- Tableau de bord de surveillance pour AWS ParallelCluster (article de blog AWS)

Autres ressources

- Système de surveillance Prometheus
- Grafana

Configurez une infrastructure de bureau virtuel à scalabilité automatique à l'aide de NICE EnginFrame et de NICE DCV Session Manager

Créée par Dario La Porta (AWS) et Salvatore Maccarone (AWS)

Récapitulatif

NICE DCV est un protocole d'affichage à distance hautes performances qui vous permet de diffuser des applications et des postes de travail distants depuis n'importe quel cloud ou centre de données vers n'importe quel appareil, quelles que soient les conditions du réseau. Avec NICE DCV et Amazon Elastic Compute Cloud EC2 (Amazon), vous pouvez exécuter à distance des applications gourmandes en graphismes sur des EC2 instances Amazon et diffuser leurs interfaces utilisateur sur des machines clientes distantes plus simples. Cela élimine le besoin de postes de travail dédiés coûteux et le besoin de transférer de grandes quantités de données entre le cloud et les machines clientes.

Ce modèle met en place une infrastructure de bureau virtuel (VDI) Linux et Windows entièrement fonctionnelle et à mise à l'échelle automatique, accessible via une interface utilisateur Web. La solution VDI fournit aux utilisateurs de la recherche et du développement (R&D) une interface utilisateur accessible et performante pour soumettre des demandes d'analyse gourmandes en graphismes et examiner les résultats à distance.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Des autorisations d'administrateur et un ensemble de clés d'accès.
- AWS Cloud Development Kit (AWS CDK) Boîte à outils, installée et configurée. Pour plus d'informations, veuillez consulter Installer l' AWS CDK.
- AWS Command Line Interface (AWS CLI), installé et configuré pour votre Compte AWS. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI.
- Python, installé et configuré. Pour plus d'informations, consultez la section Sources (site Web de Python).
- Un ou plusieurs clouds privés virtuels (VPCs) disponibles.
- Deux adresses IP élastiques ou plus sont disponibles. Pour plus d'informations sur la limite par défaut, consultez la section Limite d'adresses IP élastiques.

- Pour les EC2 instances Amazon Linux, configurez une paire de clés Secure Shell (SSH). Pour plus d'informations, consultez la section Paires de clés et instances Linux.

Versions du produit

- AWS CDK version 2.26.0 ou ultérieure
- Python version 3.8 ou ultérieure

Architecture

Architecture cible

La figure suivante montre les différents composants de cette solution VDI. L'utilisateur interagit avec NICE EnginFrame pour lancer des EC2 instances Amazon conformément aux groupes Amazon EC2 Auto Scaling pour les instances NICE DCV Windows et Linux.

Automatisation et mise à l'échelle

Le code inclus dans ce modèle crée un VPC personnalisé, des sous-réseaux publics et privés, une passerelle Internet, une passerelle NAT, un Application Load Balancer, des groupes de sécurité AWS Identity and Access Management et des politiques (IAM). AWS CloudFormation est également utilisé pour créer le parc de serveurs NICE DCV Linux et Windows.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- NICE DCV est un protocole d'affichage à distance hautes performances qui vous permet de diffuser des postes de travail distants et des applications depuis n'importe quel cloud ou centre de données vers n'importe quel appareil, dans des conditions de réseau variables. Dans ce modèle, il fournit une expérience économe en bande passante qui diffuse à distance des graphiques 3D de calcul haute performance (HPC).

- Le gestionnaire de sessions NICE DCV vous aide à créer et à gérer le cycle de vie des sessions NICE DCV sur un parc de serveurs NICE DCV.
- NICE EnginFrame est une interface Web frontale avancée permettant d'accéder à des applications techniques et scientifiques dans le cloud.

Référentiel de code

Le code de ce modèle est disponible dans la solution Auto Scaling VDI avec NICE EnginFrame et le référentiel NICE DCV Session Manager.

Épopées

Déployez l'infrastructure de bureau virtuel

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Clonez le dépôt contenant le code : `git clone https://github.com/aws-samples/elastic-vdi-infrastructure.git`	Architecte du cloud

Installez les AWS CDK bibliothèques requises.	Installez les AWS CDK bibliothèques :
	`cd elastic-vdi-infrastructure`
	`python3 -m venv .venv`
	`source .venv/bin/activate`
	`pip3 install -r requirements.txt`
		Architecte du cloud

Mettez à jour les paramètres.	1. Ouvrez le fichier app.py dans l'éditeur de texte de votre choix.	Architecte du cloud

Tâche	Description	Compétences requises
	2. Remplacez la `CHANGE_ME` valeur des paramètres obligatoires suivants : • `region`— La cible Région AWS. Pour obtenir la liste complète, consultez Régions AWS. • `account`— L'ID de la cible Compte AWS. Pour plus d'informations, consultez la section Trouver votre Compte AWS identifiant. • `key_name`— La paire de clés utilisée pour accéder aux EC2 instances Amazon Linux. 3. (Facultatif) Modifiez les valeurs des paramètres suivants afin de personnaliser la solution en fonction de votre environnement : • `ec2_type_enginframe` — Le type d' EnginFrame instance • `ec2_type_broker` — Le type d'instance de Session Manager Broker • `ebs_enginframe_size` — La taille du volume Amazon Elastic Block Store (Amazon	

Tâche	Description	Compétences requises
	EBS) pour l'instance EnginFrame • `ebs_broker_size` — La taille du volume Amazon EBS pour l'instance de Session Manager Broker • `TagName and TagValue`— L'étiquette de facturation pour les ressources • `efadmin_uid` — L'identifiant unique de l'utilisateur EnginFrame administrateur (efadmin) • `linux_shared_storage_size` — Taille d'OpenZFS en gibioctets (GiB) • `Shared_Storage_Linux` — Le point de montage du stockage partagé • `Enginframe_installer` — Le lien de téléchargement pour EnginFrame • `Session_Manager_Broker_Installer` — Le lien de téléchargement du Session Manager Broker	

Tâche	Description	Compétences requises
	4. Enregistrez et fermez le fichier app.py.	

Déployez la solution.	Exécutez les commandes suivantes dans l'ordre :
	`cdk bootstrap`
	`cdk deploy Assets-Stack Parameters-Stack`
	`cdk deploy Elastic-Vdi-Infrastructure`
	Lorsque le déploiement est terminé, les deux sorties suivantes sont renvoyées :
	• `Elastic-Vdi-Infrastructure.EnginFrameURL` — L'adresse HTTPS du EnginFrame portail
	• `Elastic-Vdi-InfrastruSecretEFadminPassword` — Le nom de ressource Amazon (ARN) du secret qui contient le mot de passe de l'utilisateur efadmin
	Prenez note de ces valeurs. Vous les utiliserez plus tard dans ce modèle.
		Architecte du cloud

Tâche	Description	Compétences requises
Déployez le parc de serveurs Linux.	1. Connectez-vous à la AWS Management ConsoleCloudFormation console et ouvrez-la. 2. Choisissez Créer une pile, puis choisissez Avec de nouvelles ressources. 3. Dans le dossier cloudform ation_files, sélectionnez le fichier .yaml. dcv-linux-fleet 4. Sur la page Spécifier les détails de la pile, définissez les paramètres suivants : • Nom de la pile : nom de la pile. • DcvFleet— Le nom de la flotte de DCV NICE. Ne laissez pas cette valeur vide et n'utilisez pas d'espaces. • InstanceType— Le type d'instance de la flotte. • RootVolumeSize— La taille du volume racine de l' EC2 instance Amazon Linux. • MinSize— Le nombre minimum de nœuds qui doivent être disponibl es et ne pas exécuter de session DCV. Par exemple, si vous entrez2, la solution commence	Architecte du cloud

Tâche	Description	Compétences requises
	avec 2 nœuds. Lorsqu'un utilisateur crée une session, le nombre de nœuds disponibles diminue à1, et la solution crée un autre nœud pour maintenir le minimum. • MaxSize— Le nombre maximum de nœuds dans le parc. Les utilisateurs ne peuvent pas démarrer de nouvelles sessions si le maximum a été atteint. • BillingTagName— Le nom du tag utilisé pour la facturation. Ce nom de balise doit être différent de celui utilisé pour la pile Windows. • BillingTagValue— La valeur du tag utilisé pour la facturation. 5. Complétez l'assistant de création de pile, puis choisissez Soumettre pour commencer à créer la pile.	

Tâche	Description	Compétences requises
Déployez le parc de serveurs Windows.	1. Connectez-vous à la AWS Management ConsoleCloudFormation console et ouvrez-la. 2. Choisissez Créer une pile, puis choisissez Avec de nouvelles ressources. 3. Dans le dossier cloudform ation_files, sélectionnez le fichier .yaml. dcv-windows-fleet 4. Sur la page Spécifier les détails de la pile, définissez les paramètres suivants : • Nom de la pile : nom de la pile. • DcvFleet— Le nom de la flotte de DCV NICE. Ne laissez pas cette valeur vide et n'utilisez pas d'espaces. • InstanceType— Le type d'instance de la flotte. • RootVolumeSize— La taille du volume racine de l' EC2 instance Amazon Windows. • MinSize— Le nombre minimum de nœuds qui doivent être disponibles et ne pas exécuter de session DCV.	Architecte du cloud

Tâche	Description	Compétences requises
	• MaxSize— Le nombre maximum de nœuds dans le parc. • BillingTagName— Le nom du tag utilisé pour la facturation. Ce nom de balise doit être différent de celui utilisé pour la pile Linux. • BillingTagValue— La valeur du tag utilisé pour la facturation. 5. Complétez l'assistant de création de pile, puis choisissez Soumettre pour commencer à créer la pile.	

Accédez à l'environnement déployé

Tâche	Description	Compétences requises
Récupérez le mot de passe EnginFrame administrateur.	Le compte d' EnginFram e administration s'appelle efadmin et le mot de passe y est enregistré en AWS Secrets Manager tant que secret. L'ARN du secret est généré dynamiquement et est visible dans le résultat du AWS CDK déploiement. 1. Dans l'épopée précédent e, dans l'histoire Déployez la solution, sous le	Architecte du cloud

Tâche	Description	Compétences requises
	`Elastic-Vdi-Infrastructure.SecretEFAdminPassword` résultat, trouvez l'ARN du secret généré. 2. Procédez de l'une des manières suivantes pour récupérer le secret : • Utilisez la console Secrets Manager. Pour plus d'informations, consultez la section Récupérer des secrets. • Entrez la commande get-secret-value . `aws secretsmanager get-secret-value \ --secret-id <secret_arn> \ --query SecretString \ --output text`	

Tâche	Description	Compétences requises
Accédez au EnginFrame portail.	1. Dans l'épopée précédente, dans l'histoire Déployer la solution, sous le `Elastic-Vdi-Infrastructure.EnginFrameURL` résultat, trouvez l'adresse HTTPS du EnginFrame portail. 2. Dans un navigateur Web, entrez l'adresse HTTPS du portail. 3. Entrez les informations d'identification de l'utilisateur efadmin.	Architecte du cloud
Démarrez une session Windows.	1. Dans le menu du EnginFrame portail, choisissez Windows Desktop. 2. Lorsque vous êtes invité à vous connecter en tant qu'administrateur Windows, entrez le même mot de passe que celui utilisé pour l'utilisateur efadmin. 3. Vérifiez que la session Windows démarre correctement.	Architecte du cloud

Tâche	Description	Compétences requises
Démarrez une session Linux.	1. Dans le menu du EnginFrame portail, choisissez Linux Desktop. 2. Lorsque vous êtes invité à vous connecter, entrez les informations d'identification de l'utilisateur efadmin. 3. Vérifiez que la session Linux démarre correctem ent.	Architecte du cloud

Nettoyage

Tâche	Description	Compétences requises
Supprimez les piles.	Dans la CloudFormation console, supprimez les piles des flottes de serveurs Windows et Linux. Pour plus d'informations, consultez la section Suppression d'une pile.	Architecte du cloud
Supprimez l'infrastructure.	Supprimez l'infrastructure déployée à l'aide de la AWS CDK commande suivante : `cdk destroy --all`	Architecte du cloud

Résolution des problèmes

Problème	Solution
Le déploiement n'a pas été terminé car il a été interrompu.	Suivez les instructions de l'épopée Clean up, puis répétez ce schéma pour déployer à nouveau l'environnement.

Ressources connexes

- NICE DCV
- JOLI EnginFrame

Cloud hybride

Rubriques

- Configuration d'une extension de centre de données vers le VMware cloud sur AWS à l'aide du mode Hybrid Linked
- Configurer VMware vRealize Automation pour le provisionner VMs sur le VMware cloud sur AWS
- Intégrer VMware vRealize Network Insight au VMware cloud sur AWS
- Migrez VMs vers VMware le cloud sur AWS à l'aide de la migration assistée par HCX OS
- Envoyez des logs depuis le VMware Cloud AWS vers Splunk en utilisant VMware Aria Operations for Logs
- Configurez un pipeline CI/CD pour les charges de travail hybrides sur Amazon ECS Anywhere à l'aide d'AWS CDK et GitLab
- Plus de modèles

Configuration d'une extension de centre de données vers le VMware cloud sur AWS à l'aide du mode Hybrid Linked

Créée par Deepak Kumar (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

Ce modèle décrit comment vous pouvez utiliser le mode Hybrid Linked pour afficher et gérer les inventaires dans un centre de données sur site et un centre de données défini par logiciel (SDDC) VMware Cloud on AWS à l'aide d'une seule interface vSphere Client. VMware

En configurant le mode Hybrid Linked Mode, vous pouvez migrer vos machines virtuelles sur site (VMs) et vos applications vers le SDDC cloud. Vos équipes informatiques peuvent ensuite gérer vos ressources basées sur le cloud avec VMware des outils familiers et sans avoir besoin de nouveaux outils. Vous pouvez également garantir des opérations cohérentes et une administration simplifiée à l'aide de l'appliance VMware Cloud Gateway.

Ce modèle fournit deux options pour configurer le mode hybride lié, mais vous ne pouvez utiliser qu'une seule option à la fois. La première option installe le dispositif Cloud Gateway et l'utilise pour établir un lien entre le vCenter Server sur site et le SDDC dans le cloud. La deuxième option configure le mode Hybrid Linked à partir du SDDC du cloud.

Conditions préalables et limitations

Prérequis (les deux options)

- Un centre de données sur site existant et un SDDC dans le cloud.
- Une connexion existante entre le centre de données sur site et le SDDC dans le cloud, à l'aide d'AWS Direct Connect, d'un VPN ou des deux.
- Le centre de données sur site et le SDDC dans le cloud sont synchronisés avec le protocole NTP (Network Time Protocol) ou une autre source de temps officielle.
- La latence maximale d'un aller-retour entre le centre de données sur site et le SDDC dans le cloud ne dépasse pas 100 ms.

- Administrateurs cloud ayant accès à votre environnement sur site.
- Le nom de domaine complet (FQDN) du vCenter Server doit être converti en adresse IP privée.

Prérequis pour l'option 1

- L'environnement sur site doit fonctionner sur vSphere 6.5.0d ou version ultérieure.
- L'appliance Cloud Gateway et vCenter Server peuvent communiquer via AWS Direct Connect, un VPN ou les deux.
- L'appliance Cloud Gateway répond aux exigences matérielles.
- Les ports du pare-feu sont ouverts.

Prérequis pour l'option 2

- Le serveur vCenter sur site s'exécute sur vSphere 6.0 Update 3 ou version ultérieure, ou sur vSphere 6.5.0d ou version ultérieure.
- Les informations de connexion sont disponibles pour le domaine vSphere Single Sign-On (SSO) sur site.
- Les utilisateurs de l'environnement local ont un accès en lecture seule au nom distinctif de base (DN de base).
- Le serveur DNS (Domain Name System) local est configuré pour VMware Management Gateway.
- Mettez en œuvre des tests de connectivité réseau à l'aide du validateur de VMware connectivité.
- Les ports du pare-feu sont ouverts.

Limites

- Le mode Hybrid Linked Mode ne peut connecter qu'un seul domaine vCenter Server Enhanced Linked Mode sur site.
- Le mode Hybrid Linked Mode prend uniquement en charge vCenter Server sur site exécutant la version 6.7 ou ultérieure.

Architecture

Le schéma suivant montre les deux options de configuration du mode Hybrid Linked Mode.

Migration de différents types de charges de travail à l'aide du mode hybride lié

Le mode Hybrid Linked prend en charge la migration des charges de travail entre un centre de données sur site et un SDDC dans le cloud en utilisant soit une migration à froid, soit une migration en direct avec vSphere vMotion. VMware Les facteurs à prendre en compte lors du choix de la méthode de migration incluent le type et la version du commutateur virtuel, le type de connexion au SDDC cloud et la version du matériel virtuel.

Une migration à froid est appropriée pour VMs cette période d'indisponibilité. Vous pouvez les arrêter VMs, les migrer, puis les réactiver. Le temps de migration est plus rapide car il n'est pas nécessaire de copier la mémoire active. Nous recommandons d'utiliser une migration à froid pour les applications qui acceptent des interruptions de service (par exemple, les applications de niveau 3 ou les charges de travail de développement et de test). Si vous VMs ne pouvez pas subir de temps d'arrêt, vous devriez envisager une migration en direct à l'aide de vMotion pour vos applications critiques.

Le schéma suivant fournit une vue d'ensemble des différents types de migration de charge de travail à l'aide du mode Hybrid Linked Mode.

Outils

- VMware Cloud on AWS est une offre cloud intégrée développée conjointement par AWS et VMware.
- VMware L'appliance Cloud Gateway permet un certain nombre de cas d'utilisation du cloud hybride dans lesquels les ressources sur site sont connectées aux ressources du cloud.
- VMware vSphere est une plate-forme VMware de virtualisation qui transforme les centres de données en infrastructures informatiques agrégées comprenant des ressources de processeur, de stockage et de réseau.

Épopées

Option 1 - Utiliser le mode hybride lié avec l'appliance Cloud Gateway

Tâche	Description	Compétences requises
Configurez l'appliance Cloud Gateway.	1. Connectez-vous à la console VMware Cloud	Administrateur du cloud

Tâche	Description	Compétences requises
	on AWS et téléchargez l'appliance Cloud Gateway. 2. Installez l'appliance Cloud Gateway dans votre environnement sur site en suivant les deux étapes suivantes : • Choisissez Démarrer pour configurer puis déployer l'appliance Cloud Gateway. • Configurez le mode Hybrid Linked. Pour plus d'informations et des étapes détaillées, consultez la section Configuration du mode hybride lié à l'aide du dispositif vCenter Cloud Gateway dans la VMware documentation.	

Option 2 - Utiliser le mode hybride lié à partir du cloud SDDC

Tâche	Description	Compétences requises
Configurez le mode Hybrid Linked à partir du cloud SDDC.	1. Connectez-vous à la console VMware Cloud on AWS et utilisez le validateur de connectivité pour vérifier toutes les connexions réseau requises. Pour plus d'informations à ce sujet, consultez la section Valider	Administrateur du cloud

Tâche	Description	Compétences requises
	la connectivité réseau pour le mode Hybrid Linked Mode dans la VMware documentation. 2. Connectez-vous au client vSphere du cloud SDDC, choisissez Menu, Administration, puis Domains. 3. Dans la section Hybrid Cloud, choisissez Linked Domains, puis connectez-vous à votre vCenter Server sur site. 4. Ajoutez une source d'identité au domaine cloud SDDC Lightweight Directory Access Protocol (LDAP). Pour plus d'informations à ce sujet, voir Ajouter une source d'identité au domaine LDAP SDDC dans la documentation. VMware	

Ressources connexes

- Configuration du mode Hybrid Linked
- Configuration du mode hybride lié pour VMware le cloud sur AWS

Configurer VMware vRealize Automation pour le provisionner VMs sur le VMware cloud sur AWS

Créée par Deepak Kumar (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

VMware vRealize Automation est un logiciel d'automatisation que vous pouvez utiliser pour demander et gérer des ressources informatiques. En choisissant de configurer vRealize Automation with VMware Cloud on AWS, vous pouvez automatiser la mise à disposition de machines virtuelles (VMs), d'applications et de services informatiques dans plusieurs centres de données et environnements cloud.

Vos équipes informatiques peuvent ensuite créer des éléments de catalogue pour configurer le provisionnement des services et les fonctionnalités opérationnelles que vos utilisateurs peuvent demander et utiliser avec leurs outils vRealize Automation existants. Vous pouvez également améliorer l'agilité et l'efficacité de votre infrastructure informatique en intégrant VMware Cloud on AWS à vRealize Automation Cloud Assembly.

Ce modèle décrit comment configurer VMware vRealize Automation pour créer automatiquement des fonctionnalités VMs d'application sur VMware Cloud on AWS.

Conditions préalables et limitations

Prérequis

- Un centre de données sur site existant et un centre de données défini par logiciel (SDDC) VMware Cloud on AWS. Pour plus d'informations sur le SDCC cloud, consultez la section À propos des centres de données définis par logiciel dans la documentation. VMware
- Une connexion existante entre le centre de données sur site et le SDDC dans le cloud, à l'aide d'AWS Direct Connect, d'un VPN (basé sur un itinéraire ou une politique), ou les deux.
- Le centre de données sur site et le SDDC dans le cloud sont synchronisés avec le protocole NTP (Network Time Protocol) ou une autre source de temps officielle.

- La latence maximale d'un aller-retour entre le centre de données sur site et le SDDC dans le cloud ne dépasse pas 100 ms.
- Le nom de domaine complet (FQDN) du vCenter Server doit être converti en adresse IP privée.
- Utilisateurs du cloud SDDC ayant accès à votre environnement sur site.
- Accès du propriétaire de l'organisation dans le rôle de service vRealize Automation Cloud Assembly.
- Utilisateurs finaux autorisés dans vRealize Automation Service Broker à utiliser le service.
- La plage CIDR (Classless Inter-Domain Routing) du centre de données sur site doit être ouverte pour la génération de jetons d'API à partir de la console Cloud VMware on AWS. La liste suivante indique les rôles minimaux requis pour générer des jetons d'API :
  - Membre de l'organisation
  - Propriétaire de l'organisation
  - Rôles de service - VMware Cloud sur AWS
  - Administrateur
  - Administrateur NSX Cloud
  - Auditeur NSX Cloud

Pour plus d'informations à ce sujet, consultez la section Options de connectivité pour le VMware cloud sur AWS sur le blog du réseau SDDCs de partenaires AWS.

Limites

- Vous ne pouvez configurer que 20 comptes VMware Cloud avec des points de terminaison publics dans un seul vRealize Automation. Pour plus d'informations à ce sujet, consultez la section Scalabilité et maximums de simultanéité dans la documentation. VMware

Versions du produit

- vRealize Automation version 8.x ou ultérieure
- VMware vRealize Identity Manager version 3.x ou ultérieure
- VMware vRealize Suite Lifecycle Manager version 8.x ou ultérieure

Architecture

Le schéma suivant montre les services vRealize Automation qui peuvent utiliser l'infrastructure des environnements sur site et VMware Cloud on AWS.

VMware Composants de Cloud Assembly

VMware Cloud Assembly est un composant essentiel de vRealize Automation et vous pouvez l'utiliser pour déployer, provisionner VMs et calculer des ressources. Le tableau suivant décrit les composants VMware Cloud Assembly qui doivent être configurés pour le provisionnement VMs sur VMware Cloud on AWS.

Composants	Définition
Compte cloud	Le compte Cloud fournit les détails de connexion (par exemple, le nom du serveur, le nom d'utilisateur et le mot de passe, la clé d'accès et le jeton d'API). VMware Cloud Assembly utilise le compte Cloud pour collecter un inventaire de vos ressources.
Zones nuageuses	Les zones cloud identifient les limites des ressources dans le compte cloud (par exemple, les régions AWS et le SDDC du cloud). Les zones de cloud associent les ressources de calcul au projet Cloud Assembly.
Projets	Un projet est une entité logique composée d'utilisateurs et de ressources telles que des zones cloud. Il comprend également des quotas de ressources et des politiques de dénominat ion des machines virtuelles qui sont utilisés lors de la création de la machine virtuelle.
Mappages de saveurs	Le mappage des saveurs fournit des informati ons sur la capacité des machines virtuelles (par exemple, le nombre CPUs et la quantité de mémoire) utilisées dans le modèle de cloud.

Mappages d'images	Le mappage d'images mappe le modèle de machine virtuelle VMware vSphere et l'image Amazon Web Services (AWS) utilisés dans le modèle de cloud. Pour plus d'informations à ce sujet, consultez la section En savoir plus sur les mappages d'images dans vRealize Automation dans la VMware documentation.
Profil du réseau	Le profil réseau contrôle la décision de placement pour choisir un réseau lors du provisionnement des machines virtuelles.
Profil de stockage	Le profil de stockage contrôle la décision de placement pour choisir le stockage lors du provisionnement des machines virtuelles.
Modèles de cloud	VMware Les modèles de cloud constituent un élément important de vRealize Automation car ils définissent le provisionnement et l'orchest ration de l'infrastructure cloud. Les modèles de cloud sont des spécifications pour les ressource s et incluent le type de ressource, les propriété s des ressources et les informations à collecter auprès des utilisateurs.

Outils

- VMware vRealize Automation — vRealize Automation est une plate-forme d'automatisation de l'infrastructure dotée d'une gestion des états et d'une conformité pilotées par les événements. Il est conçu pour aider les entreprises à contrôler et à sécuriser les clouds en libre-service, l'automatisation multicloud avec gouvernance et la fourniture d'infrastructures DevOps basées sur la fourniture d'infrastructures.
- VMware Cloud sur AWS — VMware Cloud on AWS est une offre cloud intégrée développée conjointement par AWS et VMware.

Épopées

Générez les jetons d'API

Tâche	Description	Compétences requises
Générez les jetons d'API à partir de votre compte VMware Cloud on AWS.	1. Connectez-vous à la console VMware cloud. 2. Dans la barre d'outils des services VMware cloud, choisissez Mon compte, puis choisissez API Token. 3. Entrez un nom pour votre jeton d'API, indiquez la durée de vie requise et définissez les portées du jeton. 4. Cochez la case Open ID, puis sélectionnez Generate. 5. Enregistrez les informati ons d'identification du jeton d'API. Pour plus d'informations à ce sujet, consultez la section Comment générer des jetons d'API dans la VMware documentation.	Administrateur du cloud

Installez vRealize Automation dans votre centre de données sur site

Tâche	Description	Compétences requises
Téléchargez le logiciel requis.	Téléchargez le fichier ISO de VMware vRealize Suite depuis My VMware Portal. Ce package contient vRealize Suite Lifecycle Manager, VMware Identity Manager et vRealize Automation.	Administrateur du cloud
Installez le logiciel .	Installez le logiciel et connectez-vous à votre SDCC cloud en suivant les instructions de la section Installation de vRealize Suite Lifecycle Manager avec Easy Installer pour vRealize Automation et VMware Identity Manager dans la documentation. VMware **Important** Assurez-vous que les éléments suivants sont disponibles pour votre installation : • Configuration de VMware vCenter Server sur site et informations de connexion • Détails du réseau pour l'adresse IP et le sous-réseau de vRealize Automation	Administrateur cloud, architecte cloud

Tâche	Description	Compétences requises
	• La clé de licence vRealize Automation	

Connect VMware Cloud sur AWS avec VMware Cloud Assembly

Tâche	Description	Compétences requises
Configurez vos comptes cloud.	1. Sur la console VMware cloud, ouvrez l'onglet Infrastructure, choisissez Gérer — Comptes cloud, puis choisissez Ajouter des comptes cloud. 2. Choisissez VMware Cloud on AWS comme type. 3. Collez les informations du jeton d'API que vous avez enregistrées précédemment. Cela permet de remplir tous les clouds disponibles SDDCs dans votre organisation VMware Cloud on AWS. 4. Choisissez le SDCC cloud requis, puis fournissez le nom d'utilisateur et le mot de passe vCenter pour le SDDC. 5. Une fois que vous êtes authentifié avec succès, vous pouvez consulter le compte VMware Cloud on	Architecte cloud, administrateur cloud

Tâche	Description	Compétences requises
	AWS intégré avec un statut OK. Pour plus d'informations à ce sujet, consultez la section Créer un compte VMware cloud sur AWS dans vRealize Automation dans la VMware documentation.	
Configurez le projet.	1. Sur la console VMware Cloud, ouvrez l'onglet Projets, puis choisissez Nouveau projet. 2. Entrez le nom de votre projet. 3. Ouvrez l'onglet Cloud Zones et choisissez le compte VMware Cloud on AWS Cloud par défaut.	Administrateur du cloud

Tâche	Description	Compétences requises
Configurez la zone cloud.	1. Sur la console VMware Cloud, ouvrez Cloud Zones et choisissez la zone cloud pour votre centre de données SDDC. 2. Par défaut, `cloudadmin@vmc.local` (il s'agit de l'ID utilisateur local par défaut pour le vCenter du cloud SDDC) a uniquement accès au provisionnement dans le. `Compute-ResourcePool` 3. Ouvrez l'onglet Compute sous Cloud Zones, puis choisissez Compute-ResourcePool.	Administrateur du cloud
Configurez le mappage des saveurs.	1. Ouvrez l'onglet Mappages de saveurs et créez un nouveau mappage de saveurs. 2. Entrez le nom de la saveur, choisissez le compte VMware Cloud on AWS, puis indiquez le nombre de v CPUs et la quantité de mémoire.	Administrateur du cloud

Tâche	Description	Compétences requises
Configurez le mappage d'images.	1. Ouvrez Image Mappings et créez un nouveau mappage d'image. 2. Entrez le nom de l'image. 3. Choisissez le compte VMware Cloud on AWS et fournissez les modèles de compte Cloud requis.	Administrateur du cloud
Configurez le profil réseau.	1. Ouvrez le profil réseau et créez un nouveau profil réseau. 2. Entrez le nom du profil réseau. 3. Ouvrez l'onglet Réseau et choisissez le réseau existant que vous souhaitez utiliser pour le provision nement.	Administrateur du cloud

Tâche	Description	Compétences requises
Configurez le profil de stockage.	1. Ouvrez le profil de stockage et choisissez Nouveau profil de stockage. 2. Entrez le nom du profil de stockage. 3. Dans la section Politiques, créez une nouvelle politique . 4. Choisissez Workload Datastore. Par défaut, il `cloudadmin@vmc.local` n'a accès qu'au provisionnement dans la banque de données de la charge de travail.	Administrateur du cloud

Tâche	Description	Compétences requises
Créez le modèle de cloud.	1. Ouvrez l'onglet Design, choisissez Cloud Templates , puis choisissez New From et Blank Canvas. 2. Entrez le nom et la descripti on du modèle de cloud. 3. Choisissez le projet que vous avez créé précédemm ent. 4. Depuis la page de conception des ressource s du modèle Cloud, faites glisser les composants dans le canevas vierge en fonction de vos besoins. 5. Choisissez Test pour tester le modèle et résoudre les éventuels problèmes. 6. Choisissez Deploymen t et indiquez le nom du déploiement pour déployer le VMs. Pour plus d'informations à ce sujet, consultez la section Création d'un modèle de cloud de base dans la VMware documentation.	Administrateur du cloud

Ressources connexes

- Connectez vRealize Automation version 8.x à votre SDDC :

- Déployer un SDDC depuis le VMware cloud sur la console AWS
- Intégration d'AWS Direct Connect au VMware cloud sur AWS

Intégrer VMware vRealize Network Insight au VMware cloud sur AWS

Créée par Deepak Kumar (AWS), Piotr Pitera (AWS) et Sachin Trivedi (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

Ce modèle décrit comment intégrer VMware vRealize Network Insight à VMware Cloud on AWS et inspecter le flux de trafic provenant de vos machines virtuelles. Cette intégration vous permet également de planifier les migrations d'applications vers VMware Cloud on AWS.

vRealize Network Insight offre une visibilité sur votre infrastructure réseau. Il fournit des fonctionnalités de surveillance et d'analyse du réseau pour améliorer la sécurité, atténuer les risques de migration et optimiser les performances. Vous pouvez utiliser cet outil pour surveiller les flux de trafic provenant de vos machines virtuelles et consulter les règles de sécurité recommandées en fonction du trafic observé. Pour plus d'informations sur vRealize Network Insight, consultez la VMware documentation.

VMware Cloud on AWS est un service pay-as-you-go (à la demande) qui permet aux entreprises de toutes tailles d'exécuter des charges de travail dans des environnements cloud VMware basés sur vSphere en utilisant un large éventail de. Services AWS Vous pouvez commencer avec un minimum de 2 hôtes par cluster SDDC et passer à 16 hôtes par cluster dans votre environnement de production. Pour plus d'informations, consultez le AWS site Web VMware Cloud on. Pour en savoir plus SDDCs, consultez la section À propos des centres de données définis par logiciel dans la VMware documentation.

Conditions préalables et limitations

Prérequis

- VMware Cloud sur AWS SDDC, déployé

Limites

- Pour connaître les limitations connues, consultez la VMware documentation.

Versions du produit

- vRealize Network Insight version 5.0.0
- VMware Cloud sur AWS SDDC version 1.24

Architecture

Pile technologique source

- Aperçu du réseau vRealize

Pile technologique cible

- VMware Cloud activé AWS

Architecture cible

Le schéma suivant montre la connectivité entre VMware Cloud on AWS et vRealize Network Insight sur site.

Outils

- VMware Cloud on AWS est une offre cloud intégrée développée conjointement par AWS et VMware.
- VMware vRealize Network Insight est un outil de surveillance et d'analyse qui fournit une visibilité sur l'infrastructure réseau pour la planification de la sécurité et le dépannage.

Épopées

Configuration de votre environnement pour vRealize Network Insight

Tâche	Description	Compétences requises
Créez un compte VMware utilisateur.	Créez un compte VMware utilisateur ou connectez-vous à votre VMware compte existant.	Administrateur du cloud

Tâche	Description	Compétences requises
	Pour ouvrir un nouveau compte : 1. Ouvrez un compte VMware Customer Connect en remplissant le formulaire d'inscription. Les nouveaux utilisateurs recevront un e-mail pour activer leur compte. 2. Entrez le code d'authentification indiqué dans l'e-mail. 3. Connectez-vous à Customer Connect.	
Téléchargez les fichiers OVA pour vRealize Network Insight.	Téléchargez les fichiers OVA pour vRealize Network Insight :. 1. Accédez à la page de téléchargement VMware du produit sur https://my.vmware.com/group/vmware/home. 2. Recherchez vRealize Network Insight. 3. Téléchargez la dernière version 5.0.0 de la plateforme vRealize Network Insight et les fichiers OVA du collecteur.	Administrateur du cloud

Tâche	Description	Compétences requises
Déployez vRealize Network Insight.	Pour les instructions de déploiement, consultez la VMware documentation.	Administrateur du cloud

Ajouter une source de données et un collecteur

Tâche	Description	Compétences requises
Ajoutez une source de données.	1. Connectez-vous à vRealize Network Insight. 2. Choisissez Paramètres, Comptes et sources de données, puis Ajouter une source. 3. Dans Type, sélectionnez Serveur vCenter sur site. Pour plus d'informations, consultez la documentation VMware .	Administrateur du cloud
Configurez un collecteur pour la source de données.	Pour obtenir des instructi ons, consultez la VMware documentation.	Administrateur du cloud

Analyser les dépendances des applications

Tâche	Description	Compétences requises
Créez une application	Si aucune application n'existe dans vRealize Network Insight, suivez les étapes de la	Administrateur du cloud

Tâche	Description	Compétences requises
	VMware documentation pour en créer une.	
Découvrez et analysez votre application.	1. Utilisez vRealize Network Insight pour découvrir votre application. Pour obtenir des instructions, consultez la VMware documentation. 2. Analysez votre candidature. Pour obtenir des instructions, consultez la VMware documentation.	Administrateur du cloud

Ressources connexes

- Déployez un VMware SDDC sur AWS à l'aide de VMware Cloud on AWS (directives AWS prescriptives)
- Configuration d'une extension de centre de données vers le VMware cloud à AWS l'aide du mode hybride lié (directives AWS prescriptives)
- Migrer le VMware SDDC vers le VMware cloud à l' AWS aide de VMware HCX (directives prescriptives)AWS
- VMware Documentation de vRealize Network Insight (VMware site Web)

Migrez VMs vers VMware le cloud sur AWS à l'aide de la migration assistée par HCX OS

Créée par Deepak Kumar (AWS) et Himanshu Gupta (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

Ce modèle décrit comment migrer une machine virtuelle (VM) d'un environnement autre que vSphere vers VMware Cloud on Amazon Web Services (AWS) à l'aide de la migration assistée par le système d'exploitation (OSAM).

OSAM fait partie de VMware Hybrid Cloud Extension (HCX), qui est incluse dans VMware Cloud on AWS. Vous pouvez utiliser OSAM pour migrer un environnement autre que vSphere tel que VMware KVM ou Hyper-V vers Cloud on AWS. VMware OSAM utilise le logiciel Sentinel, que vous installez sur une machine virtuelle cliente Windows ou Linux pour faciliter la réplication de la machine virtuelle de votre environnement sur site vers un centre de données défini par logiciel (SDDC) sur le cloud sur AWS. VMware

Ce modèle explique comment activer OSAM, installer le logiciel Sentinel sur une machine virtuelle Windows, se connecter et s'enregistrer auprès d'une appliance HCX Sentinel Gateway (SGW) sur le site source et établir une connexion de transfert avec une appliance HCX Sentinel Data Receiver (SDR) sur le site de destination pour lancer la migration.

Pour plus d'informations sur OSAM, consultez la VMware documentation.

Conditions préalables et limitations

Prérequis

- Installez HCX dans vos environnements source et cible. Pour les prérequis HCX, consultez la section Migrer le VMware SDDC vers le cloud VMware sur AWS à l'aide de VMware HCX dans la documentation AWS Prescriptive Guidance.
- Pour les prérequis OSAM, consultez la liste de contrôle d'installation dans la documentation. VMware

- Pour obtenir des informations sur les ports OSAM, consultez les exigences relatives aux VMware ports VMware HCX sur le site Web Ports and Protocols.

Limites

- VMware Limites de configuration HCX 4.2.0
- Considérations relatives au déploiement d'OSAM
- Systèmes d'exploitation clients pris en charge
- Considérations relatives au système d'exploitation client

Versions du produit

- VMware HCX 4.2.0
- VMware SDDC 1,12

Architecture

Le schéma suivant montre comment HCX OSAM fonctionne avec le logiciel Sentinel pour répliquer un environnement autre que vSphere VMs depuis votre environnement sur site vers Cloud on AWS. VMware

OSAM se compose de trois composants :

- L'appliance Sentinel Gateway (SGW), qui est utilisée pour connecter et transférer les charges de travail et les applications dans l'environnement basé sur les sources VMware
- Le récepteur de données Sentinel (SDR), qui est utilisé dans l'environnement VMware Cloud on AWS de destination pour recevoir les charges de travail migrées depuis la source
- Le logiciel Sentinel, qui doit être installé sur chaque machine virtuelle cliente que vous souhaitez migrer

OSAM utilise le logiciel Sentinel installé sur un client Windows ou Linux VMs pour faciliter la réplication d'une machine virtuelle sur site vers un SDDC. VMware Le logiciel Sentinel que vous installez sur le client VMs collecte les configurations du système à partir de la machine virtuelle cliente et aide à la réplication des données. Ces informations sont également utilisées pour créer

l'inventaire des clients VMs en vue de la migration et aident à préparer les disques de la machine virtuelle répliquée à des fins de réplication et de migration.

Outils

- VMware HCX 4.2.0
- VMware Cloud sur AWS SDDC

Épopées

Configurer HCX

Tâche	Description	Compétences requises
Déployez HCX Cloud et HCX Connector.	Suivez les instructions de la section Installations du connecteur HCX et du cloud HCX de la VMware documentation.	Administrateur du cloud, administrateur des systèmes

Configuration d'OSAM et migration VMs

Tâche	Description	Compétences requises
Installez HCX Sentinel.	Pour installer Sentinel sous Linux, procédez comme suit : 1. Dans le vCenter Server pour le connecteur HCX, choisissez Interconnect, Multi-Site Service Mesh, Sentinel Management. 2. Choisissez Télécharger le bundle Linux. 3. Installez l'agent Sentinel sur une machine Linux.	Administrateur du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Téléchargement et installation du logiciel HCX Sentinel Agent dans la VMware documentation.	

Tâche	Description	Compétences requises
Migrer VMs.	Pour migrer vos VMs groupes de discussion (appelés groupes de mobilité), procédez comme suit : 1. Dans vSphere Client, à partir du plug-in HCX, choisissez Services, Migration. 2. Choisissez Migrate (Migrer). 3. Choisissez Non vSphere Inventory, Remote Connections. Cela affichera la liste sur VMs laquelle vous avez installé HCX Sentinel. 4. Dans Nom du groupe, entrez le nom du groupe de mobilité que vous souhaitez créer pour VMs. 5. Choisissez ceux que VMs vous souhaitez migrer, puis choisissez Ajouter pour les ajouter au groupe de mobilité. 6. Pour chaque machine virtuelle : a. Sélectionnez le conteneur de calcul de destination. b. Sélectionnez le stockage de destination.	Administrateur du cloud

Tâche	Description	Compétences requises
	c. Sélectionnez le profil de migration. d. Sélectionnez le dossier de destination. 7. Pour démarrer le processus de migration, choisissez Go. HCX valide vos sélections de machines virtuelles avant le début de la migration. Pour plus d'informations, consultez les sections Migration de machines virtuelles avec des groupes de mobilité et Surveillance et estimation de la migration avec des groupes de mobilité dans la VMware documentation.	

Ressources connexes

VMware documentation :

- VMware Guide de l'utilisateur HCX
- Installer la liste de contrôle B - HCX avec un environnement de destination VMC SDDC
- VMware HCX dans le VMware cloud sur AWS
- Migration assistée du système d'exploitation HCX pour VMware le cloud sur AWS
- VMware Notes de mise à jour de HCX 4.2.1

Envoyez des logs depuis le VMware Cloud AWS vers Splunk en utilisant VMware Aria Operations for Logs

Créée par Deepak Kumar (AWS) et Piotr Pitera (AWS)

Récapitulatif

> Remarque : Depuis le 30 avril 2024, VMware Cloud on n' AWS est plus revendu AWS ni par ses partenaires de distribution. Le service continuera d'être disponible via Broadcom. Nous vous encourageons à contacter votre AWS représentant pour plus de détails.

Ce modèle décrit comment transférer les AWS événements ou les journaux de VMware Cloud vers un syslog ou un point de terminaison HTTP tel que Splunk en utilisant VMware Aria Operations for Logs.

VMware Aria Operations for Logs est un outil d'analyse des journaux qui offre une meilleure visibilité et un dépannage accéléré dans l' AWS environnement VMware Cloud on. Vous pouvez configurer cet outil pour envoyer la totalité ou une partie des journaux ou des événements du VMware Cloud AWS vers un point de terminaison Syslog ou HTTP. Le point de terminaison peut être un point de terminaison SaaS (logiciel en tant que service) ou un point de terminaison sur site tel que Splunk. (Ce modèle fournit les instructions pour Splunk.) Pour en savoir plus sur VMware Aria Operations for Logs, consultez la VMware documentation.

VMware Cloud on AWS est un service pay-as-you-go (à la demande) qui permet aux entreprises de toutes tailles d'exécuter des charges de travail dans des environnements cloud VMware basés sur vSphere en utilisant un large éventail de. Services AWS Vous pouvez commencer avec un minimum de 2 hôtes par cluster de centres de données définis par logiciel (SDDC) et augmenter jusqu'à 16 hôtes par cluster dans votre environnement de production. Pour plus d'informations, consultez le AWS site Web VMware Cloud on. Pour en savoir plus SDDCs, consultez la section À propos des centres de données définis par logiciel dans la VMware documentation.

Conditions préalables et limitations

Prérequis

- Splunk, configuré sur site

Limites

Vous pouvez souscrire un abonnement d'essai gratuit à VMware Aria Operations for Logs. Cet abonnement est valide pendant 30 jours et comporte les limites suivantes :

- Taille maximale des journaux que vous pouvez transférer : 50 Go de journaux par jour
- Nombre maximum de configurations de transfert de journal que vous pouvez créer : 10
- Nombre maximum de configurations de transfert de journal que vous pouvez activer : 5

Pour accéder à toutes les fonctionnalités du service, vous devez passer à un abonnement premium.

Pour plus d'informations sur les abonnements d'essai et premium, consultez la section Abonnements et facturation d'VMware Aria Operations for Logs (SaaS) dans la VMware documentation. Pour plus d'informations sur les limites d'utilisation, consultez la section Limitations d'utilisation des fonctionnalités dans la VMware documentation.

Versions du produit

- VMware Cloud sur AWS SDDC version 1.24
- VMware Opérations Aria pour Logs version 8.10
- Splunk version 9.x sur site

Architecture

Pile technologique source

- VMware Cloud activé AWS
- VMware Opérations Aria pour les journaux

Pile technologique cible

- Splunk sur site

Architecture cible

Le schéma suivant montre la connectivité entre un centre de données d'entreprise et VMware Aria Operations for Logs in VMware Cloud on AWS.

Outils

- VMware Cloud on AWS est une offre cloud intégrée développée conjointement par AWS et VMware.
- VMware Aria Operations for Logs est un outil d'analyse des journaux et de résolution des problèmes pour VMware Cloud on AWS.

Épopées

Déployez un SDDC et activez l'opération VMware Aria pour les journaux

Tâche	Description	Compétences requises
Déployez un VMware cloud sur AWS SDDC.	Suivez les instructions de la section Déployer un VMware SDDC sur AWS en utilisant VMware Cloud on AWS dans le guide AWS prescriptif.	Architecte cloud, administrateur cloud
Inscrivez-vous à VMware Aria Operations for Logs.	Pour obtenir des instructions, consultez la VMware documentation.	Architecte du cloud

Déployer un proxy cloud

Tâche	Description	Compétences requises
Déployez un proxy cloud.	Pour transférer les journaux vers une instance locale de Splunk, vous devez ajouter un proxy cloud pour VMware Aria Operations for Logs. Ce proxy reçoit les informations du centre de données sur site et les envoie à VMware	Administrateur cloud, architecte cloud

Tâche	Description	Compétences requises
	Aria Operations for Logs pour analyse. Pour télécharger et installer le proxy cloud : 1. Assurez-vous que les ports 443, 22 et 514 sont ouverts entre votre environnement sur site et VMware Cloud on AWS. Pour les ports supplémentaires, vous pouvez utiliser le 1514/TCP ou le 6514/TCP. Pour plus d'informations sur les ports, consultez les recommandations d'VMware Aria Operations for Logs Firewall dans la VMware documentation. 2. Connectez-vous à VMware Aria Operations for Logs. 3. Sur la page d'accueil , choisissez Ajouter un collecteur dans le widget. 4. Sur l'écran de l'appliance virtuelle Cloud Proxy, copiez la clé du jeton. Vous devez utiliser cette clé dans les 24 heures pour terminer les étapes suivantes. 5. Choisissez le lien de téléchargement du fichier OVA.	

Tâche	Description	Compétences requises
	6. Accédez au client Web VMware vSphere, choisissez votre cluster, puis sélectionnez Déployer le modèle OVF. 7. Lorsque vous êtes invité à saisir la clé, collez la clé de jeton que vous avez copiée à l'étape 4. 8. Choisissez Terminer pour installer le proxy cloud.	

Transférer les journaux vers un point de terminaison Splunk sur site

Tâche	Description	Compétences requises
Configurez le transfert du journal.	Pour transférer les journaux vers le point de terminaison Splunk : 1. Connectez-vous à VMware Aria Operations for Logs. 2. Accédez à Log Management. 3. Choisissez Log Forwarding. 4. Choisissez Nouvelle configuration, puis complétez les paramètres suivants : • Donnez un nom à la configuration de transfert du journal.	

Tâche	Description	Compétences requises
	• Dans Destination, choisissez Sur site. • Pour Cloud Proxy, sélectionnez le proxy cloud que vous avez installé précédemment. • Pour Type de point de terminaison, choisissez TCP. • Pour l'URL du point de terminaison, indiquez votre URL Splunk locale au format suivant : `tcp://x.x.x.x (your Splunk IP address): 514` • (Facultatif) Pour les balises, vous pouvez spécifier les noms et les valeurs des balises afin de faciliter les requêtes. • Choisissez Appliquer à tous les journaux ou Appliquer à des journaux spécifiques. Si vous souhaitez envoyer tous les journaux VMware Cloud on AWS à Splunk, choisissez Appliquer à tous les journaux. 5. Choisissez Vérifier. 6. Choisissez Enregistrer.	

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Transférer les journaux depuis VMware Aria Operations for Logs dans la VMware documentation.	

Ressources connexes

- VMware Cloud sur AWS site Web
- À propos des centres de données définis par logiciel (documentation) VMware
- Déployer un VMware SDDC à l'aide AWS de VMware Cloud on AWS (directives AWS prescriptives)
- Migrez les charges de travail vers le VMware cloud à l'aide AWS de VMware HCX (directivesAWS prescriptives)
- Configuration d'une extension de centre de données vers le VMware cloud à AWS l'aide du mode hybride lié (directives AWS prescriptives)

Configurez un pipeline CI/CD pour les charges de travail hybrides sur Amazon ECS Anywhere à l'aide d'AWS CDK et GitLab

Créée par le Dr Rahul Sharad Gaikwad (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus.

Amazon ECS Anywhere est une extension d'Amazon Elastic Container Service (Amazon ECS). Elle prend en charge l'enregistrement d'une instance externe, telle qu'un serveur sur site ou une machine virtuelle (VM), sur votre cluster Amazon ECS. Cette fonctionnalité permet de réduire les coûts et d'atténuer l'orchestration et les opérations complexes des conteneurs locaux. Vous pouvez utiliser ECS Anywhere pour déployer et exécuter des applications de conteneur dans des environnements sur site et dans le cloud. Ainsi, votre équipe n'a plus besoin d'apprendre plusieurs domaines et compétences, ou de gérer elle-même des logiciels complexes.

Ce modèle décrit une step-by-step approche pour approvisionner un cluster Amazon ECS avec des instances Amazon ECS Anywhere à l'aide de piles Amazon Web Services (AWS) Cloud Development Kit (AWS CDK). Vous utilisez ensuite AWS CodePipeline pour configurer un pipeline d'intégration et de déploiement continus (CI/CD). Ensuite, vous répliquez votre référentiel de GitLab code sur AWS CodeCommit et vous déployez votre application conteneurisée sur le cluster Amazon ECS.

Ce modèle est conçu pour aider ceux qui utilisent une infrastructure sur site à exécuter des applications de conteneur et GitLab à gérer la base de code de l'application. Vous pouvez gérer ces charges de travail à l'aide des services cloud AWS, sans perturber votre infrastructure sur site existante.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Application conteneur exécutée sur une infrastructure sur site.
- Un GitLab référentiel dans lequel vous gérez la base de code de votre application. Pour plus d'informations, consultez Repository (GitLab).

- Interface de ligne de commande AWS (AWS CLI), installée et configurée. Pour plus d'informations, consultez Installation ou mise à jour de la dernière version de l'interface de ligne de commande AWS (documentation de l'interface de ligne de commande AWS).
- AWS CDK Toolkit, installé et configuré dans le monde entier. Pour plus d'informations, consultez Installer le CDK AWS (documentation du CDK AWS).
- npm, installé et configuré pour le AWS CDK dans. TypeScript Pour plus d'informations, consultez Téléchargement et installation de Node.js et de npm (documentation npm).

Limites

- Pour connaître les limites et les considérations, consultez la section Instances externes (Amazon ECS Anywhere) dans la documentation Amazon ECS.

Versions du produit

- AWS CDK Toolkit version 2.27.0 ou ultérieure
- npm version 7.20.3 ou ultérieure
- Node.js version 16.6.1 ou ultérieure

Architecture

Pile technologique cible

- AWS CDK
- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon ECS Anywhere
- Amazon Elastic Container Registry (Amazon ECR)
- AWS Identity and Access Management (IAM)
- Gestionnaire du système AWS
- GitLab référentiel

Architecture cible

Ce diagramme représente deux flux de travail principaux décrits dans ce modèle, à savoir le provisionnement du cluster Amazon ECS et la configuration du CI/CD pipeline that sets up and deploys the CI/CD pipeline, comme suit :

1. Provisionnement du cluster Amazon ECS
    a. Lorsque vous déployez la première pile AWS CDK, elle crée une CloudFormation pile sur AWS.
    b. Cette CloudFormation pile fournit un cluster Amazon ECS et les ressources AWS associées.
    c. Pour enregistrer une instance externe auprès d'un cluster Amazon ECS, vous devez installer l'agent AWS Systems Manager (agent SSM) sur votre machine virtuelle et enregistrer la machine virtuelle en tant qu'instance gérée par AWS Systems Manager.
    d. Vous devez également installer l'agent de conteneur Amazon ECS et Docker sur votre machine virtuelle pour l'enregistrer en tant qu'instance externe auprès du cluster Amazon ECS.
    e. Lorsque l'instance externe est enregistrée et configurée avec le cluster Amazon ECS, elle peut exécuter plusieurs conteneurs sur votre machine virtuelle, qui est enregistrée en tant qu'instance externe.
    f. Le cluster Amazon ECS est actif et peut exécuter les charges de travail des applications via des conteneurs. L'instance de conteneur Amazon ECS Anywhere s'exécute dans un environnement sur site mais est associée au cluster Amazon ECS dans le cloud.
2. Configuration et déploiement du pipeline CI/CD
    a. Lorsque vous déployez la deuxième pile AWS CDK, elle en crée une autre CloudFormation sur AWS.
    b. Cette CloudFormation pile fournit un pipeline dans les ressources AWS CodePipeline et les ressources associées.
    c. Vous transférez et fusionnez les modifications du code de l'application dans un GitLab référentiel local.
    d. Le GitLab référentiel est automatiquement répliqué dans le CodeCommit référentiel.
    e. Les mises à jour du CodeCommit dépôt CodePipeline démarrent automatiquement.
    f. CodePipeline copie le code depuis CodeCommit et crée l'application déployable intégrée. CodeBuild
    g. CodePipeline crée une image Docker de l'environnement de CodeBuild construction et l'envoie vers le dépôt Amazon ECR.

h. CodePipeline lance des CodeDeploy actions qui extraient l'image du conteneur depuis le dépôt Amazon ECR.

i. CodePipeline déploie l'image du conteneur sur le cluster Amazon ECS.

Automatisation et mise à l'échelle

Ce modèle utilise le CDK AWS comme outil d'infrastructure sous forme de code (IaC) pour configurer et déployer cette architecture. AWS CDK vous aide à orchestrer les ressources AWS et à configurer Amazon ECS Anywhere et le pipeline CI/CD.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK) est un framework de développement logiciel qui vous aide à définir et à provisionner l'infrastructure du cloud AWS sous forme de code.
- AWS CodeCommit est un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.
- AWS vous CodePipeline aide à modéliser et à configurer rapidement les différentes étapes d'une version logicielle et à automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon Elastic Container Registry (Amazon ECR) est un service géré de registre d'images de conteneurs sécurisé, évolutif et fiable.
- Amazon Elastic Container Service (Amazon ECS) est un service de gestion de conteneurs évolutif et rapide, qui facilite l'exécution, l'arrêt et la gestion de conteneurs Docker sur un cluster. Ce modèle utilise également Amazon ECS Anywhere, qui permet d'enregistrer un serveur ou une machine virtuelle sur site dans votre cluster Amazon ECS.

Autres outils

- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.

- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.
- Vagrant est un utilitaire open source permettant de créer et de maintenir des environnements de développement de logiciels virtuels portables. À des fins de démonstration, ce modèle utilise Vagrant pour créer une machine virtuelle sur site.

Référentiel de code

Le code de ce modèle est disponible dans le pipeline GitHub CI/CD pour Amazon ECS Anywhere à l'aide du référentiel AWS CDK.

Bonnes pratiques

Tenez compte des meilleures pratiques suivantes lors du déploiement de ce modèle :

- Bonnes pratiques pour le développement et le déploiement d'une infrastructure cloud avec le CDK AWS
- Bonnes pratiques pour le développement d'applications cloud avec AWS CDK (article de blog AWS)

Épopées

Vérifiez la configuration du kit AWS CDK

Tâche	Description	Compétences requises
Vérifiez la version du kit AWS CDK.	Vérifiez la version du kit d'outils AWS CDK en saisissant la commande suivante. `cdk --version` Ce modèle nécessite la version 2.27.0 ou ultérieure. Si vous disposez d'une version antérieure, suivez les instructi	DevOps ingénieur

Tâche	Description	Compétences requises
	ons de la documentation AWS CDK pour la mettre à jour.	
Vérifiez la version de npm.	Vérifiez la version de npm en saisissant la commande suivante. `npm --version` Ce modèle nécessite la version 7.20.3 ou ultérieur e. Si vous avez une version antérieure, suivez les instructi ons de la documentation de npm pour la mettre à jour.	DevOps ingénieur

Configurez les informations d'identification AWS.	Configurez les informati ons d'identification AWS en saisissant la `aws configure` commande et en suivant les instructions.
	`$aws configure`
	`AWS Access Key ID [None]: <your-access-key-ID>`
	`AWS Secret Access Key [None]: <your-secret-access-key>`
	`Default region name [None]: <your-Region-name>`
	`Default output format [None]:`
		DevOps ingénieur

Démarrez l'environnement AWS CDK

Tâche	Description	Compétences requises

Clonez le référentiel de code AWS CDK.	1. Clonez le pipeline CI/CD pour Amazon ECS Anywhere à l'aide du référentiel AWS CDK pour ce modèle en saisissant la commande suivante.
	`git clone https://github.com/aws-samples/amazon-ecs-anywhere-cicd-pipeline-cdk-sample.git`
	2. Accédez au répertoire cloné en saisissant la commande suivante.
	`cd amazon-ecs-anywhere-cicd-pipeline-cdk-sample`
		DevOps ingénieur

Démarrez l'environnement.	Déployez le CloudFormation modèle sur le compte et la région AWS que vous souhaitez utiliser en saisissant la commande suivante. `cdk bootstrap <account-number>/<Region>` Pour plus d'informations, consultez la section Bootstrapping dans la documentation AWS CDK.	DevOps ingénieur

Créez et déployez l'infrastructure pour Amazon ECS Anywhere

Tâche	Description	Compétences requises

Installez les dépendances du package et compilez les TypeScript fichiers.	Installez les dépendances du package et compilez les TypeScript fichiers en saisissant les commandes suivantes.
	`$cd EcsAnywhereCdk`
	`$npm install`
	`$npm fund`
	Ces commandes installent tous les packages du référentiel d'échantillons. Pour plus d'informations, consultez npm ci et npm install dans la documentation de npm. Si vous recevez des erreurs concernant des packages manquants lorsque vous entrez ces commandes, consultez la section Dépannage de ce modèle.
		DevOps ingénieur

Générez le projet.	Pour créer le code du projet, entrez la commande suivante. `npm run build` Pour plus d'informations sur la création et le déploiement du projet, consultez Votre première application AWS	DevOps ingénieur

Tâche	Description	Compétences requises
	CDK dans la documentation du CDK AWS.	

Déployez la pile d'infrastructure Amazon ECS Anywhere.	1. Répertoriez les piles en saisissant la commande suivante.
	`$cdk list`
	2. Vérifiez que la sortie renvoie les `ECSAnywherePipelineStack` piles `EcsAnywhereInfraStack` et.
	3. Déployez la `EcsAnywhereInfraStack` pile en saisissant la commande suivante.
	`$cdk deploy EcsAnywhereInfraStack`
		DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez la création et la sortie de la pile.	1. Connectez-vous à l'AWS Management Console et ouvrez la CloudFormation console à l'adresse https://console.aws.amazon.com/cloudformation/. 2. Sur la page Stacks, sélectionnez la `EcsAnywhereInfraStack` pile. 3. Vérifiez que l'état de la pile est l'un `CREATE_IN_PROGRESS` ou l'autre`CREATE_COMPLETE` . La configuration du cluster Amazon ECS peut prendre un certain temps. Ne poursuivez pas tant que la création de la pile n'est pas terminée.	DevOps ingénieur

Configuration d'une machine virtuelle sur site

Tâche	Description	Compétences requises
Configurez votre machine virtuelle.	Créez une machine virtuelle Vagrant en entrant la `vagrant up` commande depuis le répertoire racine où se trouve Vagrantfile. Pour plus d'informations, consultez la documentation de Vagrant.	DevOps ingénieur

Tâche	Description	Compétences requises
Enregistrez votre machine virtuelle en tant qu'instance externe.	1. Connectez-vous à la machine virtuelle Vagrant à l'aide de la `vagrant ssh` commande. Pour plus d'informations, consultez la documentation de Vagrant. 2. Installez l'AWS CLI sur la machine virtuelle en suivant les instructions d'installation de l'AWS CLI et en saisissant les commandes suivantes. `$ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" \ > -o "awscliv2.zip" $sudo apt install unzip $unzip awscliv2.zip $sudo ./aws/install $aws configure AWS Access Key ID [None]: <your-access-key-ID> AWS Secret Access Key [None]: <your-secret-access-key> Default region name [None]: <your-Region-name> Default output format [None]:` 1. Créez un code d'activation et un identifiant que	DevOps ingénieur

Tâche	Description	Compétences requises

	vous pouvez utiliser pour enregistrer votre machine virtuelle auprès d'AWS Systems Manager et pour activer votre instance externe. Le résultat de cette commande inclut les valeurs de l'ID d'activation et du code d'activation.
	`aws ssm create-activation \ > --iam-role EcsAnywhereInstanceRole \ > | tee ssm-activation.json`
	Si vous recevez un message d'erreur lorsque vous exécutez cette commande, consultez la section Dépannage.
	2. Exportez l'ID d'activation et les valeurs du code.
	`export ACTIVATION_ID=<activation-ID> export ACTIVATION_CODE=<activation-code>`
	3. Téléchargez le script d'installation sur votre machine virtuelle.	

Tâche	Description	Compétences requises
	``` curl --proto "https" - o "ecs-anywhere-inst all.sh" \ > "https://amazon-ec s-agent.s3.amazona ws.com/ecs-anywher e-install-latest.s h" ``` 4. Exécutez le script d'install ation sur votre machine virtuelle. ``` sudo bash ecs-anywh ere-install.sh \ --cluster EcsAnywhe reCluster \ --activation-id $ACTIVATION_ID \ --activation-code $ACTIVATION_CODE \ --region <region-n ame> ``` Cela permet de configure r votre machine virtuelle en tant qu'instance externe Amazon ECS Anywhere et d'enregistrer l'instanc e dans le cluster Amazon ECS. Pour plus d'informa tions, consultez la section Enregistrement d'une instance externe dans un cluster dans la documentation Amazon ECS. Si vous rencontrez	

Tâche	Description	Compétences requises
	des problèmes, consultez la section Dépannage.	

Vérifiez l'état d'Amazon ECS Anywhere et de la machine virtuelle externe.	Pour vérifier si votre machine virtuelle est connectée au plan de contrôle Amazon ECS et en cours d'exécution, utilisez les commandes suivantes.
	`$aws ssm describe-instance-information`
	`$aws ecs list-container-instances --cluster $CLUSTER_NAME`
		DevOps ingénieur

Déployer le pipeline CI/CD

Tâche	Description	Compétences requises
Créez une branche dans le CodeCommit dépôt.	Créez une branche nommée `main` dans le CodeCommit dépôt en créant le premier commit pour le référentiel. Vous pouvez suivre la documentation AWS pour créer un commit dans CodeCommit. Voici un exemple de commande. `aws codecommit put-file \ --repository-name EcsAnywhereRepo \ --branch-name main \ --file-path README.md \`	DevOps ingénieur

Tâche	Description	Compétences requises
	--file-content "Test" \ --name "Dev Ops" \ --email "devops@example.com" \ --commit-message "Adding README."	

Tâche	Description	Compétences requises
Configurez la mise en miroir des dépôts.	Vous pouvez mettre en miroir un GitLab référentiel depuis et vers des sources externes. Vous pouvez sélectionner le référentiel qui servira de source. Les branches, les tags et les commits sont synchronisés automatiq uement. Configurez un miroir push entre le GitLab référenti el hébergeant votre applicati on et le CodeCommit référenti el. Pour obtenir des instructi ons, voir Configurer un miroir push de GitLab à CodeCommi t (GitLab documentation). **Note** Par défaut, la mise en miroir synchroni se automatiquement le référentiel. Si vous souhaitez mettre à jour les référentiels manuellement, voir Mettre à jour un miroir (GitLab documenta tion).	DevOps ingénieur

Tâche	Description	Compétences requises
Déployez la pile de pipelines CI/CD.	Déployez la `EcsAnywhe rePipelineStack` pile en saisissant la commande suivante. `$cdk deploy EcsAnywhe rePipelineStack`	DevOps ingénieur

Tâche	Description	Compétences requises
Testez le pipeline CI/CD.	1. Modifiez le code de l'application et transférez-le vers le GitLab dépôt source sur site. Pour plus d'informations, consultez Options push (GitLab documentation). Par exemple, modifiez le `../application/index.html` fichier pour mettre à jour la valeur de version de l'application. 2. Lorsque le code est répliqué dans le CodeCommit dépôt, le pipeline CI/CD démarre. Effectuez l'une des actions suivantes : • Si vous utilisez la mise en miroir automatique pour synchroniser le GitLab dépôt avec le CodeCommit dépôt, passez à l'étape suivante. • Si vous utilisez la mise en miroir manuelle, transférez les modifications du code de l'application vers le CodeCommit dépôt en suivant les instructions de la section Mettre à jour un miroir (GitLab documentation). 3. Sur votre ordinateur local, dans un navigateur Web,	DevOps ingénieur

Tâche	Description	Compétences requises
	entrez http://localhost:80. Cela ouvre la page Web de NGINX car le port 80 est redirigé vers localhost dans Vagrantfile. Vérifiez que vous pouvez consulter la valeur de version mise à jour de l'application. Cela valide le déploiement du pipeline et de l'image. 4. (Facultatif) Si vous souhaitez vérifier le déploiement dans l'AWS Management Console, procédez comme suit : a. Ouvrez la console Amazon ECS à l'adresse https://console.aws.amazon.com/ecs/. b. Dans la barre de navigation, sélectionnez la région à utiliser. c. Dans le panneau de navigation, choisissez Clusters. d. Sur la page Clusters, sélectionnez le EcsAnywhereCluster cluster. e. Choisissez Définitions de tâches. f. Vérifiez que le conteneur est en cours d'exécution.	

Nettoyage

Tâche	Description	Compétences requises

Nettoyez et supprimez les ressources.	Après avoir suivi ce modèle, vous devez supprimer les proof-of-concept ressource s que vous avez créées. Pour nettoyer, entrez les commandes suivantes.
	`$cdk destroy EcsAnywhe rePipelineStack`
	`$cdk destroy EcsAnywhe reInfraStack`
		DevOps ingénieur

Résolution des problèmes

Problème	Solution

Erreurs relatives aux packages manquants lors de l'installation des dépendances des packages.	Entrez l'une des commandes suivantes pour résoudre les packages manquants.
	`$npm ci`
	or
	`$npm install -g @aws-cdk/<package_ name>`

Lorsque vous exécutez la `aws ssm create-activation` commande sur la machine virtuelle, le message d'erreur suivant s'affiche. `An error occurred (Validati onException) when calling the CreateActivation operation:`	La `EcsAnywhereInfraStack` pile n'est pas complètement déployée et le rôle IAM nécessaire pour exécuter cette commande n'a pas encore été créé. Vérifiez l'état de la pile dans la CloudFormation console. Réessayez

Problème	Solution
`Nonexistent role or missing ssm service principal in trust policy: arn:aws:iam::000000000000:role/EcsAnywhereInstanceRole`	la commande une fois que le statut est passé à`CREATE_COMPLETE` .

Un bilan de santé Amazon ECS est renvoyé et l'erreur suivante s'affiche dans la section Services du cluster de la console Amazon ECS. `UNHEALTHY`
 	
`service EcsAnywhereService was unable to place a task because no container instance met all of its requirements. Reason: No Container Instances were found in your cluster.`
	Redémarrez l'agent Amazon ECS sur votre machine virtuelle Vagrant en saisissant les commandes suivantes.
	
	`$vagrant ssh`
	`$sudo systemctl restart ecs`
	`$sudo systemctl status ecs`

Ressources connexes

- Page marketing d'Amazon ECS Anywhere
- Documentation Amazon ECS Anywhere
- Démonstration d'Amazon ECS Anywhere (vidéo)
- Exemples d'ateliers Amazon ECS Anywhere (GitHub)
- Mise en miroir de référentiels (GitLab documentation)

Plus de modèles

- Automatisez la configuration du peering interrégional avec AWS Transit Gateway
- Gérez les applications de conteneur sur site en configurant Amazon ECS Anywhere avec le kit AWS CDK
- Migrez les données Hadoop vers Amazon S3 à l'aide de Migrator WANdisco LiveData
- Migrez VMware VMs avec HCX Automation à l'aide de PowerCLI
- Modifiez les en-têtes HTTP lors de la migration de F5 vers un Application Load Balancer sur AWS
- Réhébergez les charges de travail sur site dans le cloud AWS : liste de contrôle pour la migration
- Utilisez les requêtes BMC Discovery pour extraire les données de migration afin de planifier la migration

Gestion et gouvernance

Rubriques

- Identifiez et alertez lorsque les ressources Amazon Data Firehose ne sont pas chiffrées à l'aide d'une clé AWS KMS
- Automatisez l'ajout ou la mise à jour d'entrées de registre Windows à l'aide d'AWS Systems Manager
- Créez automatiquement une RFC dans AMS à l'aide de Python
- Arrêtez et démarrez automatiquement une instance de base de données Amazon RDS à l'aide de AWS Systems Manager Maintenance Windows
- Centralisez la distribution des packages logiciels dans AWS Organizations à l'aide de Terraform
- Configurez la journalisation pour les applications .NET dans Amazon CloudWatch Logs en utilisant NLog
- Copiez les produits AWS Service Catalog sur différents comptes AWS et régions AWS
- Création d'une matrice RACI ou RASCI pour un modèle d'exploitation cloud
- Créez des alarmes pour des métriques personnalisées à l'aide de la détection des CloudWatch anomalies Amazon
- Créez un IDE AWS Cloud9 qui utilise les volumes Amazon EBS avec un chiffrement par défaut
- Créez automatiquement des CloudWatch tableaux de bord Amazon basés sur des balises
- Documentez la conception de votre zone de landing zone AWS
- Améliorez les performances opérationnelles en activant Amazon DevOps Guru dans plusieurs régions AWS, sur plusieurs comptes et OUs avec le kit AWS CDK
- Implémentez Account Factory for Terraform (AFT) en utilisant un pipeline bootstrap
- Gérez les produits AWS Service Catalog dans plusieurs comptes AWS et régions AWS
- Migrer un compte de membre AWS depuis AWS Organizations vers AWS Control Tower
- Surveillez les clusters SAP RHEL Pacemaker à l'aide des services AWS
- Surveillez l'activité des applications à l'aide de CloudWatch Logs Insights
- Surveillez l'utilisation d'une Amazon Machine Image partagée sur plusieurs Comptes AWS
- Configurez des alertes pour les fermetures de comptes programmatiques dans AWS Organizations
- Afficher les détails des instantanés EBS pour votre compte AWS ou votre organisation
- Plus de modèles

Identifiez et alertez lorsque les ressources Amazon Data Firehose ne sont pas chiffrées à l'aide d'une clé AWS KMS

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Pour des raisons de conformité, certaines entreprises doivent activer le chiffrement sur les ressources de diffusion de données telles qu'Amazon Data Firehose. Ce modèle montre un moyen de surveiller, de détecter et de notifier lorsque les ressources ne sont pas conformes.

Pour respecter les exigences de chiffrement, ce modèle peut être utilisé AWS pour surveiller et détecter automatiquement les ressources de livraison Amazon Data Firehose qui ne sont pas chiffrées à l'aide d'une clé AWS Key Management Service (AWS KMS). La solution envoie des notifications d'alerte et peut être étendue pour effectuer une correction automatique. Cette solution peut être appliquée à un compte individuel ou à un environnement à comptes multiples, tel qu'un environnement utilisant une zone d' AWS atterrissage ou. AWS Control Tower

Conditions préalables et limitations

Prérequis

- Flux de livraison d'Amazon Data Firehose
- Autorisations suffisantes et connaissance de ce qui est utilisé dans le cadre de cette automatisation de l'infrastructure AWS CloudFormation

Limites

- La solution n'est pas en temps réel car elle utilise des AWS CloudTrail événements pour la détection, et il existe un délai entre le moment où une ressource non chiffrée est créée et celui où la notification est envoyée.

Architecture

Pile technologique cible

La solution utilise la technologie sans serveur et les services suivants :

- AWS CloudTrail

- Amazon CloudWatch
- AWS Command Line Interface (AWS CLI)
- AWS Identity and Access Management (JE SUIS)
- Amazon Data Firehose
- AWS Lambda
- Amazon Simple Notification Service (Amazon SNS)

Architecture cible

Le schéma illustre les étapes suivantes :

1. Un utilisateur crée ou modifie Amazon Data Firehose.
2. Un CloudTrail événement est détecté et mis en correspondance.
3. Lambda est invoqué.
4. Les ressources non conformes sont identifiées.
5. Une notification par e-mail est envoyée.

Automatisation et mise à l'échelle

Vous pouvez appliquer cette solution AWS CloudFormation StackSets à plusieurs comptes Régions AWS ou à l'aide d'une seule commande.

Outils

- AWS CloudTrailest un outil Service AWS qui vous aide à assurer la gouvernance, la conformité, ainsi que l'audit opérationnel et des risques de votre entreprise Compte AWS. Les actions entreprises par un utilisateur, un rôle ou un Service AWS sont enregistrées sous forme d'événements dans CloudTrail. Les événements incluent les actions entreprises dans le cadre des opérations AWS Management Console AWS CLI AWS SDKs,, et de l'API.
- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS en utilisant des commandes dans votre interface de ligne de commande.

- AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources. Vous pouvez utiliser IAM pour contrôler les personnes qui s’authentifient (sont connectées) et sont autorisées (disposent d’autorisations) à utiliser des ressources.
- Amazon Data Firehose est un service entièrement géré qui fournit des données de streaming en temps réel. Avec Firehose, vous n'avez pas à écrire d'applications ni à gérer de ressources. Vous configurez vos producteurs de données pour envoyer les données à Firehose, qui remet automatiquement les données à la destination que vous avez spécifiée.
- AWS Lambdaest un service de calcul qui prend en charge l'exécution de code sans provisionnement ni gestion de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l’échelle automatiquement, qu’il s’agisse de quelques requêtes par jour ou de milliers de requêtes par seconde. Vous ne payez que pour le temps de calcul que vous consommez. Aucun frais n'est facturé lorsque votre code n'est pas en cours d'exécution.
- Amazon Simple Notification Service (Amazon SNS) est un service géré qui permet aux éditeurs de transmettre des messages aux abonnés (également appelés producteurs et consommateurs).

Épopées

Appliquer le chiffrement à des fins de conformité

Tâche	Description	Compétences requises
Déployez AWS CloudFormation StackSets.	Dans le AWS CLI, utilisez le `firehose-encryption-checker.yaml` modèle (joint) pour créer l'ensemble de piles en exécutant la commande suivante. Indiquez une rubrique Amazon SNS valide (Amazon Resource Name) pour le paramètre. Le déploiement doit réussir à créer CloudWatch des règles d'événements, la fonction Lambda et un rôle IAM avec	Architecte cloud, administrateur système

Tâche	Description	Compétences requises
	les autorisations nécessaires, comme décrit dans le modèle. `aws cloudformation create-stack-set --stack-set-name my-stack-set --template-body file://firehose-encryption-checker.yaml`	
Créez des instances de pile.	Les piles peuvent être créées dans le compte Régions AWS de votre choix ainsi que dans un ou plusieurs comptes. Pour créer des instances de pile, exécutez la commande suivante. Remplacez le nom de la pile, les numéros de compte et les régions par les vôtres. `aws cloudformation create-stack-instances --stack-set-name my-stack-set --accounts 123456789012 223456789012 --regions us-east-1 us-east-2 us-west-1 us-west-2 --operation-preferences FailureToleranceCount=1`	Architecte cloud, administrateur système

Ressources connexes

- Travailler avec AWS CloudFormation StackSets

- Qu'est-ce qu'Amazon CloudWatch Events ?

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Automatisez l'ajout ou la mise à jour d'entrées de registre Windows à l'aide d'AWS Systems Manager

Créée par Appasaheb Bagali (AWS)

Récapitulatif

AWS Systems Manager est un outil de gestion à distance pour les instances Amazon Elastic Compute Cloud (Amazon EC2). Systems Manager assure la visibilité et le contrôle de votre infrastructure sur Amazon Web Services. Cet outil polyvalent peut être utilisé pour corriger les modifications du registre Windows identifiées comme des vulnérabilités par le rapport d'analyse des vulnérabilités de sécurité.

Ce modèle décrit les étapes à suivre pour sécuriser vos EC2 instances exécutant le système d'exploitation Windows en automatisant les modifications de registre recommandées pour la sécurité de votre environnement. Le modèle utilise la commande Exécuter pour exécuter un document de commande. Le code est joint, et une partie de celui-ci est incluse dans la section Code.

Conditions préalables et limitations

- Un compte AWS actif
- Autorisations d'accès à l' EC2 instance et à Systems Manager

Architecture

Pile technologique cible

- Un cloud privé virtuel (VPC), avec deux sous-réseaux et une passerelle de traduction d'adresses réseau (NAT)
- Un document de commande de Systems Manager pour ajouter ou mettre à jour le nom et la valeur du registre
- Systems Manager Run Command pour exécuter le document de commande sur les EC2 instances spécifiées

Architecture cible

Outils

Outils

- Politiques et rôles IAM — AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux ressources AWS. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources.
- Amazon Simple Storage Service — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Il est conçu pour faciliter l'informatique à l'échelle d'Internet pour les développeurs. Dans ce modèle, un compartiment S3 est utilisé pour stocker les journaux de Systems Manager.
- AWS Systems Manager — AWS Systems Manager est un service AWS que vous pouvez utiliser pour visualiser et contrôler votre infrastructure sur AWS. Systems Manager vous aide à maintenir la sécurité et la conformité en scannant vos instances gérées et en signalant (ou en prenant des mesures correctives) les violations des politiques détectées.
- Document de commande d'AWS Systems Manager — Les documents de commande d'AWS Systems Manager sont utilisés par Run Command. La plupart des documents de commande sont pris en charge sur tous les systèmes d'exploitation Linux et Windows Server pris en charge par Systems Manager.
- AWS Systems Manager Run Command — AWS Systems Manager Run Command vous permet de gérer la configuration de vos instances gérées à distance et en toute sécurité. À l'aide de Run Command, vous pouvez automatiser les tâches administratives courantes et effectuer des modifications de configuration ponctuelles à grande échelle.

Code

Vous pouvez utiliser l'exemple de code suivant pour ajouter ou mettre à jour un nom de registre Microsoft Windows vers`Version`, un chemin de registre vers `HKCU:\Software\ScriptingGuys\Scripts` et une valeur vers2.

```
#Windows registry path which needs to add/update
$registryPath ='HKCU:\\Software\\ScriptingGuys\\Scripts'
#Windows registry Name  which needs to add/update
$Name = 'Version'
#Windows registry value  which needs to add/update
```

```
$value = 2
# Test-Path cmdlet to see if the registry key exists.
IF(!(Test-Path $registryPath))
        {
           New-Item -Path $registryPath -Force | Out-Null
           New-ItemProperty -Path $registryPath -Name $name -Value     $value ` -
PropertyType DWORD -                 Force | Out-        Null
        } ELSE {
                      New-ItemProperty -Path $registryPath -Name $name -Value $value `
 -PropertyType            DWORD        -Force | Out-Null
            }
echo 'Registry Path:'$registryPath
 echo 'Registry Name:'$registryPath
 echo 'Registry Value:'(Get-ItemProperty -Path $registryPath -Name $Name).version
```

L'exemple de code complet du document JavaScript de commande Systems Manager Command Notation (JSON) est joint en annexe.

Épopées

Configurez un VPC

Tâche	Description	Compétences requises
Créez un VPC.	Sur la console de gestion AWS, créez un VPC doté de sous-réseaux publics et privés et d'une passerelle NAT. Pour plus d'informations, consultez la documentation AWS.	Administrateur du cloud
Créez des groupes de sécurité.	Assurez-vous que chaque groupe de sécurité autorise l'accès au protocole RDP (Remote Desktop Protocol) à partir de l'adresse IP source.	Administrateur du cloud

Création d'une politique IAM et d'un rôle IAM

Tâche	Description	Compétences requises
Créez une politique IAM.	Créez une politique IAM qui donne accès à Amazon S3 EC2, Amazon et Systems Manager.	Administrateur du cloud
Créez un rôle IAM.	Créez un rôle IAM et associez la politique IAM qui fournit l'accès à Amazon S3 EC2, Amazon et Systems Manager.	Administrateur du cloud

Exécutez l'automatisation

Tâche	Description	Compétences requises
Créez le document de commande de Systems Manager.	Créez un document de commande Systems Manager qui déploiera les modifications du registre Microsoft Windows à ajouter ou à mettre à jour.	Administrateur du cloud
Exécutez la commande Systems Manager Run.	Exécutez la commande Run de Systems Manager en sélectionnant le document de commande et les instances cibles de Systems Manager. Cela transmet la modificat ion du registre Microsoft Windows dans le document de commande sélectionné aux instances cibles.	Administrateur du cloud

Ressources connexes

- AWS Systems Manager
- Documents AWS Systems Manager
- AWS Systems Manager Exécuter la commande

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez automatiquement une RFC dans AMS à l'aide de Python

Créée par Gnanasekaran Kailasam (AWS)

Récapitulatif

AWS Managed Services (AMS) vous aide à exploiter votre infrastructure basée sur le cloud de manière plus efficace et sécurisée en fournissant une gestion continue de votre infrastructure Amazon Web Services (AWS). Pour apporter une modification à votre environnement géré, vous devez créer et soumettre une nouvelle demande de modification (RFC) qui inclut un ID de type de modification (CT) pour une opération ou une action particulière.

Cependant, la création manuelle d'un RFC peut prendre environ cinq minutes et les équipes de votre organisation peuvent avoir besoin d'en soumettre plusieurs RFCs chaque jour. Ce modèle vous aide à automatiser le processus de création des RFC, à réduire le temps de création de chaque RFC et à éliminer les erreurs manuelles.

Ce modèle décrit comment utiliser le code Python pour créer automatiquement la `Stop EC2 instance` RFC qui arrête les instances Amazon Elastic Compute Cloud (Amazon EC2) dans votre compte AMS. Vous pouvez ensuite appliquer l'approche de ce modèle et l'automatisation Python à d'autres types de RFC.

Conditions préalables et limitations

Prérequis

- Un compte AMS Advanced. Pour plus d'informations à ce sujet, consultez les plans d'opérations AMS dans la documentation AWS Managed Services.
- Au moins une EC2 instance existante dans votre compte AMS.
- Compréhension de la manière de créer et de soumettre RFCs dans AMS.
- Connaissance de Python.

Limites

- Vous ne pouvez l'utiliser que RFCs pour des modifications dans votre compte AMS. Votre compte AWS utilise différents processus pour des modifications similaires.

Architecture

Pile technologique

- AMS
- Interface de ligne de commande AWS (AWS CLI)
- Kit AWS SDK pour Python (Boto3)
- Python et ses packages requis (JSON et Boto3)

Automatisation et évolutivité

Ce modèle fournit un exemple de code pour automatiser le `Stop EC2 instance` RFC, mais vous pouvez utiliser l'exemple de code et l'approche de ce modèle pour d'autres RFCs.

Outils

- AWS Managed Services — AMS vous aide à exploiter votre infrastructure AWS de manière plus efficace et plus sécurisée.
- AWS CLI — AWS Command Line Interface (AWS CLI) est un outil unifié permettant de gérer vos services AWS. Dans AMS, l'API de gestion des modifications fournit des opérations à créer et à gérer RFCs.
- SDK AWS pour Python (Boto3) — Le SDK pour Python facilite l'intégration de votre application, bibliothèque ou script Python aux services AWS.

Code

Le `AMS Stop EC2 Instance.zip` fichier (joint) contient le code Python permettant de créer une `Stop EC2 instance` RFC. Vous pouvez également configurer ce code pour soumettre une seule RFC pour plusieurs EC2 instances.

Épopées

Option 1 — Configuration de l'environnement pour macOS ou Linux

Tâche	Description	Compétences requises
Installez et validez Python.	1. Ouvrez une fenêtre de terminal et exécutez la	Administrateur système AWS

Tâche	Description	Compétences requises
	`brew install python3` commande. 2. Vérifiez que Python est correctement installé en exécutant la `python --version` commande. 3. Vérifiez qu'`pip`il est correctement installé en exécutant la `pip --version` commande.	
Installez AWS CLI.	Exécutez la `pip install awscli --upgrade –user` commande pour installer l'AWS CLI.	Administrateur système AWS
Installez Boto3.	Exécutez la `pip install boto3` commande pour installer Boto3.	Administrateur système AWS
Installez JSON.	Exécutez la `pip install json` commande pour installer le JSON.	Administrateur système AWS

Tâche	Description	Compétences requises
Configurez la CLI AMS.	Connectez-vous à la console de gestion AWS, ouvrez la console AMS, puis choisissez Documentation. Téléchargez le fichier .zip qui contient la CLI AMS, décompressez-le, puis installez-le sur votre machine locale. Après avoir installé AMS CLI, exécutez la `aws amscm help` commande. La sortie fournit des informations sur le processus de gestion des modifications AMS.	Administrateur système AWS

Option 2 — Configuration de l'environnement pour Windows

Tâche	Description	Compétences requises
Installez et validez Python.	1. Ouvrez la page des versions de Python pour Windows, téléchargez la dernière version, puis installez Python. 2. Vérifiez que Python est correctement installé en exécutant la `python --version` commande. 3. Vérifiez qu'`pip`il est correctement installé en exécutant la `pip --version` commande.	Administrateur système AWS

Tâche	Description	Compétences requises
Installez AWS CLI.	Exécutez la `pip install awscli --upgrade –user` commande pour installer l'AWS CLI.	Administrateur système AWS
Installez Boto3.	Exécutez la `pip install boto3` commande pour installer Boto3.	Administrateur système AWS
Installez JSON.	Exécutez la `pip install json` commande pour installer le JSON.	Administrateur système AWS
Configurez la CLI AMS.	Connectez-vous à la console de gestion AWS, ouvrez la console AMS, puis choisissez Documentation. Téléchargez le fichier .zip qui contient la CLI AMS, décompressez-le, puis installez-le sur votre machine locale. Après avoir installé AMS CLI, exécutez la `aws amscm help` commande. La sortie fournit des informations sur le processus de gestion des modifications AMS.	Administrateur système AWS

Extraire l'ID CT et les paramètres d'exécution de la RFC

Tâche	Description	Compétences requises
Extrayez l'ID CT, la version et les paramètres d'exécution de la RFC.	Chaque RFC possède un ID CT, une version et des paramètres d'exécution différents. Vous pouvez extraire ces informations en utilisant l'une des options suivantes : 1. Suivez les instructions de la section Finding a request for change (RFC) with the CLI de RFC. Exemples d'utilisation tirés de la documentation AWS Managed Services. 2. Ouvrez un RFC existant d'un type similaire ou créez-en un nouveau à titre de test via la console AMS. Utilisez l'ID CT et les paramètres d'exécuti on du RFC. Pour plus d'informations à ce sujet, consultez Finding an RFC with the console dans la documentation AWS Managed Services. **Note** Pour adapter l'automat isation Python de ce	Administrateur système AWS

Tâche	Description	Compétences requises
	modèle à d'autres RFCs, remplacez le type CT et les valeurs des paramètre s du `AMS Stop EC2 Instance. zip` fichier de code `ams_stop_ ec2_instance` Python (joint) par ceux que vous avez extraits.	

Exécutez l'automatisation Python

Tâche	Description	Compétences requises
Exécutez l'automatisation Python.	1. Téléchargez le `AMS Stop EC2 Instance.zip` fichier (joint) sur votre ordinateur local et extrayez-le. 2. Mettez à jour `input_ins tances` avec les informati ons de votre EC2 instance. 3. Ouvrez un terminal et naviguez jusqu'au chemin de votre code extrait 4. Exécutez la commande `pythonams_stop_ec2 _instance.py` .	Administrateur système AWS

Ressources connexes

- Quels sont les types de modifications ?
- Tutoriel CLI : pile à deux niveaux à haute disponibilité (Linux/RHEL)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Arrêtez et démarrez automatiquement une instance de base de données Amazon RDS à l'aide de AWS Systems Manager Maintenance Windows

Créée par Ashita Dsilva (AWS)

Récapitulatif

Ce modèle montre comment arrêter et démarrer automatiquement une instance de base de données Amazon Relational Database Service (Amazon RDS) selon un calendrier spécifique (par exemple, arrêter une instance de base de données en dehors des heures ouvrables pour réduire les coûts) à l'aide de Windows de AWS Systems Manager maintenance.

AWS Systems Manager Automation fournit les `AWS-StartRdsInstance` manuels `AWS-StopRdsInstance` et exécutables permettant d'arrêter et de démarrer les instances de base de données Amazon RDS. Cela signifie que vous n'avez pas besoin d'écrire une logique personnalisée avec des AWS Lambda fonctions ou de créer une règle Amazon CloudWatch Events.

Systems Manager fournit deux fonctionnalités pour planifier les tâches : State Manager et Maintenance Windows. State Manager définit et gère la configuration d'état requise pour les ressources de votre compte Amazon Web Services (AWS) une fois ou selon un calendrier spécifique. Maintenance Windows exécute des tâches sur les ressources de votre compte pendant une période donnée. Bien que vous puissiez utiliser cette approche avec State Manager ou Maintenance Windows, nous vous recommandons d'utiliser Maintenance Windows car il permet d'exécuter une ou plusieurs tâches en fonction de la priorité assignée et peut également exécuter des AWS Lambda fonctions et AWS Step Functions des tâches. Pour plus d'informations sur State Manager et les fenêtres de maintenance, consultez Choisir entre les fenêtres State Manager et Maintenance dans la documentation de Systems Manager.

Ce modèle fournit des étapes détaillées pour configurer deux fenêtres de maintenance distinctes qui utilisent des expressions cron pour arrêter puis démarrer une instance de base de données Amazon RDS.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- Une instance de base de données Amazon RDS existante que vous souhaitez arrêter et démarrer selon un calendrier spécifique.

- Expressions Cron correspondant à votre calendrier requis. Par exemple, l'expression `cron(0 9 ? * MON-FRI *)` exécute la tâche à 9 h 00 tous les lundis, mardis, mercredis, jeudis et vendredis. Pour plus d'informations, consultez les expressions Cron et rate pour les fenêtres de maintenance dans la documentation de Systems Manager.
- Connaissance de Systems Manager.
- Autorisations permettant de démarrer et d'arrêter l'instance RDS. Pour plus d'informations, consultez la section Epics.

Limites

- Une instance de base de données Amazon RDS peut être arrêtée jusqu'à sept jours à la fois. Après sept jours, l'instance de base de données redémarre automatiquement pour s'assurer qu'elle reçoit toutes les mises à jour de maintenance requises.
- Vous ne pouvez pas arrêter une instance de base de données qui est une réplique en lecture ou qui possède une réplique en lecture.
- Vous ne pouvez pas arrêter une instance de base de données Amazon RDS for SQL Server dans une configuration multi-AZ.
- Les quotas de service s'appliquent à Maintenance Windows et à Systems Manager Automation. Pour plus d'informations sur les quotas de service, consultez la section AWS Systems Manager Points de terminaison et quotas dans la Références générales AWS documentation.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Le schéma suivant montre le flux de travail permettant d'arrêter et de démarrer automatiquement une instance de base de données Amazon RDS.

Le flux de travail comporte les étapes suivantes :

1. Créez une fenêtre de maintenance et utilisez des expressions cron pour définir le calendrier d'arrêt et de démarrage de vos instances de base de données Amazon RDS.

2. Enregistrez une tâche d'automatisation de Systems Manager dans la fenêtre de maintenance à l'aide du `AWS-StopRdsInstance` ou `AWS-StartRdsInstance` runbook.

3. Enregistrez une cible dans la fenêtre de maintenance en utilisant un groupe de ressources basé sur des balises pour vos instances de base de données Amazon RDS.

Pile technologique

- AWS CloudFormation
- AWS Identity and Access Management (JE SUIS)
- Amazon RDS
- Systems Manager

Automatisation et mise à l'échelle

Vous pouvez arrêter et démarrer plusieurs instances de base de données Amazon RDS en même temps en balisant les instances de base de données Amazon RDS requises, en créant un groupe de ressources incluant toutes les instances de base de données étiquetées et en enregistrant ce groupe de ressources en tant que cible pour la fenêtre de maintenance.

Outils

- AWS CloudFormationest un service qui vous aide à modéliser et à configurer vos AWS ressources.
- AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources.
- Amazon Relational Database Service (Amazon RDS) est un service Web qui facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le. AWS Cloud
- AWS Resource Groupsvous aide à organiser AWS les ressources en groupes, à étiqueter les ressources et à gérer, surveiller et automatiser les tâches sur les ressources groupées.
- AWS Systems Managerest un Service AWS outil que vous pouvez utiliser pour visualiser et contrôler votre infrastructure AWS. Ce modèle utilise les fonctionnalités suivantes de Systems Manager :
  - AWS Systems Manager L'automatisation simplifie les tâches courantes de maintenance et de déploiement des instances Amazon Elastic Compute Cloud (Amazon EC2) et d'autres AWS ressources.

- AWS Systems Manager Maintenance Windows vous aide à définir un calendrier indiquant quand effectuer des actions potentiellement perturbatrices sur vos instances.

Épopées

Création et configuration du rôle de service IAM pour Systems Manager Automation

Tâche	Description	Compétences requises
Configurez le rôle de service IAM pour Systems Manager Automation.	Connectez-vous au AWS Management Console et créez un rôle de service pour Systems Manager Automation. Vous pouvez utiliser l'une des deux méthodes suivantes pour créer ce rôle de service : • AWS CloudFormation À utiliser pour configurer un rôle de service pour Systems Manager Automation • Utiliser IAM pour configurer les rôles pour Systems Manager Automation Le flux de travail Systems Manager Automation invoque Amazon RDS en utilisant un rôle de service pour effectuer des actions de démarrage et d'arrêt sur l'instance de base de données Amazon RDS. Le rôle de service doit être configuré selon la politique en ligne suivante, qui autorise	Administrateur AWS

Tâche	Description	Compétences requises
	le démarrage et l'arrêt de l'instance de base de données Amazon RDS : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "RdsStartStop", "Effect": "Allow", "Action": [ "rds:StopDBInstance", "rds:StartDBInstance" ], "Resource": "<RDS_Instance_ARN>" }, { "Sid": "RdsDescribe", "Effect": "Allow", "Action": "rds:DescribeDBInstances", "Resource": "*" } ] }` Assurez-vous de le remplacer par le nom `<RDS_Instance_ARN>` de ressource	

Tâche	Description	Compétences requises
	Amazon (ARN) de votre instance de base de données Amazon RDS. Si vous n'êtes pas habitué à utiliser les politiques et les rôles IAM, suivez les instructions de la section Présentation de la solution du billet de AWS Systems Manager blog Schedule Amazon RDS stop and start using. ⚠ Important Assurez-vous d'enregistrer l'ARN du rôle de service.	

Création d'un groupe de ressources

Tâche	Description	Compétences requises
Marquez les instances de base de données Amazon RDS.	Ouvrez la console Amazon RDS et balisez les instances de base de données Amazon RDS que vous souhaitez ajouter au groupe de ressources. Une balise est une métadonnée attribuée à une AWS ressource et consiste en une paire clé-valeur. Nous vous recommandons d'utiliser Action comme	Administrateur AWS

Tâche	Description	Compétences requises
	clé Tag et StartStopcomme valeur. Pour plus d'informations à ce sujet, consultez la section Ajouter, répertorier et supprimer des balises dans la documentation Amazon RDS.	

Tâche	Description	Compétences requises
Créez un groupe de ressources pour vos instances de base de données Amazon RDS balisées.	Ouvrez la AWS Resource Groups console et créez un groupe de ressources en fonction de la balise que vous avez créée pour vos instances de base de données Amazon RDS. Sous Critères de regroupement, assurez-vous de choisir AWS : :RDS : : DBInstance pour le type de ressource, puis de fournir la paire clé-valeur de la balise (par exemple, « Action- »). StartStop Cela garantit que le service vérifie uniquement les instances de base de données Amazon RDS et non les autres ressources dotées de cette balise. Assurez-vous d'enregistrer le nom du groupe de ressources. Pour plus d'informations et des étapes détaillées, voir Création d'une requête basée sur des balises et création d'un groupe dans la AWS Resource Groups documentation.	Administrateur AWS

Configurer une fenêtre de maintenance pour arrêter les instances de base de données Amazon RDS

Tâche	Description	Compétences requises
Créez une fenêtre de maintenance.	1. Ouvrez la console Systems Manager, choisissez Maintenance Windows, puis Create a maintenance window. Donnez un nom à votre fenêtre de maintenance (par exemple, StopRdsInstance « »), entrez une description, puis décochez Autoriser les cibles non enregistrées. 2. Choisissez l'expression CRON/rate et fournissez l'expression de planification pour définir le moment où les instances de base de données Amazon RDS doivent être arrêtées. Entrez 1 pour la durée et 0 pour Arrêter de lancer des tâches. Par défaut, le fuseau horaire indique UTC. Vous pouvez modifier le fuseau horaire pour lancer la fenêtre de maintenance en fonction de l'horodatage défini dans votre expression cron. 3. Sélectionnez Create maintenance window (Créer une fenêtre de maintenance). Le système vous	Administrateur AWS

Tâche	Description	Compétences requises
	renvoie à la page de la fenêtre de maintenance et l'état de votre fenêtre de maintenance est Activé. ⚠ Important La tâche d'arrêt de l'instance de base de données s'exécute presque instantan ément lorsqu'elle est lancée et ne s'étend pas sur toute la durée de la fenêtre de maintenance. Ce modèle fournit les valeurs minimales pour les tâches Duration et Arrêter de lancer des tâches, car il s'agit des paramètre s requis pour une fenêtre de maintenan ce. Pour plus d'informations et des étapes détaillées, consultez la section Créer une fenêtre de maintenance (console) dans la documentation de Systems Manager.	

Tâche	Description	Compétences requises
Attribuez une cible à la fenêtre de maintenance.	1. Sur la console Systems Manager, choisissez Maintenance Windows, Actions, puis Register targets. 2. Dans la zone Cibles, spécifiez Choisir un groupe de ressources, puis choisissez le nom d'un groupe de ressources existant dans votre compte. 3. Pour les types de ressources, choisissez AWS : :RDS : : DBInstance puis choisissez Register target. Pour plus d'informations et des étapes détaillées, voir Affecter des cibles à une fenêtre de maintenance (console) dans la documentation de Systems Manager.	Administrateur AWS

Tâche	Description	Compétences requises
Affectez une tâche à la fenêtre de maintenance.	1. Sur la console Systems Manager, choisissez Maintenance Windows, puis choisissez votre fenêtre de maintenance. Choisisse z Actions, puis sélection nez Enregistrer la tâche d'automatisation. 2. Pour Document, choisissez AWS- StopRdsInstance. 3. Dans la section Cibles, choisissez Sélection des groupes cibles enregistr és, puis choisissez la cible de la fenêtre de maintenan ce que vous avez enregistr ée dans la fenêtre de maintenance actuelle. 4. Pour le contrôle du débit, spécifiez 100 % pour la simultanéité et le seuil d'erreur. Vous pouvez modifier les valeurs de contrôle du taux en fonction de vos besoins en matière de simultanéité des tâches et de seuil d'erreur. Pour plus d'informations à ce sujet, consultez la section À propos de la simultanéité et des seuils d'erreur dans la documentation de Systems Manager.	Administrateur AWS

Tâche	Description	Compétences requises
	5. Dans la section Rôle de service IAM, pour Rôle de service, laissez cette case vide ou créez votre propre rôle personnalisé. Si vous laissez le champ vide, Systems Manager crée automatiquement le rôle AWSServiceRoleForAmazonSSM lié au service, puis associe le rôle à la tâche. Pour créer votre propre rôle personnalisé, voir Créer un rôle de service personnalisé pour les fenêtres de maintenance (console), puis associez ce rôle personnalisé à la tâche. 6. Dans la section Paramètres d'entrée, spécifiez les paramètres suivants pour le runbook : • InstanceId: `{{RESOURCE_ID}}` **Note** En InstanceIdeffet, un pseudo-paramètre est utilisé pour extraire l'ID de ressource de base de données	

Tâche	Description	Compétences requises
	Amazon RDS de l'ARN. Pour en savoir plus sur les pseudo-paramètres, consultez la section À propos des pseudo-paramètres dans la documentation de Systems Manager. • AutomationAssumeRole: Indiquez l'ARN du rôle de service que vous avez créé pour Systems Manager Automation. 7. Choisissez Enregistrer la tâche d'automatisation. **Important** L'option Service role définit le rôle de service requis pour que la fenêtre de maintenance exécute les tâches. Toutefois, ce rôle n'est pas identique au rôle de service que vous avez créé précédemm	

Tâche	Description	Compétences requises
	ent pour Systems Manager Automation. Pour plus d'informations et des étapes détaillées, voir Affecter des tâches à une fenêtre de maintenance (console) dans la documentation de Systems Manager.	

Configurer une fenêtre de maintenance pour démarrer les instances de base de données Amazon RDS

Tâche	Description	Compétences requises
Configurez une fenêtre de maintenance pour démarrer les instances de base de données Amazon RDS.	Répétez les étapes décrites dans la fenêtre Configurer une maintenance pour arrêter les instances de base de données Amazon RDS (Epic) pour configurer une autre fenêtre de maintenance afin de démarrer les instances de base de données Amazon RDS à une heure planifiée. ⚠ Important Vous devez apporter les modifications suivantes lorsque vous configurez la fenêtre de maintenance pour	Administrateur AWS

Tâche	Description	Compétences requises
	démarrer les instances de base de données : • Utilisez un nouveau nom pour la fenêtre de maintenance (par exemple, StartRdsInstance « »). • Remplacez l'expression cron par l'expression cron que vous souhaitez utiliser pour démarrer les instances de base de données. • Remplacez le `AWS-StopRdsInstance` runbook par `AWS-StartRdsInstance` dans Task.	

Ressources connexes

- Utilisez les documents Systems Manager Automation pour gérer les instances et réduire les coûts en dehors des heures de bureau (article de AWS blog)

Centralisez la distribution des packages logiciels dans AWS Organizations à l'aide de Terraform

Créée par Pradip Kumar Pandey (AWS), Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Mayuri Shinde (AWS) et Pratap Kumar Nanda (AWS)

Récapitulatif

Les entreprises en maintiennent souvent plusieurs Comptes AWS réparties sur plusieurs Régions AWS afin de créer une barrière d'isolation solide entre les charges de travail. Pour garantir la sécurité et la conformité, leurs équipes d'administration installent des outils basés sur des agents tels que CrowdStrikeSentinelOne, ou des TrendMicrooutils d'analyse de sécurité, ainsi que l' CloudWatch agent Amazon, l'agentDatadog ou AppDynamics des agents de surveillance. Ces équipes sont souvent confrontées à des défis lorsqu'elles souhaitent automatiser de manière centralisée la gestion et la distribution des progiciels dans ce vaste environnement.

Distributor, une fonctionnalité de AWS Systems Manager, automatise le processus d'empaquetage et de publication de logiciels sur des instances Microsoft Windows et Linux gérées sur le cloud et sur des serveurs locaux via une interface simplifiée unique. Ce modèle montre comment vous pouvez utiliser Terraform pour simplifier davantage le processus de gestion de l'installation des logiciels et pour exécuter des scripts sur un grand nombre d'instances et de comptes membres AWS Organizations avec un minimum d'effort.

Cette solution fonctionne pour les instances Amazon, Linux et Windows gérées par Systems Manager.

Conditions préalables et limitations

- Un package de distribution contenant le logiciel à installer
- Terraform version 0.15.0 ou ultérieure
- Instances Amazon Elastic Compute Cloud (Amazon EC2) gérées par Systems Manager et dotées d'autorisations de base pour accéder à Amazon Simple Storage Service (Amazon S3) sur le compte cible
- Une zone de landing zone pour votre organisation, configurée à l'aide de AWS Control Tower
- (Facultatif) Account Factory pour Terraform (AFT)

Architecture

Détails de la ressource

Ce modèle utilise Account Factory for Terraform (AFT) pour créer toutes les AWS ressources requises et le pipeline de code pour déployer les ressources dans un compte de déploiement. Le pipeline de code s'exécute dans deux référentiels :

- La personnalisation globale contient le code Terraform qui s'appliquera à tous les comptes enregistrés auprès d'AFT.
- Les personnalisations de compte contiennent du code Terraform qui s'exécutera dans le compte de déploiement.

Vous pouvez également déployer cette solution sans utiliser AFT, en exécutant les commandes Terraform dans le dossier de personnalisation du compte.

Le code Terraform déploie les ressources suivantes :

- AWS Identity and Access Management rôle et politiques (IAM)
  - SystemsManager- AutomationExecutionRole accorde à l'utilisateur l'autorisation d'exécuter des automatisations dans les comptes cibles.
  - SystemsManager- AutomationAdministrationRole accorde à l'utilisateur l'autorisation d'exécuter des automatisations dans plusieurs comptes et unités organisationnelles (OUs).
- Fichiers compressés et manifest.json pour le package
  - Dans Systems Manager, un package inclut au moins un fichier .zip de logiciels ou de ressources installables.
  - Le manifeste JSON inclut des pointeurs vers les fichiers de code de votre package.
- Compartiment S3
  - Le package distribué partagé au sein de l'organisation est stocké de manière sécurisée dans un compartiment Amazon S3.
- AWS Systems Manager documents (documents SSM)
  - `DistributeSoftwarePackage`contient la logique permettant de distribuer le package logiciel à chaque instance cible des comptes membres.
  - `AddSoftwarePackageToDistributor`contient la logique permettant de regrouper les actifs logiciels installables et de les ajouter à Automation, une fonctionnalité de AWS Systems Manager.

- Association Systems Manager
  - Une association Systems Manager est utilisée pour déployer la solution.

Architecture et flux de travail

Le diagramme suivant illustre les étapes suivantes :

1. Pour exécuter la solution à partir d'un compte centralisé, vous téléchargez vos packages ou logiciels ainsi que les étapes de déploiement dans un compartiment S3.
2. Votre package personnalisé est disponible dans la section Documents de la console Systems Manager, dans l'onglet Owned by me.
3. State Manager, une fonctionnalité de Systems Manager, crée, planifie et exécute une association pour le package au sein de l'organisation. L'association indique que le package logiciel doit être installé et exécuté sur un nœud géré avant de pouvoir être installé sur le nœud cible.
4. L'association demande à Systems Manager d'installer le package sur le nœud cible.
5. Pour toute installation ou modification ultérieure, les utilisateurs peuvent exécuter la même association périodiquement ou manuellement à partir d'un seul emplacement afin d'effectuer des déploiements sur plusieurs comptes.
6. Dans les comptes membres, Automation envoie des commandes de déploiement au distributeur.
7. Le distributeur distribue des progiciels entre les instances.

Cette solution utilise le compte de gestion AWS Organizations intégré, mais vous pouvez également désigner un compte (administrateur délégué) pour le gérer au nom de l'organisation.

Outils

Services AWS

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données. Ce modèle utilise Amazon S3 pour centraliser et stocker en toute sécurité le package distribué.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle. Ce modèle utilise les fonctionnalités suivantes de Systems Manager :

  - Distributor vous aide à empaqueter et à publier des logiciels sur des instances gérées par Systems Manager.
  - L'automatisation simplifie les tâches courantes de maintenance, de déploiement et de correction pour de nombreux AWS services.
  - Documents exécute des actions sur vos instances gérées par Systems Manager au sein de votre organisation et de vos comptes.
- AWS Organizationsest un service de gestion de comptes qui vous aide à consolider plusieurs AWS comptes au sein d'une organisation que vous créez et gérez de manière centralisée.

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources sur site et dans le cloud.

Référentiel de code

Les instructions et le code de ce modèle sont disponibles dans le référentiel de distribution de packages GitHub centralisé.

Bonnes pratiques

- Pour attribuer des balises à une association, utilisez le AWS Command Line Interface (AWS CLI) ou le Outils AWS pour PowerShell. L'ajout de balises à une association à l'aide de la console Systems Manager n'est pas pris en charge. Pour plus d'informations, consultez les ressources de Tagging Systems Manager dans la documentation de Systems Manager.
- Pour exécuter une association en utilisant une nouvelle version d'un document partagé depuis un autre compte, définissez la version du document sur`default`.
- Pour étiqueter uniquement le nœud cible, utilisez une seule clé de balise. Si vous souhaitez cibler vos nœuds à l'aide de plusieurs clés de balise, utilisez l'option de groupe de ressources.

Épopées

Configuration des fichiers source et des comptes

Tâche	Description	Compétences requises

Pour cloner le référentiel.	1. Clonez le référentiel de distribution de packages GitHub centralisé :
	`git clone https://github.com/aws-samples/aws-organization-centralised-package-distribution`
	2. Le référentiel de code Terraform nécessite deux dossiers de personnalisation gérés par AFT. Vérifiez que votre copie locale du référentiel contient les dossiers suivants :
	`$ cd centralised-package-distribution`
	`$ ls`
	`global-customization account-customization`
		DevOps ingénieur

Mettez à jour les variables globales.	Mettez à jour les paramètres d'entrée suivants dans le `global-customization/variables.tf` fichier. Ces variables s'appliquent à tous les comptes créés et gérés par AFT.	DevOps ingénieur

Tâche	Description	Compétences requises
	• `account_id` : ID du compte sur lequel la solution de distribution sera déployée. • `aws_region` : L' Région AWS endroit où l'association sera déployée.	
Mettez à jour les variables du compte.	Mettez à jour les paramètre s d'entrée suivants dans le `account-customizat ion/variables.tf` fichier. Ces variables s'appliqu ent uniquement à des comptes spécifiques créés et gérés par l'AFT. • `package_bucket_nam e` : nom du compartiment S3 qui contient le fichier de distribution du package. • `package_name` : nom du fichier de distribution du package. • `package_version` : version du package du programme d'installation.	DevOps ingénieur

Personnalisation des paramètres et des fichiers de déploiement

Tâche	Description	Compétences requises
Mettez à jour les paramètres d'entrée pour l'association State Manager.	Mettez à jour les paramètres d'entrée suivants dans le `account-customization/association.tf` fichier pour définir l'état que vous souhaitez conserver sur vos instances. Vous pouvez utiliser les valeurs des paramètres par défaut si elles correspondent à votre cas d'utilisation. • `targetAccounts` : unité organisationnelle (UO) au IDs sein d'AWS Organizations qui représente les comptes auprès des instances cibles à des fins de distribution. OU IDs commencez par « ou ». • `targetRegions` : le Régions AWS (par exemple, « us-east-1 » ou « ap-southeast-2 ») où les instances cibles sont exécutées. • `action`: Spécifiez s'il faut installer ou désinstaller le package. • `installationType` : l'un des types d'installation suivants :	DevOps ingénieur

Tâche	Description	Compétences requises
	• `uninstall` : le package est désinstallé. • `reinstall` : L'application est mise hors ligne jusqu'à ce que le processus de réinstallation soit terminé. • `In-place update`: L'application est disponible lorsque des fichiers nouveaux ou mis à jour sont ajoutés à l'installation. • `name`: nom du package à installer ou à désinstaller. • `version`: version du package à installer ou à désinstaller. Si aucune version du package n'est installée, le système renvoie une erreur. • `bucketName` : nom du compartiment S3 dans lequel le package a été déployé. Ce compartiment doit être composé uniquement des packages et du fichier manifeste. • `bucketPrefix` : le préfixe S3 dans lequel les actifs du package sont stockés. • `AutomationAssumeRole` : le nom de	

Tâche	Description	Compétences requises
	ressource Amazon (ARN) de`SystemsManager-AutomationAdministrationRole` .	
Préparez les fichiers compressés et le `manifest.json` fichier du package.	Ce modèle fournit des exemples de fichiers PowerShell installables (.msi pour Windows et .rpm pour Linux) avec des scripts d'installation et de désinstallation dans le dossier. `account-customization/package` 1. Remplacez les fichiers PowerShell installables par vos propres fichiers ou fournissez votre fichier installable, les scripts d'installation et de désinstallation et le fichier manifeste pour créer un package dans le `account-customization` dossier de votre compte. 2. Personnalisez le `manifest.json` fichier par défaut généré par Terraform dans le `account-customization` dossier en fonction de vos besoins.	DevOps ingénieur

Exécutez des commandes Terraform pour provisionner des ressources

Tâche	Description	Compétences requises

Initialisez la configuration Terraform.	Pour déployer la solution automatiquement avec AFT, envoyez le code à AWS CodeCommit :
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
	Vous pouvez également déployer cette solution sans utiliser AFT en exécutant une commande Terraform depuis le `account-customization` dossier. Pour initialiser le répertoire de travail contenant les fichiers Terraform, exécutez :
	`$ terraform init`
		DevOps ingénieur

Prévisualisez les modifications.	Pour prévisualiser les modifications que Terraform apportera à l'infrastructure, exécutez la commande : `$ terraform plan` Cette commande évalue la configuration Terraform pour déterminer l'état souhaité des ressources déclarées.	DevOps ingénieur

Tâche	Description	Compétences requises
	Il compare également l'état souhaité avec l'infrastructure réelle à fournir dans l'espace de travail.	
Appliquez les modifications.	Exécutez la commande suivante pour implémenter les modifications que vous avez apportées aux `variables.tf` fichiers : `$ terraform apply`	DevOps ingénieur

Valider les ressources

Tâche	Description	Compétences requises
Validez la création de documents SSM.	1. Sur la console Systems Manager, dans le volet de navigation de gauche, sélectionnez Documents. 2. Choisissez l'onglet M'appartenant. Vous devriez voir les `AddSoftwarePackageToDistributor` packages `DistributeSoftwarePackage` et.	DevOps ingénieur
Validez le déploiement réussi des automatisations.	1. Sur la console Systems Manager, dans le volet de navigation de gauche, choisissez Automation.	DevOps ingénieur

Tâche	Description	Compétences requises
	2. Dans la liste des exécutions automatisées, vous devriez voir les `AddSoftwarePackageToDistributor` déploiements `DistributeSoftwarePackage` et les déploiements les plus récents. 3. Choisissez l'ID d'exécution pour vérifier qu'ils se sont bien déroulés.	
Vérifiez que le package a été déployé sur les instances de compte de membre ciblées.	1. Sur la console Systems Manager, dans le volet de navigation, choisissez Run Command. 2. Dans l'historique des commandes, vous verrez chaque appel et son statut. 3. Choisissez n'importe quel ID de commande pour voir l'historique de déploiement de chaque instance cible. 4. Choisissez l'ID d'instance et consultez la section Sortie pour la distribution.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
L'association State Manager a échoué ou est bloquée en attente.	Consultez les informations de dépannage dans le centre de AWS connaissances.

Problème	Solution
Une association planifiée n'a pas pu être exécutée.	Les spécifications de votre calendrier ne sont peut-être pas valides. State Manager ne prend actuellement pas en charge la spécification de mois dans les expressions cron pour les associations. Utilisez des expressions cron ou rate pour confirmer le planning.

Ressources connexes

- Distribution de packages centralisée (GitHub référentiel)
- Account Factory pour Terraform (AFT)
- Cas d'utilisation et meilleures pratiques (AWS Systems Manager documentation)

Configurez la journalisation pour les applications .NET dans Amazon CloudWatch Logs en utilisant NLog

Créée par Bibhuti Sahu (AWS) et Rob Hill (AWS) (AWS)

Récapitulatif

Ce modèle décrit comment utiliser le framework de journalisation NLog open source pour enregistrer l'utilisation des applications .NET et les événements dans Amazon CloudWatch Logs. Dans la CloudWatch console, vous pouvez consulter les messages du journal de l'application quasiment en temps réel. Vous pouvez également configurer des métriques et des alarmes pour vous avertir en cas de dépassement d'un seuil de métrique. À l'aide CloudWatch d'Application Insights, vous pouvez consulter des tableaux de bord automatisés ou personnalisés qui indiquent les problèmes potentiels liés aux applications surveillées. CloudWatch Application Insights est conçu pour vous aider à isoler rapidement les problèmes récurrents liés à vos applications et à votre infrastructure.

Pour écrire des messages de journal dans CloudWatch Logs, vous devez ajouter le `AWS.Logger.NLog` NuGet package au projet .NET. Ensuite, vous mettez à jour le `NLog.config` fichier pour utiliser CloudWatch Logs comme cible.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une application Web ou console .NET qui :
  - Utilise les versions .NET Framework ou .NET Core prises en charge. Pour plus d'informations, consultez la section Versions du produit.
  - Utilisée NLog pour envoyer des données de journal à Application Insights.
- Autorisations permettant de créer un rôle IAM pour un service AWS. Pour plus d'informations, consultez la section Autorisations relatives aux rôles de service.
- Autorisations permettant de transmettre un rôle à un service AWS. Pour plus d'informations, consultez la section Octroi d'autorisations à un utilisateur pour transférer un rôle à un service AWS.

Versions du produit

- .NET Framework version 3.5 ou ultérieure

- Versions .NET Core 1.0.1, 2.0.0 ou ultérieures

Architecture

Pile technologique cible

- NLog
- Amazon CloudWatch Logs

Architecture cible

1. L'application .NET écrit les données du journal dans le framework de NLog journalisation.
2. NLog écrit les données du journal dans CloudWatch Logs.
3. Vous utilisez des CloudWatch alarmes et des tableaux de bord personnalisés pour surveiller l'application .NET.

Outils

Services AWS

- Amazon CloudWatch Application Insights vous aide à observer l'état de vos applications et des ressources AWS sous-jacentes.
- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- Les outils AWS pour PowerShell sont un ensemble de PowerShell modules qui vous aident à créer des scripts pour des opérations sur vos ressources AWS à partir de la ligne de PowerShell commande.

Autres outils

- Bûcheron. NLogest une NLog cible qui enregistre les données du journal dans CloudWatch Logs.

- NLogest un framework de journalisation open source pour les plateformes .NET qui vous permet d'écrire des données de journal sur des cibles, telles que des bases de données, des fichiers journaux ou des consoles.
- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS.
- Visual Studio est un environnement de développement intégré (IDE) qui inclut des compilateurs, des outils de complétion de code, des concepteurs graphiques et d'autres fonctionnalités qui prennent en charge le développement de logiciels.

Bonnes pratiques

- Définissez une politique de conservation pour le groupe de journaux cible. Cela doit être fait en dehors de la NLog configuration. Par défaut, les données du journal sont stockées dans les CloudWatch journaux indéfiniment.
- Respectez les meilleures pratiques en matière de gestion des clés d'accès AWS.

Épopées

Configurer l'accès et les outils

Tâche	Description	Compétences requises
Créez une politique IAM.	Suivez les instructions de la section Création de politiques à l'aide de l'éditeur JSON dans la documentation IAM. Entrez la politique JSON suivante, qui dispose des autorisations de moindre privilège nécessair es pour permettre à Logs de lire et d'écrire des CloudWatch journaux. `{ "Version": "2012-10-17",`	Administrateur AWS, AWS DevOps

Tâche	Description	Compétences requises
	"Statement": [{ "Effect": "Allow", "Action": ["logs:CreateLogGroup", "logs:CreateLogStream", "logs:GetLogEvents", "logs:PutLogEvents", "logs:DescribeLogGroups", "logs:DescribeLogStreams", "logs:PutRetentionPolicy"], "Resource": ["*"] }] }	

Tâche	Description	Compétences requises
Créez un rôle IAM.	Suivez les instructions de la section Création d'un rôle pour déléguer des autorisations à un service AWS dans la documentation IAM. Sélectionnez la politique que vous avez créée précédemment. C'est le rôle que CloudWatch Logs assume pour effectuer des actions de journalisation.	Administrateur AWS, AWS DevOps
Configurez les outils AWS pour PowerShell.	1. Suivez les instructions relatives à votre système d'exploitation dans la section Installation des outils AWS pour PowerShell. 2. Utilisez les outils AWS pour les PowerShell applets de commande pour stocker votre clé d'accès et votre clé secrète dans un profil. Pour obtenir des instructions, consultez la section Gestion des profils dans les outils AWS pour obtenir de PowerShell la documentation.	AWS général

Configuration NLog

Tâche	Description	Compétences requises
Installez le NuGet package.	1. Dans Visual Studio, choisissez Fichier, puis sélectionnez Ouvrir un projet ou une solution. 2. Choisissez le projet dans lequel vous souhaitez effectuer l'installation NLog. 3. Dans Visual Studio, choisissez Outils, Gestionnaire de NuGet packages, Console du gestionnaire de packages. 4. Installez le `AWS.Logger.NLog` NuGet package en saisissant la commande suivante. `Install-Package AWS.Logger.NLog -Version 3.1.0`	Développeur d'applications
Configurez la cible de journalisation.	1. Ouvrez le fichier `NLog.config` . 2. Pour la cible`type`, entrez`AWSTarget` . 3. Pour la cible`logGroup`, entrez le nom du groupe de journaux que vous souhaitez utiliser. Si le groupe de journaux n'existe pas déjà, un nouveau groupe de journaux portant	Développeur d'applications

Tâche	Description	Compétences requises
	le nom fourni est automatiq uement créé. 4. Pour la cible`region`, entrez la région AWS dans laquelle CloudWatch Logs est configuré. 5. Pour la cible`profile`, entrez le nom du profil que vous avez créé précédemm ent pour stocker la clé d'accès et la clé secrète. 6. Enregistrez et fermez le fichier `NLog.config` . Pour un exemple de fichier de configuration, consultez la section Informations supplémentaires de ce modèle. Lorsque vous exécutez votre application, elle écrit NLog les messages du journal et les envoie à CloudWatch Logs.	

Valider et surveiller les journaux

Tâche	Description	Compétences requises
Validez la journalisation.	Suivez les instructions de la section Afficher les données de journal envoyées à CloudWatch Logs dans la documentation CloudWatc	AWS général

Tâche	Description	Compétences requises
	h Logs. Vérifiez que les événements du journal sont enregistrés pour l'applica tion .NET. Si les événement s du journal ne sont pas enregistrés, consultez la section Dépannage de ce modèle.	
Surveillez la pile d'applica tions .NET.	Configurez la surveillance CloudWatch selon les besoins de votre cas d'utilisation. Vous pouvez utiliser CloudWatch Logs Insights, CloudWatch Metrics Insights et CloudWatc h Application Insights pour surveiller votre charge de travail .NET. Vous pouvez également configurer des alarmes afin de recevoir des alertes, et vous pouvez créer un tableau de bord personnal isé pour surveiller la charge de travail à partir d'une vue unique.	AWS général

Résolution des problèmes

Problème	Solution
Les données du journal n'apparaissent pas dans CloudWatch les journaux.	Assurez-vous que la politique IAM est attachée au rôle IAM assumé par CloudWatch Logs. Pour obtenir des instructions, consultez la

Problème	Solution
	section Configurer l'accès et les outils dans la section Epics.

Ressources connexes

- Utilisation de groupes de journaux et de flux de CloudWatch journaux (documentation sur les journaux)
- Amazon CloudWatch Logs et frameworks de journalisation .NET (article de blog AWS)

Informations supplémentaires

Voici un exemple de `NLog.config` fichier.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <section name="nlog" type="NLog.Config.ConfigSectionHandler, NLog" />
  </configSections>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.7.2" />
  </startup>
  <nlog>
    <extensions>
      <add assembly="NLog.AWS.Logger" />
    </extensions>
    <targets>
      <target name="aws" type="AWSTarget" logGroup="NLog.TestGroup" region="us-east-1"
 profile="demo"/>
    </targets>
    <rules>
      <logger name="*" minlevel="Info" writeTo="aws" />
    </rules>
  </nlog>
</configuration>
```

Copiez les produits AWS Service Catalog sur différents comptes AWS et régions AWS

Créée par Sachin Vighe (AWS) et Santosh Kale (AWS)

Récapitulatif

AWS Service Catalog est un service régional, ce qui signifie que les portefeuilles et les produits AWS Service Catalog ne sont visibles que dans la région AWS où ils ont été créés. Si vous configurez un hub AWS Service Catalog dans une nouvelle région, vous devez recréer vos produits existants, ce qui peut prendre beaucoup de temps.

L'approche de ce modèle permet de simplifier ce processus en décrivant comment copier des produits depuis un hub AWS Service Catalog dans un compte ou une région AWS source vers un nouveau hub dans un compte ou une région de destination. Pour plus d'informations sur le hub et le modèle en étoile AWS Service Catalog, consultez AWS Service Catalog hub and spoke model : How to automate the deployment and management of AWS Service Catalog to many accounts sur le blog AWS Management and Governance.

Le modèle fournit également les packages de code distincts nécessaires pour copier les produits AWS Service Catalog entre comptes ou vers d'autres régions. En utilisant ce modèle, votre organisation peut gagner du temps, rendre les versions de produits existantes et précédentes disponibles dans un nouveau hub AWS Service Catalog, minimiser le risque d'erreurs manuelles et étendre l'approche à plusieurs comptes ou régions.

> **Note**
>
> La section Epics de ce modèle propose deux options pour copier des produits. Vous pouvez utiliser l'option 1 pour copier des produits d'un compte à l'autre ou choisir l'option 2 pour copier des produits d'une région à l'autre.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Produits AWS Service Catalog existants dans un compte ou une région source.

- Un hub AWS Service Catalog existant dans un compte ou une région de destination.
- Si vous souhaitez copier des produits entre comptes, vous devez partager puis importer le portefeuille AWS Service Catalog contenant les produits dans votre compte de destination. Pour plus d'informations à ce sujet, consultez la section Partage et importation de portefeuilles dans la documentation AWS Service Catalog.

Limites

- Les produits AWS Service Catalog que vous souhaitez copier entre régions ou comptes ne peuvent pas appartenir à plusieurs portefeuilles.

Architecture

Le schéma suivant montre la copie des produits AWS Service Catalog d'un compte source vers un compte de destination.

Le schéma suivant montre la copie des produits AWS Service Catalog d'une région source vers une région de destination.

Pile technologique

- Amazon CloudWatch
- AWS Identity and Access Management (IAM)
- AWS Lambda
- AWS Service Catalog

Automatisation et mise à l'échelle

Vous pouvez adapter l'approche de ce modèle à l'aide d'une fonction Lambda qui peut être adaptée en fonction du nombre de demandes reçues ou du nombre de produits AWS Service Catalog que vous devez copier. Pour plus d'informations à ce sujet, consultez la section Dimensionnement des fonctions Lambda dans la documentation AWS Lambda.

Outils

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Service Catalog vous permet de gérer de manière centralisée les catalogues de services informatiques approuvés pour AWS. Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.

Code

Vous pouvez utiliser le `cross-account-copy` package (joint) pour copier les produits AWS Service Catalog entre les comptes ou le `cross-region-copy` package (joint) pour copier les produits entre les régions.

Le `cross-account-copy` package contient les fichiers suivants :

- `copyconf.properties`— Le fichier de configuration qui contient les paramètres de région et d'ID de compte AWS pour copier les produits entre les comptes.
- `scProductCopyLambda.py`— La fonction Python pour copier des produits entre comptes.
- `createDestAccountRole.sh`— Le script permettant de créer un rôle IAM dans le compte de destination.
- `createSrcAccountRole.sh`— Le script permettant de créer un rôle IAM dans le compte source.
- `copyProduct.sh`— Le script permettant de créer et d'invoquer la fonction Lambda pour copier des produits entre comptes.

Le `cross-region-copy` package contient les fichiers suivants :

- `copyconf.properties`— Le fichier de configuration qui contient les paramètres de région et d'ID de compte AWS pour copier des produits entre les régions.
- `scProductCopyLambda.py`— La fonction Python pour copier des produits entre les régions.
- `copyProduct.sh`— Le script permettant de créer un rôle IAM et de créer et d'invoquer la fonction Lambda pour copier des produits entre les régions.

Épopées

Option 1 — Copier les produits AWS Service Catalog entre les comptes

Tâche	Description	Compétences requises
Mettez à jour le fichier de configuration.	1. Téléchargez le `cross-account-copy` package (joint) sur votre ordinateur local. 2. Mettez à jour le fichier de `copyconf.properties` configuration avec les valeurs suivantes : • `srcRegion` — Indiquez la région source qui contient les produits. • `destRegion` — Indiquez la région de destination des produits. • `sourceAccountId` — Fournissez l'ID de compte AWS de votre compte source. • `destAccountId` — Fournissez l'ID de compte AWS de votre compte de destination.	Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises

Configurez vos informations d'identification pour l'AWS CLI dans le compte de destination.	Configurez vos informations d'identification pour accéder à l'AWS CLI dans votre compte de destination en exécutant la `aws configure` commande et en fournissant les valeurs suivantes :
	`$aws configure`
	`AWS Access Key ID`
	`[None]: <your_access_key_id>`
	`AWS Secret Access Key`
	`[None]: <your_secret_access_key>`
	`Default region name`
	`[None]: Region`
	`Default output format`
	`[None]:`
	Pour plus d'informations à ce sujet, consultez les principes de base de la configuration dans la documentation de l'interface de ligne de commande AWS.
		Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises

Configurez vos informations d'identification pour l'AWS CLI dans le compte source.	Configurez vos informations d'identification pour accéder à l'AWS CLI dans votre compte source en exécutant la `aws configure` commande et en fournissant les valeurs suivantes :
	`$aws configure`
	`AWS Access Key ID [None]: <your_access_key_id>`
	`AWS Secret Access Key [None]: <your_secret_access_key>`
	`Default region name [None]: Region`
	`Default output format [None]:`
	Pour plus d'informations à ce sujet, consultez les principes de base de la configuration dans la documentation de l'interface de ligne de commande AWS.
		Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
Créez un rôle d'exécution Lambda dans votre compte de destination.	Exécutez le `createDestAccountRole.sh` script dans votre compte de destination. Le script met en œuvre les actions suivantes : • Crée un rôle d'exécution Lambda dans votre compte de destination • Crée et attache la politique IAM pour le rôle d'exécution Lambda	Administrateur AWS, administrateur système AWS, administrateur cloud
Créez le rôle IAM entre comptes dans votre compte source.	Exécutez le `createSrcAccountRole.sh` script dans votre compte source. Le script met en œuvre les actions suivantes : • Crée un rôle IAM entre comptes dans votre compte source qui est assumé par le rôle d'exécution Lambda dans le compte de destination pour copier des produits • Crée et joint une politique IAM pour le rôle multicompte dans votre compte source	Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
Exécutez le script CopyProduct dans le compte de destination.	Exécutez le `copyProduct.sh` script dans votre compte de destination. Le script met en œuvre les actions suivantes : • Crée et invoque la fonction Lambda pour copier les produits du compte source vers le compte de destination	Administrateur AWS, administrateur système AWS, administrateur cloud

Option 2 — Copier les produits AWS Service Catalog d'une région source vers une région de destination

Tâche	Description	Compétences requises
Mettez à jour le fichier de configuration.	1. Téléchargez le `cross-region-copy` package (joint) sur votre ordinateur local. 2. Mettez à jour le fichier de `copyconf.properties` configuration avec les valeurs suivantes : • `srcRegion` — Indiquez la région source qui contient les produits. • `destRegion` — Indiquez la région de destination des produits. • `accountId` — Fournissez votre identifiant de compte AWS.	Administrateur système AWS, administrateur cloud, administrateur AWS

Tâche	Description	Compétences requises

Configurez vos informations d'identification pour l'AWS CLI.	Configurez vos informations d'identification pour accéder à l'AWS CLI dans votre environnement en exécutant la `aws configure` commande et en fournissant les valeurs suivantes :
	
	`$aws configure`
	`AWS Access Key ID`
	`[None]: <your_access_key_id>`
	`AWS Secret Access Key`
	`[None]: <your_secret_access_key>`
	`Default region name`
	`[None]: Region`
	`Default output format`
	`[None]:`
	
	Pour plus d'informations à ce sujet, consultez les principes de base de la configuration dans la documentation de l'interface de ligne de commande AWS.
		Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
Exécutez le script CopyProduct.	Exécutez le `copyProduct.sh` script dans votre région de destination. Le script met en œuvre les actions suivantes : • Crée un rôle d'exécution Lambda • Crée et attache la politique IAM pour le rôle d'exécution Lambda • Crée et invoque la fonction Lambda pour copier les produits de la région source vers la région de destination	Administrateur AWS, administrateur système AWS, administrateur cloud

Ressources connexes

- Création d'un rôle d'exécution Lambda (documentation AWS Lambda)
- Création d'une fonction Lambda (documentation AWS Lambda)
- Référence de l'API AWS Service Catalog
- Documentation d'AWS Service Catalog

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Création d'une matrice RACI ou RASCI pour un modèle d'exploitation cloud

Créé par Teddy Germade (AWS), Jérôme Descreux (AWS), Josselin LE MINEUR (AWS) et Florian Leroux (AWS)

Récapitulatif

Le Cloud Center of Excellence (CCoE) ou CEE (Cloud Enablement Engine) est une équipe autonome et responsable qui se concentre sur la préparation opérationnelle au cloud. Leur objectif principal est de faire passer l'organisation informatique d'un modèle d'exploitation sur site à un modèle d'exploitation dans le cloud. Le CCo E doit être une équipe interfonctionnelle comprenant des représentants de l'infrastructure, des applications, des opérations et de la sécurité.

L'un des composants clés d'un modèle d'exploitation cloud est une matrice RACI ou une matrice RASCI. Ceci est utilisé pour définir les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), support (S), consulté (C) et informé (I). Le type de support est facultatif. Si vous l'incluez, elle est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

En commençant par le modèle ci-joint, votre CCo équipe électronique peut créer une matrice RACI ou RASCI pour votre organisation. Le modèle contient les équipes, les rôles et les tâches courants dans les modèles d'exploitation cloud. Cette matrice repose sur les tâches liées à l'intégration des opérations et aux capacités CCo E. Cependant, vous pouvez personnaliser ce modèle pour répondre aux besoins de la structure et du cas d'utilisation de votre organisation.

Il n'y a aucune limite à la mise en œuvre d'une matrice RACI. Cette approche fonctionne pour les grandes organisations, les entreprises en démarrage et tout ce qui se trouve entre les deux. Pour les petites organisations, la même ressource peut remplir plusieurs rôles.

Épopées

Création de la matrice

Tâche	Description	Compétences requises
Identifiez les principales parties prenantes.	Identifiez les principaux responsables de service et d'équipe liés aux objectifs	Gestionnaire de projet

Tâche	Description	Compétences requises
	stratégiques de votre modèle d'exploitation cloud.	

Tâche	Description	Compétences requises

Personnalisez le modèle de matrice.	Téléchargez le modèle dans la section Pièces jointes, puis mettez à jour la matrice RACI ou RASCI comme suit :
	• Dans la feuille de travail Cloud Teams, mettez à jour les CCo noms des flux électroniques, les noms des équipes et les descripti ons des équipes selon les besoins de votre organisat ion.
	• Dans la feuille de travail Cloud Roles, mettez à jour les rôles, les noms des équipes et les descriptions des rôles selon les besoins de votre organisation.
	• Sur la feuille de travail RASCI, mettez à jour les éléments suivants selon les besoins de votre organisat ion :
	  • Dans la ligne 1 et la colonne A, mettez à jour les flux CCo E.
	  • Dans la ligne 2, mettez à jour les noms des équipes.
	  • Dans la ligne 3, mettez à jour les noms des rôles.
	  • Dans les colonnes D et E, mettez à jour les
		Gestionnaire de projet

Tâche	Description	Compétences requises
	champs généraux et les activités que vous souhaitez inclure dans votre graphique RASCI.	
Planifiez des réunions.	1. Communiquez les objectifs du RASCI à toutes les parties prenantes. 2. Planifiez une ou plusieurs réunions afin qu'un représentant habilité de chaque équipe puisse y assister.	Gestionnaire de projet

Tâche	Description	Compétences requises
Complétez la matrice.	Lors de la réunion avec toutes les parties prenantes, procédez comme suit : 1. Vérifiez qu'un représentant de chaque équipe est présent. La participation de l'équipe est obligatoire afin que vous puissiez attribuer avec précision les types de responsabilité pour chaque tâche. 2. Passez en revue ce qu'est une matrice RASCI et les objectifs avec les participants. 3. Passez en revue le modèle de responsabilité partagée avec les participants afin qu'ils comprennent l'étendue des responsabilités de leur organisation en matière de sécurité dans le cloud. 4. Sur la feuille de travail RASCI, pour chaque tâche ou activité, complétez les colonnes F à AN pour attribuer les types de responsabilité suivants : • Responsable (R) — Ce rôle est chargé d'effectuer le travail nécessaire à la réalisation de la tâche.	Gestionnaire de projet

Tâche	Description	Compétences requises
	• Responsable (A) — Ce rôle est tenu de s'assurer que la tâche est terminée. Ce rôle est également chargé de s'assurer que les conditions préalable s sont remplies et de déléguer la tâche aux responsables. • Support (S) — Ce rôle aide les responsables à accomplir la tâche. Ce type de responsabilité est facultatif et vous pouvez choisir de l'exclure afin de créer une matrice RACI plus traditionnelle. • Consulté (C) — Ce rôle doit être consulté pour obtenir des opinions ou une expertise sur la tâche. Selon la tâche, ce type de responsabilité peut ne pas être requis. • Informé (I) — Ce rôle doit être tenu au courant de l'avancement de la tâche et notifié lorsque la tâche est terminée. • Vide : ce rôle n'est pas impliqué dans l'activité ou la tâche.	

Tâche	Description	Compétences requises
Partagez la matrice RASCI.	Lorsque la matrice RACI ou RASCI est terminée, faites-la approuver par la direction . Enregistrez-le dans un référentiel partagé ou dans un emplacement central où toutes les parties prenantes peuvent y accéder. Nous vous recommandons d'utiliser des processus de contrôle des documents standard pour enregistrer et approuver les révisions de la matrice.	Gestionnaire de projet

Ressources connexes

- Modèle de responsabilité partagée AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez des alarmes pour des métriques personnalisées à l'aide de la détection des CloudWatch anomalies Amazon

Créée par Ram Kandaswamy (AWS) et Raheem Jiwani (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), vous pouvez utiliser Amazon CloudWatch pour créer des alarmes qui surveillent les métriques et envoient des notifications ou apportent automatiquement des modifications en cas de dépassement d'un seuil.

Pour éviter d'être limité par des seuils statiques, vous pouvez créer des alarmes basées sur des modèles antérieurs et qui vous avertissent si des mesures spécifiques se situent en dehors de la fenêtre de fonctionnement normale. Par exemple, vous pouvez surveiller les temps de réponse de votre API depuis Amazon API Gateway et recevoir des notifications concernant des anomalies qui vous empêchent de respecter un accord de niveau de service (SLA).

Ce modèle décrit comment utiliser la détection des CloudWatch anomalies pour les métriques personnalisées. Le modèle vous montre comment créer une métrique personnalisée dans Amazon CloudWatch Logs Insights ou publier une métrique personnalisée avec une fonction AWS Lambda, puis configurer la détection des anomalies et créer des notifications à l'aide d'Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Rubrique SNS existante, configurée pour envoyer des notifications par e-mail. Pour plus d'informations à ce sujet, consultez Getting started with Amazon SNS dans la documentation Amazon SNS.
- Une application existante, configurée avec CloudWatch Logs.

Limites

- CloudWatch les métriques ne prennent pas en charge les intervalles de quelques millisecondes. Pour plus d'informations sur la granularité des métriques régulières et personnalisées, consultez Amazon CloudWatch FAQs.

Architecture

Le schéma suivant illustre le flux de travail suivant :

1. Les journaux qui utilisent les métriques créées et mises à jour par CloudWatch Logs sont diffusés vers CloudWatch.
2. Une alarme se déclenche en fonction de seuils et envoie une alerte à un sujet SNS.
3. Amazon SNS vous envoie une notification par e-mail.

Pile technologique

- CloudWatch
- AWS Lambda
- Amazon SNS

Outils

- Amazon CloudWatch fournit une solution de surveillance fiable, évolutive et flexible.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs.
- Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages aux abonnés par les éditeurs.

Épopées

Configurer la détection des anomalies pour une métrique personnalisée

Tâche	Description	Compétences requises
Option 1 - Créez une métrique personnalisée à l'aide d'une fonction Lambda.	Téléchargez le `lambda_function.py` fichier (joint), puis remplacez le `lambda_function.py` fichier d'exemple dans le aws-lambda-developer-guideréférenti	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	el de la documentation AWS GitHub. Cela vous fournit un exemple de fonction Lambda qui envoie des métriques personnalisées à CloudWatch Logs. La fonction Lambda utilise l'API Boto3 pour s'intégrer à. CloudWatch Après avoir exécuté la fonction Lambda, vous pouvez vous connecter à l'AWS Management Console, ouvrir la CloudWatch console, et la métrique publiée est disponible dans votre espace de noms publié.	

Tâche	Description	Compétences requises
Option 2 — Créez des métriques personnalisées à partir de groupes de CloudWatch journaux.	Connectez-vous à l'AWS Management Console, ouvrez la CloudWatch console, puis choisissez Log groups. Choisissez le groupe de journaux pour lequel vous souhaitez créer une métrique. Choisissez Actions, puis sélectionnez Créer un filtre métrique. Dans Modèle de filtre, entrez le modèle de filtre que vous souhaitez utiliser. Pour plus d'informations, consultez la section Syntaxe des filtres et des modèles dans la CloudWatch documentation. Pour tester votre modèle de filtre, entrez un ou plusieurs événements de journal sous Modèle de test. Chaque événement de journal doit se trouver sur une seule ligne, car des sauts de ligne sont utilisés pour séparer les événements du journal dans la boîte Messages d'événements du journal. Après avoir testé le modèle, vous pouvez saisir un nom et une valeur pour votre métrique sous Détails de la métrique.	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	Pour plus d'informations et pour connaître les étapes à suivre pour créer une métrique personnalisée, consultez la section Création d'un filtre de métrique pour un groupe de logs dans la CloudWatch documentation.	

Tâche	Description	Compétences requises
Créez une alarme pour votre métrique personnalisée.	Sur la CloudWatch console, choisissez Alarmes, puis sélectionnez Créer une alarme. Choisissez Sélectionner une métrique et entrez le nom de la métrique que vous avez créée précédemment dans le champ de recherche. Choisissez l'onglet Graphed metrics et configurez les options en fonction de vos besoins. Sous Conditions, choisissez Détection des anomalies plutôt que Seuils statiques. Cela vous montre une bande basée sur deux écarts types par défaut. Vous pouvez définir des seuils et les ajuster en fonction de vos besoins. Choisissez Suivant. **Note** La bande est dynamique et dépend de la qualité des points de données. Lorsque vous commencez à agréger davantage de données, la bande et les seuils sont	DevOps ingénieur, AWS DevOps

Tâche	Description	Compétences requises
	automatiquement mis à jour.	
Configurez les notifications SNS.	Sous Notification, choisissez la rubrique SNS pour avertir lorsque l'alarme est en `ALARM` état, `OK` état ou `INSUFFICIENT_DATA` état. Pour que l'alerte envoie plusieurs notifications pour le même état d'alerte ou pour les différents états d'alerte, choisissez Add notification (Ajouter une notification). Choisissez Suivant. Saisissez un nom et une description pour l'alerte. Le nom ne doit contenir que des caractères ASCII. Ensuite, sélectionnez Suivant. Sous Aperçu et création, vérifiez que les informations et les conditions sont correctes , puis choisissez Créer une alarme.	DevOps ingénieur, AWS DevOps

Ressources connexes

- Publication de métriques personnalisées sur CloudWatch
- Utilisation de la détection des CloudWatch anomalies
- Événements d'alarme et Amazon EventBridge

- Quelles sont les meilleures pratiques à suivre pour transférer des indicateurs personnalisés vers Cloud Watch ? (vidéo)
- Présentation d' CloudWatch Application Insights (vidéo)
- Détectez les anomalies avec CloudWatch (vidéo)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Créez un IDE AWS Cloud9 qui utilise les volumes Amazon EBS avec un chiffrement par défaut

Créée par Janardhan Malyala (AWS) et Dhrubajyoti Mukherjee (AWS)

Récapitulatif

Remarque : n' AWS Cloud9 est plus disponible pour les nouveaux clients. Les clients existants de AWS Cloud9 peuvent continuer à utiliser le service normalement. En savoir plus

Vous pouvez utiliser le chiffrement par défaut pour appliquer le chiffrement de vos volumes Amazon Elastic Block Store (Amazon EBS) et de vos copies instantanées sur le cloud Amazon Web Services (AWS).

Vous pouvez créer un environnement de développement intégré (IDE) AWS Cloud9 qui utilise des volumes EBS chiffrés par défaut. Toutefois, le rôle lié au service AWS Identity and Access Management (IAM) pour AWS Cloud9 nécessite l'accès à la clé AWS Key Management Service (AWS KMS) pour ces volumes EBS. Si l'accès n'est pas fourni, l'IDE AWS Cloud9 risque de ne pas démarrer et le débogage peut s'avérer difficile.

Ce modèle indique les étapes à suivre pour ajouter le rôle lié au service pour AWS Cloud9 à la clé AWS KMS utilisée par vos volumes EBS. La configuration décrite par ce modèle vous aide à créer et à lancer avec succès un IDE qui utilise des volumes EBS avec chiffrement par défaut.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Le chiffrement par défaut est activé pour les volumes EBS. Pour plus d'informations sur le chiffrement par défaut, consultez le chiffrement Amazon EBS dans la documentation Amazon Elastic Compute Cloud (Amazon EC2).
- Une clé KMS existante gérée par le client pour chiffrer vos volumes EBS.

> **Note**
>
> Il n'est pas nécessaire de créer le rôle lié à un service pour AWS Cloud9. Lorsque vous créez un environnement de développement AWS Cloud9, AWS Cloud9 crée le rôle lié au service pour vous.

Architecture

Pile technologique

- AWS Cloud9
- IAM
- AWS KMS

Outils

- AWS Cloud9 est un environnement de développement intégré (IDE) qui vous aide à coder, créer, exécuter, tester et déboguer des logiciels. Il vous aide également à publier des logiciels sur le cloud AWS.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances Amazon Elastic Compute Cloud (Amazon). EC2
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.

Épopées

Trouvez la valeur de la clé de chiffrement par défaut

Tâche	Description	Compétences requises
Enregistrez la valeur de la clé de chiffrement par défaut pour les volumes EBS.	Connectez-vous à l'AWS Management Console et ouvrez la EC2 console Amazon. Choisissez le EC2 tableau de bord, puis sélection nez Protection et sécurité des données dans Attributs du compte. Dans la section Chiffrement EBS, copiez et enregistrez la valeur dans la clé de chiffrement par défaut.	Architecte cloud, DevOps ingénieur

Fournir un accès à la clé AWS KMS

Tâche	Description	Compétences requises
Fournissez à AWS Cloud9 l'accès à la clé KMS pour les volumes EBS.	1. Ouvrez la console AWS KMS, puis choisisse z Customer managed keys. Sélectionnez la clé AWS KMS utilisée pour le chiffrement Amazon EBS, puis choisissez View key. 2. Dans l'onglet Politique clé, vérifiez que vous pouvez voir le texte de la politique clé. Si vous ne pouvez pas voir le formulaire texte, choisissez Basculer en mode politique.	Architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	3. Choisissez Modifier. Ajoutez le code de la section Informations supplémentaires à la politique, puis choisissez Enregistrer les modifications. Les modifications de politique permettent au rôle lié au service pour AWS Cloud9 `AWSServiceRoleForAWSCloud9` d'accéder à la clé. Pour plus d'informations sur la mise à jour d'une politique clé, consultez Comment modifier une politique clé (documentation AWS KMS). ⚠ Important Le rôle lié à un service pour AWS Cloud9 est automatiquement créé lorsque vous lancez votre premier IDE. Pour plus d'informations, consultez la section Création d'un rôle lié à un service dans la documentation AWS Cloud9.	

Créez et lancez l'IDE

Tâche	Description	Compétences requises
Créez et lancez l'IDE AWS Cloud9.	Ouvrez la console AWS Cloud9 et choisissez Create environment. Configurez l'IDE en fonction de vos besoins en suivant les étapes décrites dans la section Création d'un EC2 environnement dans la documentation AWS Cloud9.	Architecte cloud, DevOps ingénieur

Ressources connexes

- Chiffrer les volumes EBS utilisés par AWS Cloud9
- Création d'un rôle lié à un service pour AWS Cloud9
- Création d'un EC2 environnement dans AWS Cloud9

Informations supplémentaires

Mises à jour des politiques clés d'AWS KMS

Remplacez <aws_accountid> par votre ID de compte AWS.

```
{
            "Sid": "Allow use of the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow attachment of persistent resources",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<aws_accountid>:role/aws-service-role/
cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        }
```

Utilisation d'une clé multicompte

Si vous souhaitez utiliser une clé KMS entre comptes, vous devez utiliser une autorisation en combinaison avec la politique de clé KMS. Cela permet d'accéder à la clé entre comptes. Dans le compte que vous avez utilisé pour créer l'environnement Cloud9, exécutez la commande suivante dans le terminal.

```
aws kms create-grant \
 --region <Region where Cloud9 environment is created> \
 --key-id <The cross-account KMS key ARN> \
 --grantee-principal arn:aws:iam::<The account where Cloud9 environment is
 created>:role/aws-service-role/cloud9.amazonaws.com/AWSServiceRoleForAWSCloud9 \
 --operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

Après avoir exécuté cette commande, vous pouvez créer des environnements Cloud9 en utilisant le chiffrement EBS avec une clé d'un autre compte.

Créez automatiquement des CloudWatch tableaux de bord Amazon basés sur des balises

Créée par Janak Vadaria (AWS), RAJNEESH TYAGI (AWS) et Vinodkumar Mandalapu (AWS)

Récapitulatif

La création manuelle de différents CloudWatch tableaux de bord Amazon peut prendre beaucoup de temps, en particulier lorsque vous devez créer et mettre à jour plusieurs ressources pour adapter automatiquement votre environnement. Une solution qui crée et met à jour automatiquement vos CloudWatch tableaux de bord peut vous faire gagner du temps. Ce modèle vous permet de déployer un AWS Cloud Development Kit (AWS CDK) pipeline entièrement automatisé qui crée et met à jour CloudWatch des tableaux de bord pour vos AWS ressources en fonction des événements de modification des balises, afin d'afficher les métriques Golden Signals.

Dans le domaine de l'ingénierie de fiabilité des sites (SRE), Golden Signals fait référence à un ensemble complet de mesures qui offrent une vue d'ensemble d'un service du point de vue de l'utilisateur ou du consommateur. Ces indicateurs incluent la latence, le trafic, les erreurs et la saturation. Pour plus d'informations, voir Qu'est-ce que l'ingénierie de fiabilité des sites (SRE) ? sur le AWS site Web.

La solution fournie par ce modèle est axée sur les événements. Une fois déployé, il surveille en permanence les événements de modification des balises et met automatiquement à jour les CloudWatch tableaux de bord et les alarmes.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- AWS Command Line Interface (AWS CLI), installé et configuré
- Prérequis pour la v2 AWS CDK
- Un environnement amorcé sur AWS
- Version 3 de Python
- AWS SDK pour Python (Boto3), installé
- Node.js version 18 ou ultérieure
- Gestionnaire de packages de nœuds (npm), installé et configuré pour le AWS CDK

- Connaissance modérée (niveau 200) du et AWS CDK AWS CodePipeline

Limites

Cette solution crée actuellement des tableaux de bord automatisés pour les services AWS suivants uniquement :

- Amazon Relational Database Service (Amazon RDS)
- AWS Auto Scaling
- Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB
- AWS Lambda

Architecture

Pile technologique cible

- CloudWatch tableaux de bord
- CloudWatch alarmes

Architecture cible

1. Un événement de modification de AWS balise pour les balises d'application configurées ou les modifications de code initie un pipeline AWS CodePipeline pour créer et déployer des CloudWatch tableaux de bord mis à jour.
2. AWS CodeBuild exécute un script Python pour rechercher les ressources dont les balises sont configurées et stocke la ressource IDs dans un fichier local dans un CodeBuild environnement.
3. CodeBuild exécute cdk synth pour générer des AWS CloudFormation modèles qui déploient des CloudWatch tableaux de bord et des alarmes.
4. CodePipeline déploie les AWS CloudFormation modèles dans la région spécifiée Compte AWS .
5. Lorsque la AWS CloudFormation pile a été déployée avec succès, vous pouvez consulter les CloudWatch tableaux de bord et les alarmes.

Automatisation et évolutivité

Cette solution a été automatisée à l'aide du AWS CDK. Vous pouvez trouver le code dans le CloudWatch référentiel GitHub Golden Signals Dashboards sur Amazon. Pour une mise à l'échelle supplémentaire et pour créer des tableaux de bord personnalisés, vous pouvez configurer plusieurs clés et valeurs de balise.

Outils

Services Amazon

- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources, notamment des AWS Lambda fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres domaines. Comptes AWS
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Bonnes pratiques

Pour des raisons de sécurité, vous pouvez utiliser le chiffrement et l'authentification pour les référentiels sources qui se connectent à vos pipelines. Pour connaître les meilleures pratiques supplémentaires, consultez les CodePipeline meilleures pratiques et les cas d'utilisation dans la CodePipeline documentation.

Épopées

Configuration et déploiement de l'exemple d'application

Tâche	Description	Compétences requises
Configurez et déployez l'exemple d'application.	1. Clonez le référentiel GitHub d'exemples de code à l'aide de la commande : `git clone https://github.com/aws-samples/golden-signals-dashboards-sample-app` 2. Accédez au référentiel cloné sur votre ordinateur et ouvrez le `src/project-settings.ts` fichier avec l'éditeur de votre choix. 3. Modifiez la valeur `projectSettings` constante en fonction de vos balises de AWS ressources et des mappages d'applications. 4. Définissez les variables `AWS_ACCOUNT` `AWS_REGION` , et d'`GS_DASHBOARD_INSTANCE` environnement : • Réglez `AWS_ACCOUNT` sur le numéro de compte de votre AWS compte.	AWS DevOps

Tâche	Description	Compétences requises
	• Définissez `AWS_REGION` la région dans laquelle vous souhaitez déployer l'exemple d'application. • Définissez `GS_DASHBOARD_INSTANCE` sur `dev`, ou `testprod`, en fonction de votre environnement de développement. (Nous recommandons `test` la procédure de test décrite dans ce modèle.) 5. Configurez le AWS CLI avec vos AWS informations d'identification. Pour plus d'informations, consultez la section Définir et afficher les paramètres de configuration à l'aide de commandes dans la AWS CLI documentation. 6. Exécutez la commande suivante pour déployer l'exemple d'application de tableau de bord Golden Signals : `sh deploy.sh`	

Tâche	Description	Compétences requises
Créez automatiquement des tableaux de bord et des alarmes.	Après avoir déployé l'exemple d'application, vous pouvez créer toutes les ressource s prises en charge par cette solution avec les valeurs de balise attendues, ce qui créera automatiquement les tableaux de bord et les alarmes spécifiés. Pour tester cette solution, créez une AWS Lambda fonction : 1. Connectez-vous à l' AWS Management Console Région AWS endroit où vous avez déployé l'exemple d'application. 2. Ouvrez la console Lambda à l'adresse. https://c onsole.aws.amazon.com/ lambda/ 3. Choisissez Créer une fonction, puis entrez un nom de fonction. 4. Dans le volet des paramètre s avancés, sélectionnez Activer les balises, puis choisissez Ajouter une nouvelle balise. Entrez la clé et la valeur suivantes : • Clé : `AutoDashboard` • Valeur : `True`	AWS DevOps

Tâche	Description	Compétences requises
	5. Choisissez Créer une fonction. La fonction Lambda démarre immédiatement un pipeline de code, qui crée automatiquement les tableaux de bord et les alarmes pour cette fonction Lambda en particulier. 6. Pour consulter les tableaux de bord automatisés et les alarmes, ouvrez la CloudWatch console à https://console.aws.amazon.com/cloudwatch/l'adresse. Vous pouvez consulter les tableaux de bord personnalisés et les alarmes pour la fonction que vous avez spécifiée dans la `projectSettings` constante (APP1-lambda par défaut). 7. Sélectionnez le tableau de bord de la fonction Lambda pour afficher les tableaux de bord automatisés supplémentaires créés dans le cadre de cette solution. 8. Répétez ces étapes pour les autres services, tels	

Tâche	Description	Compétences requises
	qu'Amazon RDS, Amazon SNS et DynamoDB AWS Auto Scaling, afin de générer les tableaux de bord associés. Pour un exemple pour Amazon RDS, consultez la section Informations supplémentaires.	

Supprimer l'exemple d'application

Tâche	Description	Compétences requises
Retirez la `golden-signals-dashboard` construction.	1. Pour supprimer toutes les AWS CloudFormation piles créées par l'exemple d'application, vous devez reconfigurer les variables d'`GS_DASHBOARD_INSTANCE` environnement `AWS_ACCOUNT` `AWS_REGION` , et. La `destroy.sh` commande nécessite ces configurations. • `AWS_ACCOUNT` est l'identifiant de votre AWS compte. • `AWS_REGION` est la région dans laquelle vous avez déployé votre exemple d'application.	AWS DevOps

Tâche	Description	Compétences requises
	• `GS_DASHBOARD_INSTANCE` est `devtest`, ou`prod`, en fonction de vos paramètres précédents. 2. Configurez AWS CLI avec vos AWS informations d'identification. 3. Exécutez la commande suivante pour supprimer l'exemple d'application et toutes les AWS CloudFormation piles associées : `sh destroy.sh`	

Résolution des problèmes

Problème	Solution
Commande Python introuvable (référence à `findresources.sh` la ligne 8).	Vérifiez la version de votre installation Python. Si vous avez installé la version 3 de Python, `python` `python3` remplacez-la par la ligne 8 du `resources.sh` fichier, puis réexécutez la `sh deploy.sh` commande pour déployer la solution.

Ressources connexes

- Bootstrapping (documentation)AWS CDK
- Utilisation de profils nommés (AWS CLI documentation)
- AWS CDK Atelier

Informations supplémentaires

L'illustration suivante montre un exemple de tableau de bord pour Amazon RDS créé dans le cadre de cette solution.

Documentez la conception de votre zone de landing zone AWS

Créée par Michael Daehnert (AWS), Florian Langer (AWS) et Michael Lodemann (AWS)

Récapitulatif

Une zone d'atterrissage est un environnement multi-comptes bien conçu, basé sur les meilleures pratiques en matière de sécurité et de conformité. Il s'agit du conteneur à l'échelle de l'entreprise qui contient toutes vos unités organisationnelles (OUs) Comptes AWS, vos utilisateurs et vos autres ressources. Une zone d'atterrissage peut être adaptée aux besoins d'une entreprise de toute taille. AWS propose deux options pour créer votre zone d'atterrissage : une zone d'atterrissage basée sur un service à l'aide AWS Control Towerou une zone d'atterrissage personnalisée que vous créez vous-même. Chaque option nécessite un niveau de AWS connaissance différent.

AWS créé AWS Control Tower pour vous aider à gagner du temps en automatisant la configuration d'une zone d'atterrissage. AWS Control Tower est géré par AWS et utilise les meilleures pratiques et directives pour vous aider à créer votre environnement de base. AWS Control Tower utilise des services intégrés, tels que AWS Service Cataloget AWS Organizations, pour approvisionner des comptes dans votre zone de landing zone et gérer l'accès à ces comptes.

AWS les projets de zone d'atterrissage varient en termes d'exigences, de détails de mise en œuvre et d'actions opérationnelles. Certains aspects de personnalisation doivent être pris en compte lors de chaque mise en œuvre de zone d'atterrissage. Cela inclut (mais sans s'y limiter) la manière dont la gestion des accès est gérée, la pile technologique utilisée et les exigences de surveillance pour l'excellence opérationnelle. Ce modèle fournit un modèle qui vous aide à documenter votre projet de zone d'atterrissage. En utilisant le modèle, vous pouvez documenter votre projet plus rapidement et aider vos équipes de développement et d'exploitation à comprendre votre zone de landing zone.

Conditions préalables et limitations

Limites

Ce modèle ne décrit pas ce qu'est une zone d'atterrissage ni comment l'implémenter. Pour plus d'informations sur ces sujets, consultez la section Ressources connexes.

Épopées

Création du document de conception

Tâche	Description	Compétences requises
Identifiez les principales parties prenantes.	Identifiez les principaux responsables de service et d'équipe liés à votre zone de landing zone.	Gestionnaire de projet
Personnalisez le modèle.	Téléchargez le modèle dans la section Pièces jointes, puis mettez-le à jour comme suit : 1. Supprimez toutes les sections qui ne s'appliqu ent pas à la zone de landing ou aux processus de votre organisation. 2. Ajoutez toutes les sections propres à votre organisat ion.	Gestionnaire de projet
Complétez le modèle.	Lors de réunions avec les parties prenantes ou en utilisant un write-and-review processus, complétez le modèle comme suit : 1. Utilisez les conseils et les informations figurant dans les cases bleues pour compléter chaque section. 2. Remplacez ou supprimez les champs jaunes par des valeurs personnalisées pour votre organisation.	Gestionnaire de projet

Tâche	Description	Compétences requises
	3. Remplacez ou supprimez tous les champs d'image par votre architecture personnalisée ou vos diagrammes de flux. 4. Complétez la section Historique des révisions et contributeurs du modèle.	
Partagez le document de conception.	Lorsque votre documentation de conception de zone d'atterrissage est terminée, enregistrez-la dans un référentiel partagé ou dans un emplacement central où toutes les parties prenantes peuvent y accéder. Nous vous recommandons d'utiliser des processus de contrôle des documents standard pour enregistrer et approuver les révisions du document de conception.	Gestionnaire de projet

Ressources connexes

- AWS Control Tower documentation
  - Planifiez votre zone de AWS Control Tower landing
  - AWS stratégie multi-comptes pour votre zone de AWS Control Tower landing zone
  - Conseils administratifs pour la configuration de la zone d'atterrissage
  - Attentes relatives à la configuration de la zone d'atterrissage
- Personnalisations pour AWS Control Tower (bibliothèque de AWS solutions)

- Configuration d'un AWS environnement multi-comptes sécurisé et évolutif (directivesAWS prescriptives)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Améliorez les performances opérationnelles en activant Amazon DevOps Guru dans plusieurs régions AWS, sur plusieurs comptes et OUs avec le kit AWS CDK

Créée par le Dr Rahul Sharad Gaikwad (AWS)

Récapitulatif

Ce modèle décrit les étapes à suivre pour activer le service Amazon DevOps Guru dans plusieurs régions, comptes et unités organisationnelles Amazon Web Services (AWSOUs) à l'aide du kit de développement AWS Cloud (AWS CDK) dans TypeScript. Vous pouvez utiliser les piles AWS CDK pour déployer AWS CloudFormation StackSets depuis le compte AWS de l'administrateur (principal) afin d'activer Amazon DevOps Guru sur plusieurs comptes, au lieu de vous connecter à chaque compte et d'activer DevOps Guru individuellement pour chaque compte.

Amazon DevOps Guru fournit des fonctionnalités d'intelligence artificielle (AIOps) pour vous aider à améliorer la disponibilité de vos applications et à résoudre les problèmes opérationnels plus rapidement. DevOps Guru réduit vos efforts manuels en appliquant des recommandations basées sur l'apprentissage automatique (ML), sans aucune expertise en ML. DevOps Guru analyse vos ressources et vos données opérationnelles. S'il détecte des anomalies, il fournit des mesures, des événements et des recommandations pour vous aider à résoudre le problème.

Ce modèle décrit trois options de déploiement pour activer Amazon DevOps Guru :

- Pour toutes les ressources cumulées sur plusieurs comptes et régions
- Pour toutes les ressources empilées OUs
- Pour des ressources de stockage spécifiques sur plusieurs comptes et régions

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée. (Voir Installation, mise à jour et désinstallation de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS.)

- AWS CDK Toolkit, installé et configuré. (Voir le kit d'outils AWS CDK dans la documentation AWS CDK.)
- Node Package Manager (npm), installé et configuré pour le AWS CDK dans. TypeScript (Voir Téléchargement et installation de Node.js et de npm dans la documentation de npm.)
- Python3 installé et configuré, pour exécuter un script Python afin d'injecter du trafic dans l'exemple d'application sans serveur. (Voir Configuration et utilisation de Python dans la documentation Python.)
- Pip, installé et configuré pour installer la bibliothèque de requêtes Python. (Voir les instructions d'installation de pip sur le PyPI site Web.)

Versions du produit

- AWS CDK Toolkit version 1.107.0 ou ultérieure
- npm version 7.9.0 ou ultérieure
- Node.js version 15.3.0 ou ultérieure

Architecture

Technologies

L'architecture de ce modèle inclut les services suivants :

- Amazon DevOps Guru
- AWS CloudFormation
- Amazon API Gateway
- AWS Lambda
- Amazon DynamoDB
- Amazon CloudWatch
- AWS CloudTrail

Piles de kits de développement AWS

Le modèle utilise les piles AWS CDK suivantes :

- `CdkStackSetAdminRole`— Crée un rôle d'administrateur AWS Identity and Access Management (IAM) afin d'établir une relation de confiance entre l'administrateur et les comptes cibles.
- `CdkStackSetExecRole`— Crée un rôle IAM pour faire confiance au compte administrateur.
- `CdkDevopsGuruStackMultiAccReg`— Active DevOps Guru dans plusieurs régions et comptes AWS pour toutes les piles, et configure les notifications Amazon Simple Notification Service (Amazon SNS).
- `CdkDevopsGuruStackMultiAccRegSpecStacks`— Active DevOps Guru dans plusieurs régions AWS et compte pour des stacks spécifiques, et configure les notifications Amazon SNS.
- `CdkDevopsguruStackOrgUnit`— Permet à DevOps Guru de OUs passer et de configurer les notifications Amazon SNS.
- `CdkInfrastructureStack`— Déploie des exemples de composants d'application sans serveur tels que API Gateway, Lambda et DynamoDB dans le compte administrateur pour démontrer l'injection de défauts et la génération d'informations.

Exemple d'architecture d'application

Le schéma suivant illustre l'architecture d'un exemple d'application sans serveur qui a été déployée sur plusieurs comptes et régions. Le modèle utilise le compte administrateur pour déployer toutes les piles AWS CDK. Il utilise également le compte administrateur comme l'un des comptes cibles pour configurer DevOps Guru.

1. Lorsque DevOps Guru est activé, il définit d'abord le comportement de chaque ressource comme base de référence, puis ingère les données opérationnelles issues des métriques vendues CloudWatch .
2. S'il détecte une anomalie, il la met en corrélation avec les événements qui en découlent CloudTrail et génère un aperçu.
3. Les informations fournissent une séquence d'événements corrélée ainsi que des recommandations prescrites pour permettre à l'opérateur d'identifier la ressource responsable.
4. Amazon SNS envoie des messages de notification à l'opérateur.

Automatisation et mise à l'échelle

Le GitHub référentiel fourni avec ce modèle utilise le AWS CDK comme outil d'infrastructure en tant que code (IAc) pour créer la configuration de cette architecture. AWS CDK vous aide à orchestrer les ressources et à activer DevOps Guru sur plusieurs comptes AWS, régions et. OUs

Outils

Services AWS

- AWS CDK — AWS Cloud Development Kit (AWS CDK) vous aide à définir votre infrastructure cloud sous forme de code dans l'un des cinq langages de programmation pris en charge : JavaScript Python TypeScript, Java et C#.
- AWS CLI — AWS Command Line Interface (AWS CLI) est un outil unifié qui fournit une interface de ligne de commande cohérente pour interagir avec les services et ressources AWS.

Code

Le code source de ce modèle est disponible sur GitHub, dans le référentiel Amazon DevOps Guru CDK Samples. Le code AWS CDK est écrit dedans. TypeScript Pour cloner et utiliser le référentiel, suivez les instructions de la section suivante.

> **Important**
>
> Certains des articles de ce modèle incluent des exemples de commandes AWS CDK et AWS CLI formatés pour Unix, Linux et macOS. Pour Windows, remplacez le caractère de continuation de la barre oblique inverse (\) à la fin de chaque ligne par un curseur (^).

Épopées

Préparer les ressources AWS pour le déploiement

Tâche	Description	Compétences requises
Configurez les profils nommés AWS.	Configurez vos profils nommés AWS comme suit pour déployer des stacks dans un environnement multi-com ptes.	DevOps ingénieur

Tâche	Description	Compétences requises

	Pour le compte administrateur :
	
	`$aws configure --profile administrator`
	`AWS Access Key ID [****]: <your-administrator-access-key-ID>`
	`AWS Secret Access Key [****]: <your-administrator-secret-access-key>`
	`Default region name [None]: <your-administrator-region>`
	`Default output format [None]: json`
	
	Pour le compte cible :
	
	`$aws configure --profile target`
	`AWS Access Key ID [****: <your-target-access-key-ID>`
	`AWS Secret Access Key [****]: <your-target-secret-access-key>`
	`Default region name [None]: <your-target-region>`
	`Default output format [None]: json`
	
	Pour plus d'informations, consultez la section Utilisation de profils nommés dans la documentation de l'AWS CLI.	

Tâche	Description	Compétences requises
Vérifiez les configurations des profils AWS.	(Facultatif) Vous pouvez vérifier les configurations de votre profil AWS dans les `config` fichiers `credentials` et en suivant les instructions de la section Définir et afficher les paramètres de configuration dans la documentation de l'AWS CLI.	DevOps ingénieur
Vérifiez la version du kit AWS CDK.	Vérifiez la version du kit d'outils AWS CDK en exécutant la commande suivante : `$cdk --version` Ce modèle nécessite la version 1.107.0 ou ultérieure. Si vous disposez d'une version antérieure du CDK AWS, suivez les instructions de la documentation du CDK AWS pour la mettre à jour.	DevOps ingénieur
Clonez le code du projet.	Clonez le GitHub référentiel pour ce modèle à l'aide de la commande : `$git clone https://github.com/aws-samples/amazon-devopsguru-cdk-samples.git`	DevOps ingénieur

Tâche	Description	Compétences requises

Installez les dépendances du package et compilez les TypeScript fichiers.	Installez les dépendances du package et compilez les TypeScript fichiers en exécutant les commandes suivantes :
	`$cd amazon-devopsguru-cdk-samples`
	`$npm install`
	`$npm fund`
	Ces commandes installent tous les packages du référentiel d'échantillons.
	Important
	Si vous recevez des erreurs concernant des packages manquants, utilisez l'une des commandes suivantes :
	`$npm ci`
	—ou—
	`$npm install -g @aws-cdk/<package-name>`
	Vous trouverez la liste des noms et des versions des packages dans la Dependenc
		DevOps ingénieur

Tâche	Description	Compétences requises
	`ies` section du `/amazon-devopsguru-cdk-samples/package.json` fichier. Pour plus d'informations, consultez npm ci et npm install dans la documentation de npm.	

Créez (synthétisez) les piles AWS CDK

Tâche	Description	Compétences requises
Configurez une adresse e-mail pour les notifications Amazon SNS.	Suivez ces étapes pour fournir une adresse e-mail pour les notifications Amazon SNS : 1. Modifiez les fichiers `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-stack.ts` et `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-org-uni-stack.ts` . 2. Dans la `Subscription` section `DevOpsGuruTopic` , mettez à jour le `Endpoint` paramètre avec votre adresse e-mail. 3. Enregistrez et fermez les fichiers.	DevOps ingénieur

Tâche	Description	Compétences requises

Créez le code du projet.	Créez le code du projet et synthétisez les piles en exécutant la commande suivante :
	`npm run build && cdk synth`
	Vous devez voir des résultats similaires à ce qui suit :
	`$npm run build && cdk synth`
	`> cdk-devopsguru@0.1.0 build`
	`> tsc`
	`Successfully synthesized to ~/amazon-devopsguru-cdk-samples/cdk.out`
	`Supply a stack id (CdkDevopsGuruStackMultiAccReg,CdkDevopsGuruStackMultiAccRegSpecStacks, CdkDevopsguruStackOrgUnit, CdkInfrastructureStack, CdkStackSetAdminRole, CdkStackSetExecRole) to display its template.`
	Pour plus d'informations et pour connaître les étapes à suivre, consultez Votre première application AWS
		DevOps ingénieur

Tâche	Description	Compétences requises
	CDK dans la documentation AWS CDK.	

Répertoriez les piles de CDK AWS.	Exécutez la commande suivante pour répertorier toutes les piles AWS CDK :
	`$cdk list`
	La commande affiche la liste suivante :
	`CdkDevopsGuruStack`
	`MultiAccReg`
	`CdkDevopsGuruSt`
	`ackMultiAccRegSpec`
	`Stacks`
	`CdkDevopsguruStackOr`
	`gUnit`
	`CdkInfrastructureStac`
	`k`
	`CdkStackSetAdminRole`
	`CdkStackSetExecRole`
		DevOps ingénieur

Option 1 - Activez DevOps Guru pour toutes les ressources de pile sur plusieurs comptes

Tâche	Description	Compétences requises
Déployez les piles AWS CDK pour créer des rôles IAM.	Ce modèle utilise AWS CloudFormation StackSets pour effectuer des opérations de stack sur plusieurs comptes. Si vous créez votre premier stack set, vous devez créer les rôles IAM suivants pour obtenir les autorisations	DevOps ingénieur

Tâche	Description	Compétences requises
	requises configurées dans vos comptes AWS : • `AWSCloudFormationStackSetAdministrationRole` • `AWSCloudFormationStackSetExecutionRole` **Note** Les rôles doivent porter ces noms exacts. 1. Créez le `AWSCloudFormationStackSetAdministrationRole` rôle IAM dans le compte administrateur (principal) en exécutant la commande CLI suivante : `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Créez le `AWSCloudFormationStackSetExecutionRole` rôle IAM dans tous les comptes cibles sur lesquels vous souhaitez exécuter les	

Tâche	Description	Compétences requises

	instances de stack. Pour créer ce rôle, exécutez les commandes CLI suivantes :
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile administrator`
	
	`$cdk deploy CdkStackSetExecRole \`
	`  --parameters AdministratorAccountId=<administrator-account-ID> \`
	`  --profile target`
	
	Pour plus d'informations, consultez la section Accorder des autorisations autogérées dans la CloudFormation documentation AWS.	

Tâche	Description	Compétences requises
Déployez la pile AWS CDK pour activer DevOps Guru sur plusieurs comptes.	La `CdkDevopsGuruStack MultiAccReg` pile AWS CDK crée des ensembles de piles pour déployer des instances de pile sur plusieurs comptes et régions. Pour déployer la pile, exécutez la commande CLI suivante avec les paramètres spécifiés : `$cdk deploy CdkDevops GuruStackMultiAccReg \ --profile administr ator \ --parameters AdministratorAccou ntId=<administrator- account-ID> \ --parameters TargetAccountId=<t arget-account-ID> \ --parameters RegionIds="<region -1>,<region-2>"` Amazon DevOps Guru est actuellement disponible dans les régions AWS répertoriées dans la FAQ DevOps Guru.	DevOps ingénieur

Option 2 - Activez DevOps Guru pour toutes les ressources empilées OUs

Tâche	Description	Compétences requises
Extrayez l'OU IDs.	Sur la console AWS Organizations, identifiez IDs les unités organisationnelles dans lesquelles vous souhaitez activer DevOps Guru.	DevOps ingénieur
Activez les autorisations gérées par le service pour. OUs	Si vous utilisez AWS Organizations pour la gestion de votre compte, vous devez accorder des autorisations gérées par le service pour activer DevOps Guru. Au lieu de créer les rôles IAM manuellement, utilisez un accès sécurisé basé sur l'organisation et des rôles liés à un service (). SLRs	DevOps ingénieur
Déployez la pile AWS CDK pour permettre à DevOps Guru de passer à travers. OUs	La `CdkDevopsguruStack OrgUnit` pile AWS CDK permet d'étendre le service DevOps Guru. OUs Pour déployer la pile, exécutez la commande suivante avec les paramètres spécifiés : `$cdk deploy CdkDevops guruStackOrgUnit \ --profile administr ator \ --parameters RegionIds="<region -1>,<region-2>" \`	DevOps ingénieur

Tâche	Description	Compétences requises
	`--parameters OrganizationalUnitIds="<OU-1>,<OU-2>"`	

Option 3 - Activez DevOps Guru pour des ressources de pile spécifiques sur plusieurs comptes

Tâche	Description	Compétences requises
Déployez les piles AWS CDK pour créer des rôles IAM.	Si vous n'avez pas encore créé les rôles IAM requis indiqués dans la première option, faites-le d'abord : 1. Créez le `AWSCloudFormationStackSetAdministrationRole` rôle IAM dans le compte administrateur (principal) en exécutant la commande CLI suivante : `$cdk deploy CdkStackSetAdminRole --profile administrator` 2. Créez le `AWSCloudFormationStackSetExecutionRole` rôle IAM dans tous les comptes cibles sur lesquels vous souhaitez exécuter les instances de stack. Pour créer ce rôle, exécutez les commandes de la CLI :	DevOps ingénieur

Tâche	Description	Compétences requises

	``
	$cdk deploy CdkStackSetExecRole \
	  --parameters AdministratorAccountId=<administrator-account-ID> \
	  --profile administrator
	
	$cdk deploy CdkStackSetExecRole \
	  --parameters AdministratorAccountId=<administrator-account-ID> \
	  --profile target
	``
	
	Pour plus d'informations, consultez la section Accorder des autorisations autogérées dans la CloudFormation documentation AWS.	

Tâche	Description	Compétences requises
Supprimez les piles existantes.	Si vous avez déjà utilisé la première option pour activer DevOps Guru pour toutes les ressources de la pile, vous pouvez supprimer l'ancienne pile en utilisant la commande suivante : `$cdk destroy CdkDevopsGuruStackMultiAccReg --profile administrator` Vous pouvez également modifier le `RegionIds` paramètre lorsque vous redéployez la pile pour éviter une erreur Stacks already exist.	DevOps ingénieur

Tâche	Description	Compétences requises
Mettez à jour la pile AWS CDK avec une liste de piles.	1. Modifiez le fichier `/amazon-devopsguru-cdk-samples/lib/cdk-devopsguru-multi-acc-reg-spec-stack.ts` . 2. Sous `Resources` ,`CloudFormation` ,`StackNames` ,, listez les piles pour lesquelles vous souhaitez activer DevOps Guru. À des fins de démonstration, le paramètre spécifie la `CdkInfrastructureStack` pile, mais vous pouvez modifier cette entrée en fonction de vos besoins. 3. Enregistrez et fermez le fichier . 4. Pour synthétiser et mettre à jour le modèle de pile, exécutez : `$cdk synth`	Ingénieur de données

Tâche	Description	Compétences requises
Déployez la pile AWS CDK pour permettre à DevOps Guru d'accéder à des ressources de pile spécifiques sur plusieurs comptes.	La `CdkDevopsGuruStack MultiAccRegSpecSta cks` pile AWS CDK permet à DevOps Guru d'accéder à des ressources de pile spécifiques sur plusieurs comptes. Pour déployer la pile, exécutez la commande suivante : `$cdk deploy CdkDevops GuruStackMultiAccR egSpecStacks \ --profile administr ator \ --parameters AdministratorAccou ntId=<administrator- account-ID> \ --parameters TargetAccountId=<t arget-account-ID> \ --parameters RegionIds="<region -1>,<region-2>"` **Note** Si vous avez déjà déployé cette pile pour l'option 1, modifiez le `RegionIds` paramètre (en veillant à choisir parmi les régions disponibles) pour éviter une erreur Stacks already exist.	DevOps ingénieur

Déployez la pile d'infrastructure AWS CDK

Tâche	Description	Compétences requises
Déployez l'exemple de pile d'infrastructure sans serveur.	La `CdkInfrastructureStack` pile AWS CDK déploie des composants sans serveur tels qu'API Gateway, Lambda et une table DynamoDB pour illustrer les connaissances de Guru. DevOps Pour déployer la pile, exécutez la commande suivante : `$cdk deploy CdkInfrastructureStack --profile administrator`	DevOps ingénieur
Insérez des exemples d'enregistrements dans DynamoDB.	Exécutez la commande suivante pour remplir la table DynamoDB avec des exemples d'enregistrements. Indiquez le chemin correct pour le `populate-shops-dynamodb-table.json` script. `$aws dynamodb batch-write-item \ --request-items file://scripts/populate-shops-dynamodb-table.json \ --profile administrator` La commande affiche la sortie suivante :	DevOps ingénieur

Tâche	Description	Compétences requises

	<pre>{
	    "UnprocessedItems"
	: {}
	}</pre>	

Tâche	Description	Compétences requises

Vérifiez les enregistrements insérés dans DynamoDB.	Pour vérifier que la table DynamoDB inclut les exemples d'enregistrements du fichier, accédez à `populate-shops-dynamodb-table.json` l'URL de `ListRestApiEndpointMonitorOperator` l'API, qui est publiée en tant que sortie de la pile AWS CDK. Vous pouvez également trouver cette URL dans l'onglet Outputs de la CloudFormation console AWS pour la `CdkInfrastructureStack` pile. La sortie du AWS CDK ressemblerait à ce qui suit :
	
	`CdkInfrastructureStack.CreateRestApiMonitorOperatorEndpointD1D00045 = https://oure17c5vob.execute-api.<your-region>.amazonaws.com/prod/`
	
	`CdkInfrastructureStack.ListRestApiMonitorOperatorEndpointABBDB8D8 = https://cdff8icfrn4.execute-api.<your-region>.amazonaws.com/prod/`
		DevOps ingénieur

Tâche	Description	Compétences requises
Attendez que les ressources aient terminé la définition de base.	Cette pile sans serveur dispose de quelques ressources. Nous vous recommandons d'attendre 2 heures avant de passer aux étapes suivantes. Si vous avez déployé cette pile dans un environnement de production, l'établissement de la base de référence peut prendre jusqu'à 24 heures, en fonction du nombre de ressources que vous avez sélectionné pour surveiller dans DevOps Guru.	DevOps ingénieur

Générez des informations sur DevOps Guru

Tâche	Description	Compétences requises
Mettez à jour la pile d'infrast ructure AWS CDK.	Pour essayer DevOps Guru Insights, vous pouvez apporter des modifications de configura tion afin de reproduire un problème de fonctionnement typique. 1. Modifiez le fichier `/amazon-devopsguru-cdk-samples/lib/infrastructure-stack.ts` . 2. Dans `DDB Table` cette section, modifiez la capacité	DevOps ingénieur

Tâche	Description	Compétences requises

	de lecture de la table DynamoDB de 5 à 1.
	3. Enregistrez et fermez le fichier .
	4. Exécutez les commandes suivantes pour synthétiser et déployer la pile d'infrast ructure AWS CDK mise à jour :
	`$cdk synth`
	`$cdk deploy CdkInfras tructureStack -- profile administrator`	

Tâche	Description	Compétences requises
Injectez des requêtes HTTP sur l'API.	Injectez du trafic entrant sous forme de requêtes HTTP sur l'`ListRestApiMonitorOperatorEndpointxxxx` API : 1. Modifiez le script Python `/amazon-devopsguru-cdk-samples/scripts/sendAPIRequest.py` . 2. Mettez à jour la `url` variable avec le lien API pour`ListRestApiMonitorOperatorEndpointxxxx` . Vous pouvez trouver cette URL dans le résultat de la commande de déploiement d'AWS CDK ou sur la console AWS Cloudformation, dans l'onglet Sorties de la pile. 3. Enregistrez et fermez le fichier . 4. Exécutez le script Python à l'aide de la commande : `$python sendAPIRequest.py` 5. Assurez-vous d'obtenir un code de statut 200. 6. Vous devrez peut-être exécuter le script via	DevOps ingénieur

Tâche	Description	Compétences requises
	plusieurs terminaux (de préférence quatre) pour injecter du trafic à un débit élevé. 7. Une fois le script exécuté en boucle pendant environ 10 minutes, vous pouvez voir un aperçu du fonctionnement sur la console DevOps Guru.	
Passez en revue DevOps Guru Insights.	Dans des conditions standard, le tableau de bord DevOps Guru affiche zéro dans le compteur d'informations continues. S'il détecte une anomalie, il déclenche une alerte sous forme d'aperçu. Dans le volet de navigation, choisissez Insights pour voir les détails de l'anomalie, notamment une vue d'ensemble, des mesures agrégées, des événements pertinents et des recommandations. Pour plus d'informations sur l'examen des informations, consultez le billet de blog Obtenir des informations opérationnelles AIOps grâce à Amazon DevOps Guru.	DevOps ingénieur

Nettoyage

Tâche	Description	Compétences requises

Nettoyez et supprimez les ressources.	Après avoir suivi ce schéma, vous devez supprimer les ressources que vous avez créées pour éviter d'encourir des frais supplémentaires. Exécutez les commandes suivantes :
	`$cdk destroy CdkDevopsGuruStackMultiAccReg --profile administrator`
	`$cdk destroy CdkDevopsguruStackOrgUnit --profile administrator`
	`$cdk destroy CdkDevopsGuruStackMultiAccRegSpecStacks --profile administrator`
	`$cdk destroy CdkInfrastructureStack --profile administrator`
	`$cdk destroy CdkStackSetAdminRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile administrator`
	`$cdk destroy CdkStackSetExecRole --profile target`
		DevOps ingénieur

Ressources connexes

- Obtenir des informations opérationnelles AIOps grâce à Amazon DevOps Guru

- Configurez facilement Amazon DevOps Guru sur plusieurs comptes et régions à l'aide d'AWS CloudFormation StackSets
- DevOps Atelier Guru

Implémentez Account Factory for Terraform (AFT) en utilisant un pipeline bootstrap

Créée par Vinicius Elias (AWS) et Edgar Costa Filho (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

Ce modèle fournit une méthode simple et sécurisée pour déployer AWS Control Tower Account Factory for Terraform (AFT) à partir du compte de gestion de. AWS Organizations Le cœur de la solution est un AWS CloudFormation modèle qui automatise la configuration AFT en créant un pipeline Terraform, qui est structuré de manière à être facilement adaptable pour le déploiement initial ou les mises à jour ultérieures.

La sécurité et l'intégrité des données étant des priorités absolues AWS, le fichier d'état Terraform, qui est un composant essentiel permettant de suivre l'état de l'infrastructure et des configurations gérées, est stocké en toute sécurité dans un bucket Amazon Simple Storage Service (Amazon S3). Ce bucket est configuré avec plusieurs mesures de sécurité, notamment le chiffrement côté serveur et des politiques visant à bloquer l'accès public, afin de garantir que votre état Terraform est protégé contre les accès non autorisés et les violations de données.

Le compte de gestion orchestre et supervise l'ensemble de l'environnement, il constitue donc une ressource essentielle dans. AWS Control Tower Ce modèle suit les AWS meilleures pratiques et garantit que le processus de déploiement est non seulement efficace, mais également conforme aux normes de sécurité et de gouvernance, afin de proposer un moyen complet, sécurisé et efficace de déployer AFT dans votre AWS environnement.

Pour plus d'informations sur l'AFT, consultez la AWS Control Tower documentation.

Conditions préalables et limitations

Prérequis

- Un environnement AWS multi-comptes de base avec au minimum les comptes suivants : compte de gestion, compte Log Archive, compte d'audit et un compte supplémentaire pour la gestion de l'AFT.
- Un AWS Control Tower environnement établi. Le compte de gestion doit être correctement configuré, car le CloudFormation modèle y sera déployé.

- Les autorisations nécessaires dans le compte AWS de gestion. Vous aurez besoin d'autorisations suffisantes pour créer et gérer des ressources telles que les compartiments S3, AWS Lambda les fonctions, les rôles AWS Identity and Access Management (IAM) et AWS CodePipeline les projets.
- Connaissance de Terraform. Il est important de comprendre les concepts fondamentaux et le flux de travail de Terraform, car le déploiement implique la génération et la gestion de configurations Terraform.

Limites

- Tenez compte des quotas de AWS ressources de votre compte. Le déploiement peut créer plusieurs ressources et le fait de rencontrer des quotas de service peut entraver le processus de déploiement.
- Le modèle est conçu pour des versions spécifiques de Terraform et. Services AWS La mise à niveau ou la modification des versions peuvent nécessiter des modifications du modèle.
- Le modèle ne prend pas en charge les services de système de contrôle de version (VCS) autogérés tels que GitHub Enterprise.

Versions du produit

- Terraform version 1.6.6 ou ultérieure
- AFT version 1.11 ou ultérieure

Architecture

Pile technologique cible

- AWS CloudFormation
- AWS CodeBuild
- AWS CodeCommit
- AWS CodePipeline
- Amazon EventBridge
- IAM
- AWS Lambda
- Amazon S3

Architecture cible

Le schéma suivant illustre la mise en œuvre décrite dans ce modèle.

Le flux de travail comprend trois tâches principales : créer les ressources, générer le contenu et exécuter le pipeline.

Création des ressources

Le CloudFormation modèle fourni avec ce modèle crée et configure toutes les ressources requises, en fonction des paramètres que vous sélectionnez lorsque vous déployez le modèle. Le modèle crée au minimum les ressources suivantes :

- Un CodePipeline pipeline pour mettre en œuvre l'AFT
- Un compartiment S3 pour stocker le fichier d'état Terraform associé à l'implémentation AFT
- Deux CodeBuild projets pour implémenter le plan Terraform et appliquer des commandes à différentes étapes du pipeline
- Rôles CodeBuild et CodePipeline services IAM
- Un deuxième compartiment S3 pour stocker les artefacts d'exécution du pipeline

Selon le fournisseur VCS que vous sélectionnez (CodeCommit ou VCS externe), le modèle crée les ressources suivantes.

- Dans CodeCommit :
  - Un CodeCommit référentiel pour stocker le code bootstrap AFT Terraform
  - Une EventBridge règle pour capturer les modifications CodeCommit du référentiel sur la `main` branche
  - Un autre rôle IAM pour la règle EventBridge
- Pour tout autre fournisseur de VCS externe, tel que : GitHub
  - Une AWS CodeConnections connexion

En outre, lorsque vous sélectionnez CodeCommit comme fournisseur VCS, si vous définissez le `Generate AFT Files` paramètre sur`true`, le modèle crée les ressources supplémentaires suivantes pour générer le contenu :

- Un compartiment S3 pour stocker le contenu généré et à utiliser comme source du CodeCommit référentiel
- Une fonction Lambda pour traiter les paramètres donnés et générer le contenu approprié
- Une fonction IAM pour exécuter la fonction Lambda
- Une ressource CloudFormation personnalisée qui exécute la fonction Lambda lorsque le modèle est déployé

Génération du contenu

Pour générer les fichiers bootstrap AFT et leur contenu, la solution utilise une fonction Lambda et un compartiment S3. La fonction crée un dossier dans le compartiment, puis crée deux fichiers dans le dossier : `main.tf` et`backend.tf`. La fonction traite également les CloudFormation paramètres fournis et remplit ces fichiers avec du code prédéfini, en remplaçant les valeurs de paramètres respectives.

Pour consulter le code utilisé comme modèle pour générer les fichiers, consultez le GitHub référentiel de la solution. En gros, les fichiers sont générés comme suit.

main.tf

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory?
ref=<aft_version>"

  # Required variables
  ct_management_account_id  = "<ct_management_account_id>"
  log_archive_account_id    = "<log_archive_account_id>"
  audit_account_id          = "<audit_account_id>"
  aft_management_account_id = "<aft_management_account_id>"
  ct_home_region            = "<ct_home_region>"

  # Optional variables
  tf_backend_secondary_region = "<tf_backend_secondary_region>"
  aft_metrics_reporting       = "<false|true>"

  # AFT Feature flags
  aft_feature_cloudtrail_data_events      = "<false|true>"
  aft_feature_enterprise_support          = "<false|true>"
  aft_feature_delete_default_vpcs_enabled = "<false|true>"
```

```
  # Terraform variables
  terraform_version      = "<terraform_version>"
  terraform_distribution = "<terraform_distribution>"

  # VCS variables (if you have chosen an external VCS)
  vcs_provider                                = "<github|githubenterprise|gitlab|
gitlabselfmanaged|bitbucket>"
  account_request_repo_name                   = "<org-name>/aft-account-request"
  account_customizations_repo_name            = "<org-name>/aft-account-
customizations"
  account_provisioning_customizations_repo_name = "<org-name>/aft-account-provisioning-
customizations"
  global_customizations_repo_name             = "<org-name>/aft-global-
customizations"

}
```

backend.tf

```
terraform {
  backend "s3" {
    region = "<aft-main-region>"
    bucket = "<s3-bucket-name>"
    key    = "aft-setup.tfstate"
  }
}
```

Lors de la création du CodeCommit référentiel, si vous définissez le `Generate AFT Files` paramètre sur`true`, le modèle utilise le compartiment S3 contenant le contenu généré comme source de la `main` branche pour remplir automatiquement le référentiel.

Gestion du pipeline

Une fois les ressources créées et les fichiers bootstrap configurés, le pipeline s'exécute. La première étape (Source) récupère le code source depuis la branche principale du référentiel, et la deuxième étape (Build) exécute la commande Terraform plan et génère les résultats à examiner. Au cours de la troisième étape (Approbation), le pipeline attend une action manuelle pour approuver ou rejeter la dernière étape (Déploiement). À la dernière étape, le pipeline exécute la commande Terraform en utilisant le résultat de la `apply` commande Terraform `plan` précédente comme entrée. Enfin, un rôle entre comptes et les autorisations du compte de gestion sont utilisés pour créer les ressources AFT dans le compte de gestion AFT.

> **Note**
>
> Si vous sélectionnez un fournisseur VCS externe, vous devez autoriser la connexion à l'aide des informations d'identification de votre fournisseur VCS. Pour terminer la configuration, suivez les étapes décrites dans Mettre à jour une connexion en attente dans la documentation de la console AWS Developer Tools.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git sans avoir à gérer votre propre système de contrôle de source.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS CodeConnectionspermet aux AWS ressources et aux services CodePipeline, tels que la connexion à des référentiels de code externes, tels que GitHub.
- AWS Lambdaest un service informatique qui exécute votre code en réponse à des événements et gère automatiquement les ressources de calcul, fournissant ainsi un moyen rapide de créer une application moderne sans serveur pour la production.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) qui vous permet de créer, de modifier et de versionner une infrastructure de manière sûre et efficace. Cela inclut les composants de bas niveau tels que les instances de calcul, le stockage et le réseau, et les composants de haut niveau tels que les entrées DNS et les fonctionnalités SaaS.

- Python est un langage de programmation puissant et facile à apprendre. Il possède des structures de données de haut niveau efficaces et fournit une approche simple mais efficace de la programmation orientée objet.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel de pipeline GitHub AFT bootstrap.

Pour le référentiel AFT officiel, voir AWS Control Tower Account Factory for Terraform dans. GitHub

Bonnes pratiques

Lorsque vous déployez AFT à l'aide du CloudFormation modèle fourni, nous vous recommandons de suivre les meilleures pratiques pour garantir une mise en œuvre sûre, efficace et réussie. Les principales directives et recommandations pour la mise en œuvre et le fonctionnement de l'AFT sont les suivantes.

- Examen approfondi des paramètres : examinez attentivement et comprenez chaque paramètre du CloudFormation modèle. La configuration précise des paramètres est cruciale pour une configuration et un fonctionnement corrects de l'AFT.
- Mises à jour régulières du modèle : maintenez le modèle à jour avec les dernières AWS fonctionnalités et versions de Terraform. Les mises à jour régulières vous aident à tirer parti des nouvelles fonctionnalités et à garantir la sécurité.
- Gestion des versions : épinglez la version de votre module AFT et utilisez un déploiement AFT distinct pour les tests si possible.
- Champ d'application : utilisez AFT uniquement pour déployer des garde-fous et des personnalisations d'infrastructure. Ne l'utilisez pas pour déployer votre application.
- Linting et validation : Le pipeline AFT nécessite une configuration Terraform linted et validée. Exécutez lint, validez et testez avant de transférer la configuration vers les référentiels AFT.
- Modules Terraform : créez du code Terraform réutilisable sous forme de modules et spécifiez toujours les versions de Terraform et du AWS fournisseur correspondant aux exigences de votre organisation.

Épopées

Configuration et configuration de l' AWS environnement

Tâche	Description	Compétences requises
Préparez l' AWS Control Tower environnement.	Configurez et configurez AWS Control Tower dans votre AWS environnement pour garantir une gestion et une gouvernance centralisées pour votre Comptes AWS. Pour plus d'informations, consultez la section Mise en route AWS Control Tower dans la AWS Control Tower documentation.	Administrateur du cloud
Lancez le compte de gestion AFT.	Utilisez l' AWS Control Tower Account Factory pour lancer un nouveau compte Compte AWS qui vous servira de compte de gestion AFT. Pour plus d'informations, consultez la section Provisionner des comptes avec AWS Service Catalog Account Factory dans la AWS Control Tower documentation.	Administrateur du cloud

Déployer le CloudFormation modèle dans le compte de gestion

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle.	Dans cette épopée, vous déployez le CloudFormation modèle fourni avec cette solution pour configurer le	Administrateur du cloud

Tâche	Description	Compétences requises
	pipeline de démarrage AFT dans votre compte AWS de gestion. Le pipeline déploie la solution AFT dans le compte de gestion AFT que vous avez configuré dans l'épopée précédente. Étape 1 : ouvrir la AWS CloudFormation console • Connectez-vous à la AWS CloudFormation console AWS Management Console et ouvrez-la. Assurez-vous que vous opérez dans la bonne région AWS Control Tower principale. Étape 2 : créer une nouvelle pile 1. Choisissez de créer une nouvelle pile. 2. Sélectionnez l'option permettant de télécharger un fichier modèle, puis téléchargez le CloudFormation modèle fourni avec ce modèle. Étape 3 : configurer les paramètres de la pile	

Tâche	Description	Compétences requises
	• `VCS Provider`: Sélectionnez le fournisseur de système de contrôle de version (VCS) à utiliser. Vous pouvez sélectionner un VCS externe tel que GitHub, ou utiliser CodeCommit si votre compte est autorisé à utiliser le service. • `Repository Name` : Spécifiez le nom du référentiel pour stocker le module de démarrage AFT. Pour les fournisseurs VCS externes, utilisez le chemin complet, y compris le nom de l'organisation (par exemple,`my-github-org/my-repo`). • `Branch Name`: Spécifiez la branche du référentiel source. • `CodeBuild Docker Image`: Choisissez le fichier à utiliser comme image de base CodeBuild Docker. • Si vous configurez le fournisseur VCS sur une autre option que CodeCommit, passez à l'étape 8. Étape 4 : Décider de la génération du fichier	

Tâche	Description	Compétences requises

	• Si vous l'avez sélection né CodeCommit comme fournisseur VCS, vous pouvez utiliser le `Generate AFT Files` paramètre pour contrôler la génération des fichiers de déploiement AFT par défaut. Définissez ce paramètre sur :
	  • `true`pour créer et stocker automatiquement les fichiers de déploiement AFT dans le référentiel spécifié.
	  • `false`si vous souhaitez gérer manuellement la création du fichier ou si vous avez déjà les fichiers en place.
	• Si vous avez sélection né`false`, passez à l'étape 8 ; sinon, suivez d'abord les étapes 5 à 7.
	
	Étape 5 : Renseignez AWS Control Tower les informations du compte AFT
	
	• Si vous définissez le `Generate AFT Files` paramètre sur`true`, fournissez les informati ons suivantes AWS Control Tower ainsi que les	

Tâche	Description	Compétences requises
	informations spécifiques au compte AFT. • `Log Archive Account ID`: ID du compte Log Archive dans AWS Control Tower. • `Audit Account ID`: ID du compte d'audit dans AWS Control Tower. • `AFT Management Account ID`: L'identifiant du compte de gestion AFT que vous avez créé dans le premier épisode épique. • `AFT Main Regionet AFT Secondary Region` : Le principal et le secondaire Régions AWS pour le déploiement de l'AFT. Étape 6 : Configuration des options AFT • Configurez les rapports sur les métriques : • `AFT Enable Metrics Reporting` : Activez ou désactivez le reporting des métriques AFT. Pour plus d'informations, consultez la section Mesures opérationnelles	

Tâche	Description	Compétences requises

	dans la AWS Control Tower documentation.
	
	• Définissez les options des fonctionnalités AFT :
	  • `Enable AFT CloudTrail Data Events`: Activez CloudTrail les événement s de données dans tous les comptes gérés par AFT. Pour plus d'informa tions, consultez la section sur AWS CloudTrail les événements liés aux données dans la AWS Control Tower documenta tion.
	  • `Enable AFT Enterprise Support` : Activez le Support d'entreprise dans tous les comptes gérés par AFT. Pour plus d'informa tions, consultez le plan de support aux AWS entreprises dans la AWS Control Tower documenta tion.
	  • `Enable AFT Delete Default VPC`: Supprimez tout VPCs dans le compte de gestion AFT uniquement. Pour	

Tâche	Description	Compétences requises
	plus d'informations, consultez Supprimer le VPC AWS par défaut dans la AWS Control Tower documentation. Étape 7 : Spécifier les versions • `AFT Terraform Version`: Choisissez la version de Terraform à utiliser dans les pipelines AFT. • `AFT Version`: Définissez la version AFT pour le déploiement. Conservez le paramètre par défaut (`latest`) pour utiliser la version d'AFT la plus récente. Étape 8 : Réviser et créer la pile • Passez en revue tous les paramètres et réglages. Si tout est en ordre, procédez à la création de la pile. Étape 9 : Surveiller la création de la pile • AWS CloudFormation fournit et configure les	

Tâche	Description	Compétences requises
	ressources que vous avez définies. Surveillez le processus de création de la pile sur la CloudFormation console. Ce processus peut prendre plusieurs minutes. Étape 10 : vérifier le déploiement • Lorsque le statut de la pile indique CREATE_COMPLETE, vérifiez que toutes les ressources ont été correctement créées. • Dans la section Sorties, notez la `Terraform BackendBucketName` valeur.	

Renseignez et validez le référentiel et le pipeline de bootstrap AFT

Tâche	Description	Compétences requises
Option 1 : remplir le référentiel de bootstrap AFT pour un VCS externe.	Si vous configurez le fournisseur VCS sur un VCS externe (pas pour CodeCommit), procédez comme suit. (Facultatif) Après avoir déployé le CloudFormation modèle, vous pouvez renseigner ou valider le contenu dans le nouveau	Administrateur du cloud

Tâche	Description	Compétences requises
	référentiel de bootstrap AFT, et tester si le pipeline s'est correctement exécuté. Étape 1 : mise à jour de la connexion 1. Sur la CodePipeline console, dans le volet de navigation, choisissez Paramètres, Connexions. 2. Sélectionnez la `aft-vcs-connection` connexion. Il devrait être en `Pending` état. 3. Choisissez Mettre à jour la connexion en attente et suivez les instructions de la section Mettre à jour une connexion en attente dans la documentation de la console Developer Tools. 4. Lorsque le `Available` statut de la connexion est en cours, passez à l'étape suivante. Étape 2 : remplir le référentiel 1. Utilisez vos informations d'identification VCS externes pour cloner le référentiel que vous avez spécifié dans le modèle sur votre machine locale.	

Tâche	Description	Compétences requises
	Si vous avez conservé le nom par défaut, le dépôt est appeléaft-setup . 2. Dans le dépôt, créez un dossier appelé terraform contenant deux fichiers vides : backend.tf etmain.tf. 3. Ouvrez le backend.tf fichier et ajoutez cet extrait de code : `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` Dans le dossier : • Remplacez <aft-main-region> par la région AFT principale. Cela devrait correspondre à la région AWS Control Tower principale. • <s3-bucket-name>Remplacez-le par le nom du bucket principal Terraform. Vous pouvez le trouver dans le	

Tâche	Description	Compétences requises
	`TerraformBackendBucketName` résultat généré par le CloudFormation modèle que vous avez déployé précédemment. 4. Ouvrez le `main.tf` fichier et utilisez l'un des exemples disponibles dans le référentiel AFT pour déployer AFT. Par exemple, vous pouvez travailler avec votre fournisseur de VCS préféré (CodeCommit, GitHub, ou Bitbucket) ou personnaliser le VPC AFT. Pour plus d'options d'entrée AFT, consultez le fichier README dans le référentiel AFT. Étape 2 : valider et appliquer vos modifications • Après avoir créé et renseigné le dossier et les fichiers, confirmez vos modifications et téléchargez le code dans le référentiel. Le pipeline démarre automatiquement, passe par les étapes Source et Build, puis attend une action	

Tâche	Description	Compétences requises
	d'approbation avant l'étape Deploy.	

Tâche	Description	Compétences requises
Option 2 : remplir le référentiel de bootstrap AFT pour. CodeCommit	Si vous configurez le fournisseur VCS sur CodeCommit, procédez comme suit. (Facultatif) Après avoir déployé le CloudFormation modèle, vous pouvez renseigner ou valider le contenu dans le nouveau référentiel de bootstrap AFT, et tester si le pipeline s'est correctement exécuté. Si vous définissez le `Generate AFT Files` paramètre sur`true`, passez à l'histoire suivante (validation du pipeline). Étape 1 : remplir le référentiel 1. Ouvrez la AWS CodeCommit console et sélectionnez le dépôt nouvellement créé. Si vous avez conservé le nom par défaut, le nom du référentiel doit être`aft-setup` . 2. Clonez le dépôt sur votre machine locale à l'aide de SSH, HTTPS ou HTTPS (GRC), puis ouvrez-le dans un éditeur. 3. Créez un dossier appelé `terraform` et deux	Administrateur du cloud

Tâche	Description	Compétences requises
	fichiers vides à l'intérieur : `backend.tf` et `main.tf`. 4. Ouvrez le `backend.tf` fichier et ajoutez cet extrait de code : `terraform { backend "s3" { region = "<aft-main-region>" bucket = "<s3-bucket-name>" key = "aft-setup" } }` Dans le dossier : • Remplacez `<aft-main-region>` par la région AFT principale. Cela devrait correspondre à la région AWS Control Tower principale. • `<s3-bucket-name>`Remplacez-le par le nom du bucket principal Terraform. Vous pouvez le trouver dans le `TerraformBackendBucketName` résultat généré par le CloudFormation modèle que vous avez déployé précédemment.	

Tâche	Description	Compétences requises
	5. Ouvrez le `main.tf` fichier et utilisez l'un des exemples disponibles dans le référentiel AFT pour déployer AFT. Par exemple, vous pouvez travailler avec votre fournisseur de système de contrôle de version (VCS) préféré (CodeCommit, GitHub, ou Bitbucket) ou personnaliser le VPC AFT. Pour plus d'options d'entrée AFT, consultez le fichier README dans le référentiel AFT. Étape 2 : valider et appliquer vos modifications • Après avoir créé et renseigné le dossier et les fichiers, confirmez vos modifications et télécharg ez le code dans le référenti el. Le pipeline démarre automatiquement, passe par les étapes Source et Build, puis attend une action d'approbation avant l'étape Deploy.	

Tâche	Description	Compétences requises
Validez le pipeline d'amorçage AFT.	Étape 1 : Afficher le pipeline • Ouvrez la CodePipeline console et vérifiez si le `aft-bootstrap-pipeline` pipeline a bien démarré. Il doit exécuter un plan Terraform ou attendre une action d'approbation manuelle. Étape 2 : Approuver les résultats du plan Terraform • Vous pouvez consulter les résultats du plan Terraform en consultant les journaux d'exécution de la phase de construction, puis en approuvant ou en rejetant l'exécution lors de la phase d'approbation. Si vous l'approuvez, le pipeline commence à déployer les ressources AFT dans le compte de gestion AFT fourni. Étape 3 : attendre le déploiement • Attendez que le pipeline fonctionne correctement. Cela devrait prendre environ 30 minutes. Les défaillances	Administrateur du cloud

Tâche	Description	Compétences requises
	que vous pourriez rencontrer sont souvent dues aux quotas d'API. Dans ces cas, vous pouvez réexécuter le pipeline pour poursuivre le déploiement. Étape 4 : Vérifier les ressources créées • Accédez au compte de gestion de l'AFT et confirmez que les ressources ont été créées.	

Résolution des problèmes

Problème	Solution
La fonction Lambda personnalisée incluse dans le CloudFormation modèle échoue pendant le déploiement.	Consultez les CloudWatch journaux Amazon pour la fonction Lambda afin d'identifier l'erreur. Les journaux fournissent des informations détaillées et peuvent aider à identifier le problème spécifique. Vérifiez que la fonction Lambda dispose des autorisations nécessaires et que les variables d'environnement ont été correctement définies.
Vous rencontrez des échecs lors de la création ou de la gestion des ressources en raison d'autorisations inadéquates.	Passez en revue les rôles et les politiques IAM attachés à la fonction Lambda CodeBuild, ainsi qu'aux autres services impliqués dans le déploiement. Vérifiez qu'ils disposent des autorisations nécessaires. En cas de problème

Problème	Solution
	d'autorisation, ajustez les politiques IAM pour accorder l'accès requis.
Vous utilisez une version obsolète du CloudFormation modèle avec des versions plus récentes Services AWS ou des versions de Terraform.	Mettez régulièrement à jour le CloudForm ation modèle pour qu'il soit compatible avec les dernières versions AWS et avec Terraform . Consultez les notes de publication ou la documentation pour connaître les modifications ou les exigences spécifiques à la version.
Vous atteignez Service AWS les quotas lors du déploiement.	Avant de déployer le pipeline, vérifiez les Service AWS quotas pour les ressources telles que les compartiments S3, les rôles IAM et les fonctions Lambda. Demandez des augmentat ions si nécessaire. Pour plus d'informations, consultez les Service AWS quotas sur le AWS site Web.
Vous rencontrez des erreurs en raison de paramètres d'entrée incorrects dans le CloudFormation modèle.	Vérifiez que tous les paramètres d'entrée ne contiennent pas de fautes de frappe ou de valeurs incorrectes. Vérifiez que les identifiants des ressources, tels que les noms de compte IDs et de région, sont exacts.

Ressources connexes

Pour implémenter ce modèle avec succès, consultez les ressources suivantes. Ces ressources fournissent des informations et des conseils supplémentaires qui peuvent être inestimables pour configurer et gérer l'AFT en utilisant AWS CloudFormation.

AWSdocumentation :

- AWS Control Tower Le guide de l'utilisateur fournit des informations détaillées sur la configuration et la gestion AWS Control Tower.
- AWS CloudFormation la documentation fournit des informations sur les CloudFormation modèles, les piles et la gestion des ressources.

Politiques et meilleures pratiques en matière d'IAM :

- Les meilleures pratiques de sécurité dans le domaine de l'IAM expliquent comment sécuriser les AWS ressources à l'aide des rôles et des politiques IAM.

Terraform sur : AWS

- La documentation du AWS fournisseur Terraform fournit des informations complètes sur l'utilisation de Terraform avec. AWS

Service AWS quotas :

- Service AWS quotas fournit des informations sur la façon de consulter Service AWS les quotas et de demander des augmentations.

Gérez les produits AWS Service Catalog dans plusieurs comptes AWS et régions AWS

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Amazon Web Services (AWS) Service Catalog simplifie et accélère la gouvernance et la distribution des modèles d'infrastructure sous forme de code (IaC) pour les entreprises. Vous utilisez des CloudFormation modèles AWS pour définir un ensemble de ressources AWS (piles) requises pour un produit. AWS CloudFormation StackSets étend cette fonctionnalité en vous permettant de créer, de mettre à jour ou de supprimer des piles sur plusieurs comptes et régions AWS en une seule opération.

Les administrateurs d'AWS Service Catalog créent des produits à l'aide de CloudFormation modèles créés par des développeurs, puis les publient. Ces produits sont ensuite associés à un portefeuille, et des contraintes sont appliquées pour la gouvernance. Pour mettre vos produits à la disposition des utilisateurs d'autres comptes AWS ou unités organisationnelles (OUs), vous partagez généralement votre portefeuille avec eux. Ce modèle décrit une approche alternative pour gérer les offres de produits AWS Service Catalog basée sur AWS CloudFormation StackSets. Au lieu de partager des portefeuilles, vous utilisez des contraintes de stack pour définir les régions et les comptes AWS dans lesquels votre produit peut être déployé et utilisé. En utilisant cette approche, vous pouvez approvisionner vos produits AWS Service Catalog sur plusieurs comptes et régions AWS, et les gérer depuis un emplacement central, tout en respectant vos exigences de gouvernance. OUs

Les avantages de cette approche :

- Le produit est approvisionné et géré à partir du compte principal et n'est pas partagé avec d'autres comptes.
- Cette approche fournit une vue consolidée de tous les produits provisionnés (piles) basés sur un produit spécifique.
- La configuration avec AWS Service Management Connector est plus simple, car elle ne cible qu'un seul compte.
- Il est plus facile d'interroger et d'utiliser les produits d'AWS Service Catalog.

Conditions préalables et limitations

Prérequis

- CloudFormation Modèles AWS pour IaC et gestion des versions
- Configuration multi-comptes et AWS Service Catalog pour le provisionnement et la gestion des ressources AWS

Limites

- Cette approche utilise AWS CloudFormation StackSets, et ses limites StackSets s'appliquent :
  - StackSets ne prend pas en charge le déploiement de CloudFormation modèles via des macros. Si vous utilisez une macro pour prétraiter le modèle, vous ne pourrez pas utiliser un déploiement StackSets basé.
  - StackSets permet de dissocier une pile de l'ensemble de piles, afin que vous puissiez cibler une pile spécifique pour résoudre un problème. Cependant, une pile dissociée ne peut pas être réassociée à l'ensemble de piles.
- AWS Service Catalog génère automatiquement StackSet des noms. La personnalisation n'est actuellement pas prise en charge.

Architecture

Architecture cible

1. L'utilisateur crée un CloudFormation modèle AWS pour provisionner les ressources AWS, au format JSON ou YAML.
2. Le CloudFormation modèle crée un produit dans AWS Service Catalog, qui est ajouté à un portefeuille.
3. L'utilisateur crée un produit provisionné, qui crée des CloudFormation piles dans les comptes cibles.
4. Chaque pile fournit les ressources spécifiées dans les CloudFormation modèles.

Outils

Services AWS

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Service Catalog vous permet de gérer de manière centralisée les catalogues de services informatiques approuvés pour AWS. Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.

Épopées

Provisionner des produits sur plusieurs comptes

Tâche	Description	Compétences requises
Créez un portefeuille.	Un portefeuille est un conteneur qui inclut un ou plusieurs produits regroupés en fonction de critères spécifiques. L'utilisation d'un portefeuille pour vos produits vous permet d'appliquer des contraintes communes à l'ensemble de votre gamme de produits. Pour créer un portefeuille, suivez les instructions de la documentation AWS Service Catalog. Si vous utilisez l'AWS CLI, voici un exemple de commande : `aws servicecatalog create-portfolio --provider-name my-provid`	AWS Service Catalog, IAM

Tâche	Description	Compétences requises
	`er --display-name my-portfolio` Pour plus d'informations, consultez la documentation de l'AWS CLI.	
Créez un CloudFormation modèle.	Créez un CloudFormation modèle qui décrit les ressources. Les valeurs des propriétés des ressources doivent être paramétrées le cas échéant.	AWS CloudFormation, JSON/YAML

Tâche	Description	Compétences requises
Créez un produit avec des informations de version.	Le CloudFormation modèle devient un produit lorsque vous le publiez dans AWS Service Catalog. Fournissez des valeurs pour les paramètres de détail de version facultatifs, tels que le titre et la description de la version ; cela sera utile pour rechercher le produit ultérieurement. Pour créer un produit, suivez les instructions de la documentation AWS Service Catalog. Si vous utilisez l'AWS CLI, voici un exemple de commande : `aws servicecatalog create-product --cli-input-json file://create-product-input.json` où se `create-product-input.json` trouve le fichier qui transmet les paramètres du produit. Pour un exemple de ce fichier, consultez la section Informations supplémentaires. Pour plus d'informations, consultez la documentation de l'AWS CLI.	AWS Service Catalog

Tâche	Description	Compétences requises
Appliquez des contraintes.	Appliquez des contraintes d'ensemble au portefeuille afin de configurer les options de déploiement du produit, telles que plusieurs comptes AWS, régions et autorisations. Pour obtenir des instructions, consultez la documentation AWS Service Catalog.	AWS Service Catalog
Ajoutez à des autorisations .	Donnez des autorisations aux utilisateurs afin qu'ils puissent lancer les produits du portefeuille. Pour les instructi ons relatives à la console, consultez la documentation AWS Service Catalog. Si vous utilisez l'AWS CLI, voici un exemple de commande : `aws servicecatalog associate-principal-with-portfolio \ --portfolio-id port-2s6abcdefwdh4 \ --principal-arn arn:aws:iam::444455556666:role/Admin \ --principal-type IAM` Pour plus d'informations, consultez la documentation de l'AWS CLI.	AWS Service Catalog, IAM

Tâche	Description	Compétences requises
Fournissez le produit.	Un produit provisionné est une instance avec ressource s d'un produit. Le provision nement d'un produit basé sur un CloudFormation modèle lance une CloudFormation pile et ses ressources sous-jace ntes. Provisionnez le produit en ciblant les régions et les comptes AWS applicables, en fonction des contraintes liées au stack set. Dans l'AWS CLI, voici un exemple de commande : `aws servicecatalog provision-product \ --product-id prod-abcdfz3syn2rg \ --provisioning-artifact-id pa-abc347pcsccfm \ --provisioned-product-name "mytestppname3"` Pour plus d'informations, consultez la documentation de l'AWS CLI.	AWS Service Catalog

Ressources connexes

Références

- Présentation d'AWS Service Catalog
- Utilisation d'AWS CloudFormation StackSets

Tutoriels et vidéos

- AWS re:Invent 2019 : Automatisez tout : options et meilleures pratiques (vidéo)

Informations supplémentaires

Lorsque vous utilisez la `create-product` commande, le `cli-input-json` paramètre pointe vers un fichier qui spécifie des informations telles que le responsable du produit, l'e-mail d'assistance et les détails du CloudFormation modèle. Voici un exemple d'un tel fichier :

```
{
   "Owner": "Test admin",
      "SupportDescription": "Testing",
         "Name": "SNS",
            "SupportEmail": "example@example.com",
            "ProductType": "CLOUD_FORMATION_TEMPLATE",
               "AcceptLanguage": "en",
                  "ProvisioningArtifactParameters": {
                     "Description": "SNS product",
                        "DisableTemplateValidation": true,
                           "Info": {
                              "LoadTemplateFromURL": "<url>"
                     },
                           "Name": "version 1"
}
```

Migrer un compte de membre AWS depuis AWS Organizations vers AWS Control Tower

Créée par Rodolfo Jr. Cerrada (AWS)

Récapitulatif

Ce modèle décrit comment migrer un compte Amazon Web Services (AWS) d'AWS Organizations, où il s'agit d'un compte membre régi par un compte de gestion, vers AWS Control Tower. En inscrivant le compte dans AWS Control Tower, vous pouvez bénéficier de dispositifs de sécurité et de fonctionnalités de prévention et de détection qui rationalisent la gouvernance de votre compte. Vous souhaiterez peut-être également migrer votre compte membre si votre compte de gestion AWS Organizations a été compromis, et si vous souhaitez déplacer les comptes membres vers une nouvelle organisation régie par AWS Control Tower.

AWS Control Tower fournit une structure qui combine et intègre les fonctionnalités de plusieurs autres services AWS, notamment AWS Organizations, et garantit une conformité et une gouvernance cohérentes dans votre environnement multi-comptes. Avec AWS Control Tower, vous pouvez suivre un ensemble de règles et de définitions prescrites qui étendent les capacités d'AWS Organizations. Par exemple, vous pouvez utiliser des garde-fous pour vous assurer que les journaux de sécurité et les autorisations d'accès entre comptes nécessaires sont créés, et non modifiés.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Configuration d'AWS Control Tower dans votre organisation cible dans AWS Organizations (pour obtenir des instructions, consultez la section Configuration dans la documentation AWS Control Tower)
- Informations d'identification d'administrateur pour AWS Control Tower (membre du AWSControlTowerAdminsgroupe)
- Informations d'identification de l'administrateur pour le compte AWS source

Limites

- Le compte de gestion source dans AWS Organizations doit être différent du compte de gestion cible dans AWS Control Tower.

Versions du produit

- AWS Control Tower version 2.3 (février 2020) ou ultérieure (voir les notes de publication)

Architecture

Le schéma suivant illustre le processus de migration et l'architecture de référence. Ce modèle fait migrer le compte AWS de l'organisation source vers une organisation cible régie par AWS Control Tower.

Le processus d'inscription comprend les étapes suivantes :

1. Le compte quitte l'organisation source dans AWS Organizations.
2. Le compte devient un compte autonome. Cela signifie qu'il n'appartient à aucune organisation, de sorte que la gouvernance et la facturation sont gérées indépendamment par les administrateurs de compte.
3. L'organisation cible envoie une invitation pour que le compte rejoigne l'organisation.
4. Le compte autonome accepte l'invitation et devient membre de l'organisation cible.
5. Le compte est inscrit dans AWS Control Tower et transféré vers une unité organisationnelle (UO) enregistrée. (Nous vous recommandons de consulter le tableau de bord AWS Control Tower pour confirmer l'inscription.) À ce stade, tous les garde-corps activés dans l'unité d'organisation enregistrée prennent effet.

Outils

Services AWS

- AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs comptes AWS en une seule entité (une organisation) que vous créez et gérez de manière centralisée.
- AWS Control Tower intègre les fonctionnalités d'autres services, notamment AWS Organizations, AWS IAM Identity Center (successeur d'AWS Single Sign-On) et AWS Service Catalog, pour vous aider à appliquer et à gérer les règles de gouvernance relatives à la sécurité, aux opérations et à la conformité à grande échelle dans l'ensemble de vos organisations et comptes dans le cloud AWS.

Épopées

Supprimer le compte membre de l'organisation source

Tâche	Description	Compétences requises
Vérifiez que le compte du membre peut fonctionner en tant que compte autonome.	Vérifiez que le compte membre qui quittera l'organisation source contient les informations nécessaires pour fonctionner en tant que compte autonome. Par exemple, si le compte membre ne contient pas d'informations de facturation, il ne peut pas fonctionner comme un compte autonome, car AWS utilise les informations de paiement pour facturer toute activité AWS facturable qui se produit alors que le compte n'est pas rattaché à une organisation. Généralement, si vous avez créé le compte membre à l'aide de la console AWS Organizations, de l'API ou des commandes de l'interface de ligne de commande (CLI) AWS, les informations requises pour les comptes autonomes ne sont pas collectées automatiquement. Pour ajouter ces informations, connectez-vous au compte et spécifiez un plan d'assistance,	Administrateur du compte

Tâche	Description	Compétences requises
	des informations de contact et un mode de paiement. Pour plus d'informations sur ce que vous devez savoir avant de supprimer un compte d'une organisation, consultez la section Avant de supprimer un compte d'une organisation dans la documentation d'AWS Organizations.	

Tâche	Description	Compétences requises
Supprimez le compte membre de son organisation source.	Suivez les instructions de la documentation d'AWS Organizations pour supprimer un compte membre d'une organisation. Vous pouvez vous connecter au compte de gestion de l'organisation et supprimer le compte membre, ou vous connecter au compte membre et quitter l'organisation. Si vous ne disposez pas des informations d'identification de niveau administrateur pour supprimer ou quitter le compte, demandez de l'aide à l'administrateur de votre organisation. S'il manque un plan d'assistance, des coordonnées ou des informations de paiement sur le compte du membre, vous serez invité à fournir et à vérifier ces informations. Lorsque vous quittez l'organisation, vous êtes redirigé vers la page Getting Started de la console AWS Organizations, où vous pouvez consulter les invitations à rejoindre d'autres organisations pour votre compte.	Administrateur du compte de gestion ou administrateur du compte

Tâche	Description	Compétences requises
	Important À ce stade, votre compte est un compte autonome. Si vous exécutez des charges de travail qui ne sont pas couvertes par le niveau gratuit d'AWS, vous serez débité en fonction des informations de paiement et de facturation que vous avez fournies pour le compte.	
Vérifiez que le compte du membre ne fait plus partie de l'organisation source.	Dans la console AWS Organizations, vous ne devriez plus voir le bouton Quitter l'organisation. Au lieu de cela, vous devriez voir les invitations en attente, le cas échéant, provenant d'autres organisations.	Administrateur du compte

Tâche	Description	Compétences requises
Supprimez les rôles IAM qui accordent l'accès à votre compte à l'organisation que vous avez quittée.	Lorsque vous supprimez le compte de l'organisation source, les rôles AWS Identity and Access Managemen t (IAM) créés par AWS Organizations ou par des administrateurs ne sont pas automatiquement supprimés . Pour mettre fin à l'accès depuis le compte de gestion de l'organisation source, vous devez supprimer manuellem ent les rôles IAM. Pour plus d'informations, consultez la section Suppression de rôles ou de profils d'instance dans la documentation IAM. Lorsqu'un compte membre quitte une organisation, toutes les balises associées au compte sont supprimées. Les comptes autonomes ne prennent pas en charge les tags.	Administrateur du compte

Invitez le compte à rejoindre la nouvelle organisation avec AWS Control Tower

Tâche	Description	Compétences requises
Connectez-vous à AWS Control Tower.	Connectez-vous à la console AWS Control Tower en tant qu'administrateur.	Administrateur de la tour de contrôle AWS

Tâche	Description	Compétences requises
	À l'heure actuelle, il n'existe aucun moyen direct de déplacer un compte AWS d'une organisation source vers une organisation au sein d'une unité d'organisation régie par AWS Control Tower. Cependant, vous pouvez étendre la gouvernance d'AWS Control Tower à un compte AWS existant lorsque vous l'inscrivez dans une unité d'organisation déjà régie par AWS Control Tower. C'est pourquoi vous devez vous connecter à AWS Control Tower pour cette étape.	

Tâche	Description	Compétences requises
Invitez le compte du membre.	1. Connectez-vous à la console AWS Organizations et accédez à la page des comptes AWS. 2. Sur la page Ajouter un compte AWS, choisissez Inviter un compte AWS existant. 3. Complétez les informations du compte, y compris le numéro de compte à 12 chiffres (sans tirets) ainsi que la description et les tags facultatifs, puis choisissez Envoyer une invitation. **Important** Vérifiez qu'aucune application ou connexion réseau ne sera affectée par le transfert de compte. Cette action envoie un e-mail d'invitation contenant un lien vers le compte du membre. Lorsque l'administrateur du compte suit le lien et accepte l'invitation, le compte du membre apparaît sur la page des comptes AWS. Pour plus	Administrateur de la tour de contrôle AWS

Tâche	Description	Compétences requises
	d'informations, consultez la section Inviter un compte AWS à rejoindre votre organisation dans la documentation AWS Organizations.	

Tâche	Description	Compétences requises
Testez les applications et la connectivité.	Lorsque le compte du membre a été enregistré dans la nouvelle organisation, il apparaît dans l'unité d'organisation au sein d'une racine. Il apparaît également dans la console AWS Control Tower, marqué comme non inscrit dans les comptes, car il n'a pas encore été inscrit dans l'unité d'organisation enregistrée dans AWS Control Tower. Vérifiez les paramètres suivants : • Consultez le tableau de bord d'AWS Control Tower pour voir s'il y a des violations des garde-corps. • Vérifiez la connectivité réseau (VPN ou AWS Direct Connect) pour vous assurer qu'elle n'a pas été affectée par le transfert. • (Propriétaires de l'application) Testez les applications associées à ce compte pour vérifier qu'elles s'exécutent comme prévu et que les dépendances n'ont pas été affectées par le transfert de compte.	Administrateur AWS Control Tower, administrateur du compte membre, propriétaires de l'application

Préparez le compte pour l'inscription

Tâche	Description	Compétences requises
Passez en revue les rambardes et corrigez les violations.	Passez en revue les garde-corps définis dans l'unité d'organisation cible, en particulier les garde-corps préventifs, et corrigez les violations éventuelles. Un certain nombre de garde-corps préventifs obligatoires sont activés par défaut lorsque vous configurez la zone de landing de votre AWS Control Tower. Ils ne peuvent pas être désactivés. Vous devez passer en revue ces garde-fous obligatoires et corriger le compte du membre (manuellement ou à l'aide d'un script) avant d'enregistrer le compte. **Note** Des garde-fous préventifs garantissent la conformité des comptes enregistrés dans AWS Control Tower et préviennent les violations des politiques. Toute violation des garde-fous préventifs peut affecter l'inscription.	Administrateur AWS Control Tower, administrateur du compte membre

Tâche	Description	Compétences requises
	Les violations des garde-fous Detective apparaissent dans le tableau de bord AWS Control Tower, si elles sont détectées, une fois l'inscription réussie. Ils n'ont aucune incidence sur le processus d'inscription. Pour plus d'informations, consultez la section Guardrails in AWS Control Tower dans la documentation AWS.	
Vérifiez les problèmes de connectivité après avoir corrigé les violations des garde-corps.	Dans certains cas, vous devrez peut-être fermer des ports spécifiques ou désactiver des services pour corriger les violations des garde-corps. Assurez-vous que les applications qui utilisent ces ports et services sont corrigées avant d'inscrire le compte.	Propriétaire de l'application

Enregistrez le compte dans AWS Control Tower

Tâche	Description	Compétences requises
Connectez-vous à la console AWS Control Tower.	Utilisez des identifiants de connexion dotés d'autorisations administratives pour	Administrateur de la tour de contrôle AWS

Tâche	Description	Compétences requises
	AWS Control Tower. N'utilisez pas les informations d'identification de l'utilisateur root (compte de gestion) pour inscrire un compte AWS Organizations. Cela affichera un message d'erreur.	

Tâche	Description	Compétences requises
Enregistrez le compte.	1. Sur la page Account Factory d'AWS Control Tower, choisissez Inscrire un compte. 2. Renseignez les informations, notamment l'adresse e-mail associée au compte que vous souhaitez enregistrer, le nom d'affichage qui apparaîtra dans AWS Control Tower, l'adresse e-mail de l'IAM Identity Center, le prénom et le nom de famille du titulaire du compte, ainsi que l'unité d'organisation dans laquelle vous souhaitez enregistrer le compte. L'adresse e-mail de l'IAM Identity Center est votre adresse e-mail utilisateur préférée. Vous pouvez utiliser la même adresse e-mail que celle du compte. 3. Choisissez Inscrire un compte. Pour plus d'informations, consultez la section Enregistrer un compte existant dans la documentation AWS Control Tower.	Administrateur de la tour de contrôle AWS

Vérifiez le compte après l'inscription

Tâche	Description	Compétences requises
Vérifiez le compte.	Dans AWS Control Tower, sélectionnez Accounts. L'état initial du compte que vous venez de créer est « Inscripti on ». Lorsque l'inscription est terminée, son état passe à Inscrit.	Administrateur AWS Control Tower, administrateur du compte membre
Vérifiez s'il y a des violations du garde-corps.	Les garde-fous définis dans l'UO s'appliqueront automatiq uement au compte du membre inscrit. Surveillez le tableau de bord d'AWS Control Tower pour détecter les violations et corrigez-les en conséquen ce. Pour plus d'informations, consultez la section Guardrails in AWS Control Tower dans la documentation AWS.	Administrateur AWS Control Tower, administrateur du compte membre

Résolution des problèmes

Problème	Solution
Vous recevez le message d'erreur suivant : Une erreur inconnue s'est produite. Réessayez ultérieurement ou contactez le support AWS.	Cette erreur se produit lorsque vous utilisez les informations d'identification de l'utilisateur root (compte de gestion) dans AWS Control Tower pour inscrire un nouveau compte. AWS Service Catalog ne parvient pas à associer le portefeui lle ou le produit Account Factory à l'utilisateur root, ce qui entraîne le message d'erreur. Pour corriger cette erreur, utilisez des informations

Problème	Solution
	d'identification d'utilisateur (administrateur) à accès complet (administrateur) autres que root pour inscrire le nouveau compte. Pour plus d'informations sur la façon d'attribuer un accès administratif à un utilisateur administr atif, consultez la documentation Getting started in the AWS IAM Identity Center (successeur d'AWS Single Sign-On).
La page AWS Control Tower Activities affiche une action Get Catastrophic Drift.	Cette action reflète une vérification à la dérive du service et n'indique aucun problème lié à la configuration d'AWS Control Tower. Aucune action n’est requise.

Ressources connexes

Documentation

- Terminologie et concepts d'AWS Organizations (documentation AWS Organizations)
- Qu'est-ce qu'AWS Control Tower ? (documentation AWS Control Tower)
- Supprimer un compte membre de votre organisation (documentation AWS Organizations)
- Création d'un compte administrateur dans AWS Control Tower (documentation AWS Control Tower)

Tutoriels et vidéos

- Atelier AWS Control Tower (atelier à suivre à votre rythme)
- Qu'est-ce qu'AWS Control Tower ? (vidéo)
- Provisionnement des utilisateurs dans AWS Control Tower (vidéo)
- Activer AWS Control Tower pour une organisation existante (vidéo)

Surveillez les clusters SAP RHEL Pacemaker à l'aide des services AWS

Créée par Harsh Thoria (AWS), Randy Germann (AWS) et RAVEENDRA Voore (AWS)

Récapitulatif

Ce modèle décrit les étapes de surveillance et de configuration des alertes pour un cluster Red Hat Enterprise Linux (RHEL) Pacemaker pour les applications SAP et les services de base de données SAP HANA à l'aide d'Amazon et CloudWatch d'Amazon Simple Notification Service (Amazon SNS).

La configuration vous permet de surveiller les ressources des clusters SAP SCS ou ASCS, Enqueue Replication Server (ERS) et SAP HANA lorsqu'elles sont « arrêtées » à l'aide de flux de CloudWatch journaux, de filtres métriques et d'alarmes. Amazon SNS envoie un e-mail à l'équipe chargée de l'infrastructure ou à l'équipe SAP Basis concernant l'état du cluster arrêté.

Vous pouvez créer les AWS ressources pour ce modèle à l'aide de AWS CloudFormation scripts ou de consoles AWS de service. Ce modèle suppose que vous utilisez les consoles ; il ne fournit pas de CloudFormation scripts ni ne couvre le déploiement de l'infrastructure pour CloudWatch Amazon SNS. Les commandes du stimulateur cardiaque sont utilisées pour définir la configuration des alertes du cluster.

Conditions préalables et limitations

Prérequis

- Un AWS compte actif.
- Amazon SNS est configuré pour envoyer des notifications par e-mail ou mobiles.
- Un cluster SAP ASCS/ERS for ABAP or SCS/ERS pour Java et SAP HANA Database RHEL Pacemaker. Pour obtenir des instructions, veuillez consulter les sections suivantes :
  - Configuration du cluster SAP HANA
  - Configuration du cluster SAP Netweaver ABAP/Java

Limites

- Cette solution fonctionne actuellement pour les clusters basés sur RHEL version 7.3 et versions ultérieures basés sur Pacemaker. Il n'a pas été testé sur les systèmes d'exploitation SUSE.

Versions du produit

- RHEL 7.3 et versions ultérieures

Architecture

Pile technologique cible

- Agent piloté par un événement d'alerte RHEL Pacemaker
- Amazon Elastic Compute Cloud (Amazon EC2)
- CloudWatch alarme
- CloudWatch groupe de logs et filtre métrique
- Amazon SNS

Architecture cible

Le schéma suivant illustre les composants et les flux de travail de cette solution.

Automatisation et mise à l'échelle

- Vous pouvez automatiser la création de AWS ressources à l'aide de CloudFormation scripts. Vous pouvez également utiliser des filtres métriques supplémentaires pour redimensionner et couvrir plusieurs clusters.

Outils

Services AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Outils

- CloudWatch agent (unifié) est un outil qui collecte les métriques, les journaux et les traces au niveau du système à partir des EC2 instances, et récupère les métriques personnalisées de vos applications.

- L'agent d'alerte Pacemaker (pour RHEL 7.3 et versions ultérieures) est un outil qui lance une action en cas de modification, par exemple lorsqu'une ressource s'arrête ou redémarre, dans un cluster Pacemaker.

Bonnes pratiques

- Pour connaître les meilleures pratiques relatives à l'utilisation des charges de travail SAP AWS, consultez le SAP Lens for the AWS Well-Architected Framework.
- Tenez compte des coûts liés à la mise en place CloudWatch de la surveillance des clusters SAP HANA. Pour plus d'informations, consultez la documentation CloudWatch .
- Envisagez d'utiliser un téléavertisseur ou un mécanisme de billetterie pour les alertes Amazon SNS.
- Vérifiez toujours les versions RHEL à haute disponibilité (HA) du package RPM pour PC, Pacemaker et agent de clôture AWS .

Épopées

Configurer Amazon SNS

Tâche	Description	Compétences requises
Créez une rubrique SNS.	1. Connectez-vous à la console Amazon SNS AWS Management Console et ouvrez-la sur v3/ home. https://console.aws.amazon.com/sns/ 2. Dans le tableau de bord Amazon SNS, sous Common actions (Actions courantes), choisissez Create topic (Créer une rubrique). 3. Dans la boîte de dialogue Créer un nouveau sujet,	Administrateur AWS

Tâche	Description	Compétences requises
	pour Type, sélectionnez Standard. 4. Dans Nom du sujet, entrez le nom du sujet (par exemple,`my-topic`). 5. Choisissez Créer une rubrique. Cela crée une rubrique SNS avec une politique de ressources qui vous permet de publier des notifications. 6. Copiez l'ARN de la rubrique (par exemple,`arn:aws:sns:us-east-1:111122223333:my-topic`). Vous utiliserez cet ARN dans une étape ultérieure.	

Tâche	Description	Compétences requises
Modifiez la politique d'accès pour la rubrique SNS.	1. Sur la console Amazon SNS, dans le volet de navigation, choisissez Rubriques, puis choisissez la rubrique que vous avez créée. 2. Choisissez Modifier et accédez à la section Politique d'accès. 3. Assurez-vous que la politique d'accès inclut CloudWatch l'un des principaux services autorisés à publier sur cette rubrique. Par exemple : `{ "Sid": "Allow AWS CloudWatch to Publish to this SNS topic", "Effect": "Allow", "Principal": { "Service": [ "cloudwatch.amazonaws.com" ] }, "Action": "SNS:Publish", "Resource": "arn:aws:sns:us-east-1:111122223333:my-topic" }`	Administrateur système AWS

Tâche	Description	Compétences requises
	4. Sélectionnez Enregistrer les modifications.	

Tâche	Description	Compétences requises
Abonnez-vous à la rubrique SNS.	1. Sur la console Amazon SNS, dans le volet de navigation, choisissez Subscriptions, Create subscription. 2. Pour l'ARN du sujet, collez l'ARN que vous avez créé lors de la première tâche. 3. Pour Protocole, choisissez E-mail. 4. Pour Endpoint, entrez l'adresse e-mail de la personne ou de l'équipe responsable du cluster SAP Pacemaker et qui doit recevoir des notificat ions. Par exemple, il peut s'agir de l'adresse e-mail de la liste de distribution de SAP Basis ou de l'équipe d'infrastructure. 5. Choisissez Créer un abonnement. 6. Depuis votre application de messagerie, ouvrez le message dans AWS Notifications et confirmez votre abonnement. Votre navigateur Web affiche une réponse de confirmation provenant de Amazon SNS.	Administrateur système AWS

Confirmez la configuration du cluster

Tâche	Description	Compétences requises
Vérifiez l'état du cluster.	Utilisez la commande pcs status pour vérifier que les ressources sont en ligne.	Administrateur SAP Basis

Configuration des alertes Pacemaker

Tâche	Description	Compétences requises

Configurez l'agent d'alerte Pacemaker sur l'instance de cluster principale.	Connectez-vous à l' EC2 instance dans le cluster principal et exécutez les commandes suivantes :
	`install --mode=0755 /usr/share/pacemaker/alerts/alert_file.sh.sample`
	`touch /var/lib/pacemaker/alert_file.sh`
	`touch /var/log/pcmk_alert_file.log`
	`chown hacluster:haclient /var/log/pcmk_alert_file.log`
	`chmod 600 /var/log/pcmk_alert_file.log`
	`pcs alert create id=alert_file description="Log events to a file." path=/var/lib/pacemaker/alert_file.sh`
	`pcs alert recipient add alert_file id=my-alert_logfile value=/va`
		Administrateur SAP Basis

Tâche	Description	Compétences requises
	`r/log/pcmk_alert_f ile.log`	

Configurez l'agent d'alerte Pacemaker sur l'instance de cluster secondaire.	Connectez-vous à l' EC2 instance de cluster secondaire dans le cluster secondaire et exécutez les commandes suivantes :
	`install --mode=0755 / usr/share/pacemak er/alerts/alert_fi le.sh.sample`
	`touch /var/lib/ pacemaker/alert_fi le.sh`
	`touch /var/log/ pcmk_alert_file.log`
	`chown hacluster :haclient /var/log/ pcmk_alert_file.log`
	`chmod 600 /var/log/ pcmk_alert_file.log`
		Administrateur SAP Basis

Tâche	Description	Compétences requises

Vérifiez que la ressource d'alerte RHEL a été créée.	Utilisez la commande suivante pour confirmer que la ressource d'alerte a été créée :
	`pcs alert`
	Le résultat de la commande ressemblera à ceci :
	`[root@xxxxxxx ~]# pcs alert`
	`Alerts:`
	`Alert: alert_file (path=/var/lib/pacemaker/alert_file.sh)`
	`Description: Log events to a file.`
	`Recipients:`
	`Recipient: my-alert_logfile (value=/var/log/pcmk_alert_file.log)`
		Administrateur SAP Basis

Configuration de l' CloudWatch agent

Tâche	Description	Compétences requises
Installez l' CloudWatch agent.	Il existe plusieurs méthodes pour installer l' CloudWatch agent sur une EC2 instance. Pour utiliser la ligne de commande : 1. Téléchargez le package de CloudWatch l'agent :	Administrateur système AWS

Tâche	Description	Compétences requises

	`wget https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-region/redhat/amd64/latest/amazon-cloudwatch-agent.rpm`
	
	où `<region>` est située l' EC2 instance (par exemple,`us-west-2`). Région AWS
	2. (Facultatif) Vérifiez la signature du package. Pour obtenir des instructions, consultez la section Vérification de la signature du package de l' CloudWatch agent dans la CloudWatch documentation.
	3. Installez le package sur la première instance :
	
	`sudo rpm -U ./amazon-cloudwatch-agent.rpm`
	
	4. Répétez l'opération pour l'instance secondaire.
	
	Pour plus d'informations, consultez la documentation CloudWatch .	

Tâche	Description	Compétences requises
Attachez un rôle IAM à l' EC2 instance.	Pour permettre à l' CloudWatch agent d'envoyer des données depuis les instances, vous devez associer le CloudWatchAgentServerRolerôle IAM à chaque instance. Vous pouvez également ajouter une politique pour l' CloudWatch agent à votre rôle IAM existant. Pour plus d’informations, consultez la documentation CloudWatch .	Administrateur AWS

Tâche	Description	Compétences requises
Configurez l' CloudWatch agent pour surveiller le fichier journal de l'agent d'alerte Pacemaker sur l'instance de cluster principale.	1. Configurez l'instance de cluster principale en exécutant la commande suivante : `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard` 2. Choisissez 1 pour Linux, puis sélectionnez les options correspondant à votre stratégie de surveillance. 3. Pour la question « Voulez-vous surveiller des fichiers journaux », choisissez Oui et indiquez le chemin du fichier journal du Pacemaker à partir de la commande pcs alert. Dans notre cas, c'est le cas`var/log/pcmk_alert_file.log` . 4. Indiquez le nom du groupe de journaux et du flux de journaux. Si vous ne spécifiez aucun flux de journal, l'ID d' AWS instance est utilisé par défaut.	Administrateur AWS

Tâche	Description	Compétences requises
	5. Répétez les étapes 1 à 4 pour l'instance de cluster secondaire.	
Démarrez l' CloudWatch agent sur les instances de cluster principales et secondaires.	Pour démarrer l'agent, exécutez la commande suivante sur les EC2 instances des clusters principal et secondaire : `sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json`	Administrateur AWS

Configuration des CloudWatch ressources

Tâche	Description	Compétences requises
Configurez des groupes de CloudWatch journaux.	1. Ouvrez la CloudWatch console à https://console.aws.amazon.com/cloudwatch/ 2. Dans le volet de navigation, choisissez Log groups, Create log group. 3. Entrez un nom pour le groupe de journaux, puis choisissez Create log group.	Administrateur AWS

Tâche	Description	Compétences requises
	L' CloudWatch agent transférera le fichier d'alerte Pacemaker vers le groupe de CloudWatch journaux sous forme de flux de journal.	

Tâche	Description	Compétences requises
Configurez des filtres CloudWatch métriques.	Les filtres métriques vous aident à rechercher un modèle, par exemple `stop <cluster-resource-name>` dans les flux de CloudWatch journaux. Lorsque ce modèle est identifié, le filtre métrique met à jour une métrique personnalisée. 1. Sur la CloudWatch console, dans le volet de navigation, choisissez Log groups. 2. Choisissez le nom du groupe de journaux que vous avez créé lors de la tâche précédente. 3. Choisissez Actions, Créer un filtre de métriques. 4. Pour Modèle de filtre, entrez le modèle de filtre à utiliser, par exemple pour correspondre à l'événement d'arrêt d'une ressource de cluster SAP SCS nomméeABC_scs. `stop ABC_scs` Pour plus d'informations, consultez la section Syntaxe du modèle de filtre dans la CloudWatch documentation.	Administrateur AWS, administrateur SAP Basis

Tâche	Description	Compétences requises
	5. (Facultatif) Pour tester votre modèle de filtre, sous Test Pattern (Modèle de test), saisissez un ou plusieurs événements du journal à utiliser pour tester le modèle. Chaque événement du journal doit être spécifié sur une ligne distincte, car les sauts de ligne sont utilisés pour séparer les événements du journal dans la zone Messages des événements du journal. 6. Sélectionnez Next (Suivant), puis saisissez un nom pour le filtre. 7. Sous Détails de la métrique, pour l'espace de noms métrique, entrez le nom de l' CloudWatch espace de noms dans lequel la métrique sera publiée (par exemple,`sapcluster_monitoring`). Si cet espace de noms n'existe pas déjà, sélectionnez Créer un nouveau. 8. Dans Nom de la métrique, entrez le nom de la nouvelle métrique (par exemple`sapcluster_<sid>` , où `<sid>` est	

Tâche	Description	Compétences requises
	le nom d'identification du système SAP). 9. Dans le champ Valeur métrique, entrez 1. Vous pouvez également saisir un jeton tel que`$size`. Cela incrémente la métrique de la valeur du nombre dans le champ `size` pour chaque événement de journal qui contient un champ `size`. 10. Dans le champ Valeur par défaut, entrez 0. 11. Choisissez Créer un filtre de métriques. Lorsque le filtre métrique identifie le modèle à l'étape 4, il met à jour la valeur de la métrique CloudWatch personnalisée `sapcluster_abc` à 1. L' CloudWatch alarme `SAP-Cluster-QA1-ABC` surveille la métrique `sapcluster_abc` et envoie une notification SNS lorsque la valeur de la métrique passe à 1. Cela indique que la ressource du cluster s'est	

Tâche	Description	Compétences requises
	arrêtée et que des mesures doivent être prises.	

Tâche	Description	Compétences requises
Configurez une alarme CloudWatch métrique pour la métrique SAP ASCS/SCS et ERS.	Pour créer une alarme basée sur une seule métrique, procédez comme suit : 1. Sur la CloudWatch console, dans le volet de navigation, choisissez Alarmes, Toutes les alarmes. 2. Choisissez Create alarm (Créer une alerte). 3. Choisissez Select Metric (Sélectionner une métrique) . 4. Recherchez la métrique `sapcluster_monitoring` personnalisée créée lors de la tâche précédente. 5. Choisissez le nom de la métrique pour SAP SCS (par exemple,`sapcluster_<abc>`), qui a également été créé lors de la tâche précédente. 6. Dans l'onglet Mesures graphiques, définissez les paramètres suivants : • Pour Statistique, choisissez Maximum. • Pour Période, choisissez 1 minute. • Pour le type de seuil, choisissez Statique et définissez le seuil sur	Administrateur AWS

Tâche	Description	Compétences requises
	une valeur supérieure ou égale à 1. **`sapcluster_<sid>`** 7. Choisissez Suivant. 8. Pour Notification, sélectionnez le sujet SNS que vous avez créé dans le premier épisode épique. 9. Dans Nom et description, indiquez le nom de l'alarme et une brève description, puis choisissez Next. 10. Sélectionnez Create Alarm (Créer une alerte).	
Configurez une alarme CloudWatch métrique pour la métrique SAP HANA.	Répétez les étapes de configuration d'une alarme CloudWatch métrique à partir de la tâche précédente, avec les modifications suivantes : • Pour l'étape 5, choisissez le nom de la métrique pour SAP HANA (par exemple, `sapcluster_db_<abc>`). • Pour l'étape 6, définissez le seuil `sapcluster_<sid>` pour une valeur supérieure à 0.	Administrateur AWS

Ressources connexes

- Scripts de déclenchement pour les événements du cluster (documentation RHEL)

- Création du fichier de configuration de l' CloudWatch agent à l'aide de l'assistant (CloudWatch documentation)
- Installation et exécution de l' CloudWatch agent sur vos serveurs (CloudWatch documentation)
- Création d'une CloudWatch alarme basée sur un seuil statique (CloudWatch documentation)
- Déploiement manuel de SAP HANA sur AWS avec des clusters à haute disponibilité (documentation SAP sur AWS le site Web)
- NetWeaver Guides SAP (documentation SAP sur le AWS site Web)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Surveillez l'activité des applications à l'aide de CloudWatch Logs Insights

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Ce modèle fournit une solution pour détecter et signaler automatiquement les exceptions d'application à l'aide d'Amazon CloudWatch Logs Insights. En mettant en œuvre une analyse automatique des journaux et des alertes, vous pouvez rapidement identifier les problèmes liés aux applications dans votre environnement de production et y répondre.

Les journaux jouent un rôle crucial dans la surveillance du comportement du système, l'identification des problèmes et la garantie de performances optimales. Au cours d'un processus de migration, les fichiers journaux sont essentiels pour valider le fonctionnement du système dans le nouvel environnement, détecter les problèmes de compatibilité et identifier les comportements inattendus. Les problèmes peuvent être liés aux opérations ou à la sécurité. Pour les problèmes liés à la sécurité, il est essentiel de détecter à un stade précoce les tentatives d'accès non autorisées ou les activités suspectes afin de garantir la sécurité et la conformité réglementaire. Cette fonctionnalité est particulièrement importante lorsqu'il s'agit de données sensibles ou de systèmes critiques.

Ce modèle est particulièrement utile pour les équipes qui doivent maintenir une haute disponibilité des applications et répondre rapidement aux problèmes de production. Il est pertinent dans différents secteurs et cas d'utilisation. Par exemple, dans le domaine des télécommunications, il permet d'identifier rapidement les mauvaises configurations ou les pannes du réseau et de détecter les chemins de routage sous-optimaux pour identifier les encombrements potentiels. Dans le domaine de l'Internet des objets (IoT), les composants de Greengrass peuvent publier des journaux CloudWatch, ce qui permet à cette technique d'extraire les détails pertinents des journaux et de les présenter dans un tableau de bord complet.

Conditions préalables et limitations

Prérequis

- Une application de production déployée en mode actif Compte AWS
- Compréhension de base du format de journalisation et des modèles d'exception de l'application de production
- Les journaux d'application sont configurés pour être diffusés sur Amazon CloudWatch Logs

Limites

- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, consultez la section AWS Services par région. Pour des points de terminaison spécifiques, consultez Points de terminaison de service et quotas, puis choisissez le lien correspondant au service.

Architecture

Le schéma suivant montre comment CloudWatch Logs Insights évalue les journaux des ressources et envoie une visualisation des données pertinente à un CloudWatch tableau de bord.

Le schéma suivant illustre le flux de travail suivant :

1. Les ressources publient des journaux dans CloudWatch Logs. Les ressources peuvent inclure AWS des ressources telles que des instances Amazon Elastic Compute Cloud (Amazon EC2) ou des buckets Amazon Simple Storage Service (Amazon S3). Un autre exemple inclut les systèmes sur site sur lesquels un CloudWatch agent est installé et qui peuvent publier des journaux sur. CloudWatch
2. CloudWatch Logs Insights filtre la chaîne de modèle appropriée. Les exemples de chaînes de modèles de recherche incluent « error », « exception » ou une expression régulière spécifique.
3. Généralement, l'équipe d'assistance à la production ou les développeurs ajoutent la visualisation du modèle au CloudWatch tableau de bord.

Automatisation et mise à l'échelle

Les développeurs peuvent automatiser la solution de ce modèle en utilisant le AWS Cloud Development Kit (AWS CDK) AWS CloudFormation, ou AWS SDKs pour gérer plusieurs modèles de chaînes. Les équipes peuvent intégrer cette automatisation dans leurs processus d'intégration et de déploiement continus (CI/CD). DevOps

Outils

Services AWS

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes et applications, Services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.

- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.

Bonnes pratiques

- Définissez et configurez des groupes de journaux pour analyser les données de journal pertinentes.
- Utilisez les explorateurs de champs pour comprendre la structure et les champs disponibles dans les données de votre journal.
- Rédigez des requêtes efficaces en utilisant la syntaxe des requêtes de CloudWatch Logs Insights.
- Adaptez les exemples de requêtes à vos besoins spécifiques pour une analyse plus rapide.
- Surveillez les requêtes pour identifier les problèmes de performances ou les goulots d'étranglement potentiels.
- Définissez des limites de requêtes pour éviter des coûts ou une consommation de ressources excessifs.
- Enregistrez les requêtes pour une utilisation future afin de gagner du temps et de garantir une analyse cohérente.
- Appliquez les politiques IAM appropriées pour contrôler l'accès à CloudWatch Logs Insights et aux groupes de journaux. Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.
- Activez le chiffrement des données de journal à AWS KMS l'aide de données de journal sensibles.

Épopées

Créez un groupe de journaux et configurez les journaux à afficher dans le tableau de bord.

Tâche	Description	Compétences requises
Configurez les autorisations IAM.	Pour configurer les autorisations IAM, procédez comme suit :	Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	1. Identifiez les rôles IAM utilisés par votre application pour écrire des journaux et par les utilisateurs ou les services qui créeront des tableaux de bord, des requêtes et des alarmes. 2. Pour le rôle d'application, ajoutez les actions et ressources d'API suivantes à une politique : `{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents" ], "Resource": [ "arn:aws:logs:*:*:*" ] } ]`	

Tâche	Description	Compétences requises

	<pre>}</pre>
	3. Pour gérer les CloudWatch ressources, ajoutez ce qui suit à une politique :
	<pre>{
	    "Version":
	"2012-10-17",
	    "Statement": [
	        {
	            "Effect":
	"Allow",
	            "Action":
	[
	
	"cloudwatch:PutDas
	hboard",
	
	"cloudwatch:GetDas
	hboard",
	
	"logs:StartQuery",
	
	"logs:StopQuery",
	
	"logs:GetQueryResu
	lts",
	
	"cloudwatch:PutMet
	ricAlarm"
	            ],
	            "Resource
	": "*"
	        }
	    ]
	}</pre>
	Pour plus d'informations sur la façon de créer des politiques	

Tâche	Description	Compétences requises
	IAM ou d'ajouter des autorisations à des politiques existantes, voir Définir des autorisations IAM personnalisées avec des politiques gérées par le client et Modifier les politiques IAM dans le Guide de l'utilisateur IAM. Pour plus d'informations, consultez la référence sur la gestion des identités et des accès pour Amazon CloudWatch CloudWatch Logs et les autorisations dans le guide de l'utilisateur Amazon CloudWatch Logs.	

Tâche	Description	Compétences requises

Créez un groupe de journaux .	Pour créer un groupe de journaux, utilisez l'une des options suivantes :
	• Créez ou ouvrez un fichier CloudFormation modèle (format YAML ou JSON) avec une `.json` extension `.yaml` or. (Le code suivant utilise le format YAML.) Ajoutez la définition de ressource suivante à la section Ressources de votre modèle :
	`MyLogGroup:`
	`  Type: AWS::Logs`
	`::LogGroup`
	`  Properties:`
	`  LogGroupName: my-`
	`log-group`
	Pour plus d'informations, consultez Quick Start : Use AWS CloudFormation to get started with CloudWatch Logs dans le guide de l'utilisateur Amazon CloudWatch Logs.
	• Utilisez la CloudWatch console, comme décrit dans la section Créer un groupe de CloudWatch journaux dans Logs
		Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	du guide de l'utilisateur Amazon CloudWatch Logs. • Utilisez l'CreateLog Groupopération dans l'API CloudWatch Logs.	

Tâche	Description	Compétences requises
Générez une requête CloudWatch Logs Insights.	Pour créer et enregistrer une requête CloudWatch Logs Insights, procédez comme suit : 1. Ouvrez la CloudWatch console. 2. Accédez à Logs Insights. 3. Créez votre requête à l'aide de l'une des méthodes suivantes : • Commencez par un exemple de requête de la section Requêtes. • Rédigez une requête personnalisée. • Modifiez l'exemple de requête suivant : `fields @timestamp, @message | filter @message like /(?i)exception/|stats count() by bin(30s)` Cette requête vérifie le fichier journal, extrait l'horodatage et le contenu du message, filtre le mot « exception » (sans distinction majuscules/minuscules) et compte les occurrences toutes les 30 secondes.	Administrateur AWS, AWS DevOps, administrateur système AWS, administr ateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
Créez une visualisation dans un CloudWatch tableau de bord.	Pour utiliser un CloudWatch tableau de bord afin de créer une visualisation, procédez comme suit : 1. Ouvrez la CloudWatch console et créez un CloudWatch tableau de bord (si vous n'en avez pas déjà un) ou ouvrez un tableau de bord existant. 2. Ajoutez votre visualisation de surveillance des exceptions. Des diagrammes à barres, linéaires et à secteurs sont disponibles, en fonction des besoins de votre entreprise. Pour plus d'informations, consultez la section Utilisation de widgets sur les CloudWatch tableaux de bord dans le guide de l'utilisateur Amazon CloudWatch Logs. Pour les visualisations de données en temps réel, vous pouvez personnaliser un widget en fonction de vos besoins. Pour plus d'informations sur les options et fonctionnalités des tableaux de bord, consultez les sections Utilisati	Administrateur AWS, AWS DevOps, administrateur système AWS, administrateur cloud, architecte cloud, DevOps ingénieur

Tâche	Description	Compétences requises
	on CloudWatch des tableaux de bord Amazon et Création de CloudWatch tableaux de bord flexibles avec des variables de tableau de bord dans le guide de l'utilisateur Amazon CloudWatch Logs.	

Résolution des problèmes

Problème	Solution
Impossible de voir les résultats de la requête ou la requête semble interrompue	Commencez par une requête fonctionnelle qui a été modifiée à partir d'un exemple de requête. Apportez de petites modifications incrément ielles à certaines parties de la requête (comme un filtre ou un champ) et tirez parti de la fonctionnalité de générateur de requêtes CloudWatch Logs.
Les groupes de journaux ne créent pas de flux de journaux	Dans la politique IAM, assurez-vous que la ressource pour les opérations CreateLog Streamet les CreateLogGroupopérations est dotée d'une valeur de caractère générique (`*`). L'`create` opération ne réussira pas sans cette autorisation générique.

Ressources connexes

- Analyse des données des CloudWatch journaux avec Logs Insights
- Amazon CloudWatch FAQs
- Création de CloudWatch tableaux de bord flexibles avec des variables de tableau de bord
- Commencez avec Logs Insights QL : tutoriels sur les requêtes

- Utiliser le langage naturel pour générer et mettre à jour CloudWatch les requêtes Logs Insights
- Utilisation PutDashboard avec un AWS SDK ou une CLI
- Utilisation de groupes de journaux et de flux de journaux

Surveillez l'utilisation d'une Amazon Machine Image partagée sur plusieurs Comptes AWS

Créée par Naveen Suthar (AWS) et Sandeep Gawande (AWS)

Récapitulatif

Les images Amazon Machine (AMIs) sont utilisées pour créer des instances Amazon Elastic Compute Cloud (Amazon EC2) dans votre environnement Amazon Web Services (AWS). Vous pouvez créer AMIs dans un compte AWS distinct et centralisé, appelé compte de créateur dans ce modèle. Vous pouvez ensuite partager l'AMI entre plusieurs Comptes AWS comptes identiques Région AWS, appelés comptes consommateurs dans ce modèle. La gestion AMIs à partir d'un seul compte assure l'évolutivité et simplifie la gouvernance. Dans les comptes clients, vous pouvez référencer l'AMI partagée dans les modèles de lancement Amazon EC2 Auto Scaling et les groupes de nœuds Amazon Elastic Kubernetes Service (Amazon EKS).

Lorsqu'une AMI partagée est déconseillée, désenregistrée ou non partagée, les personnes qui Services AWS font référence à l'AMI dans les comptes des consommateurs ne peuvent pas utiliser cette AMI pour lancer de nouvelles instances. Tout événement de mise à l'échelle automatique ou tout redémarrage de la même instance échoue. Cela peut entraîner des problèmes dans l'environnement de production, tels que des temps d'arrêt des applications ou une dégradation des performances. Lorsque des événements de partage et d'utilisation d'AMI se produisent en plusieurs fois Comptes AWS, il peut être difficile de surveiller cette activité.

Ce modèle vous permet de surveiller l'utilisation et le statut des AMI partagées entre les comptes d'une même région. Il utilise le mode sans serveur Services AWS, tel qu'Amazon EventBridge, Amazon AWS Lambda DynamoDB et Amazon Simple Email Service (Amazon SES). Vous provisionnez l'infrastructure sous forme de code (iAc) à l'aide de HashiCorp Terraform. Cette solution fournit des alertes lorsqu'un service d'un compte client fait référence à une AMI désenregistrée ou non partagée.

Conditions préalables et limitations

Prérequis

- Deux comptes actifs ou plus Comptes AWS : un compte créateur et un ou plusieurs comptes consommateurs
- Un ou plusieurs AMIs éléments partagés entre le compte du créateur et le compte du consommateur

- Terraform CLI, installée (documentation Terraform)
- AWS Fournisseur Terraform, configuré (documentation Terraform)
- (Facultatif, mais recommandé) Backend Terraform, configuré (documentation Terraform)
- Git, installé

Limites

- Ce modèle surveille ceux AMIs qui ont été partagés avec des comptes spécifiques à l'aide de l'identifiant du compte. Ce modèle ne surveille pas ceux AMIs qui ont été partagés avec une organisation à l'aide de l'ID de l'organisation.
- AMIs ne peut être partagé qu'avec des comptes appartenant au même compte Région AWS. Ce modèle surveille AMIs au sein d'une seule région cible. Pour surveiller l'utilisation AMIs dans plusieurs régions, vous déployez cette solution dans chaque région.
- Ce modèle ne surveille aucun élément AMIs partagé avant le déploiement de cette solution. Si vous souhaitez surveiller le partage antérieur AMIs, vous pouvez annuler le partage de l'AMI, puis le partager à nouveau avec les comptes clients.

Versions du produit

- Terraform version 1.2.0 ou ultérieure
- Terraform AWS Provider version 4.20 ou ultérieure

Architecture

Pile technologique cible

Les ressources suivantes sont fournies en tant qu'iAc via Terraform :

- Tables Amazon DynamoDB
- EventBridge Règles d'Amazon
- AWS Identity and Access Management Rôle (IAM)
- AWS Lambda fonctions
- Amazon SES

Architecture cible

Le schéma suivant illustre le flux de travail suivant :

1. Une AMI dans le compte créateur est partagée avec un compte client dans le même compte Région AWS.
2. Lorsque l'AMI est partagée, une EventBridge règle du compte créateur capture l'`ModifyImageAttribute`événement et lance une fonction Lambda dans le compte créateur.
3. La fonction Lambda stocke les données relatives à l'AMI dans une table DynamoDB du compte créateur.
4. Lorsqu'un Service AWS compte client utilise l'AMI partagée pour lancer une EC2 instance Amazon ou lorsque l'AMI partagée est associée à un modèle de lancement, une EventBridge règle du compte client capture l'utilisation de l'AMI partagée.
5. La EventBridge règle initie une fonction Lambda dans le compte client. La fonction Lambda effectue les opérations suivantes :
   a. La fonction Lambda met à jour les données relatives à l'AMI dans une table DynamoDB du compte client.
   b. La fonction Lambda assume un rôle IAM dans le compte de créateur et met à jour la table Lambda dans le compte de créateur. Dans le `Mapping` tableau, il crée un élément qui associe l'ID d'instance ou l'ID du modèle de lancement à son ID d'AMI respectif.
6. L'AMI gérée de manière centralisée dans le compte du créateur est obsolète, désenregistrée ou n'est plus partagée.
7. La EventBridge règle du compte créateur capture l'`DeregisterImage`événement `ModifyImageAttribute` ou associé à l'`remove`action et lance la fonction Lambda.
8. La fonction Lambda vérifie la table DynamoDB pour déterminer si l'AMI est utilisée dans l'un des comptes consommateurs. Si aucune instance IDs ou modèle de lancement n'est IDs associé à l'AMI dans le `Mapping` tableau, le processus est terminé.
9. Si une instance IDs ou un modèle IDs de lancement est associé à l'AMI dans le `Mapping` tableau, la fonction Lambda utilise Amazon SES pour envoyer une notification par e-mail aux abonnés configurés.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, des AWS Lambda fonctions, des points de terminaison d'invocation HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Email Service (Amazon SES) vous permet d'envoyer et de recevoir des e-mails en utilisant vos propres adresses e-mail et domaines.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub cross-account-ami-monitoring-terraform-samples.

Bonnes pratiques

- Suivez les meilleures pratiques relatives à l'utilisation des AWS Lambda fonctions.
- Suivez les meilleures pratiques en matière de construction AMIs.
- Lorsque vous créez le rôle IAM, suivez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation IAM.
- Configurez la surveillance et les alertes pour les AWS Lambda fonctions. Pour plus d'informations, consultez la section Surveillance et résolution des problèmes des fonctions Lambda.

Épopées

Personnalisez les fichiers de configuration Terraform

Tâche	Description	Compétences requises
Créez les profils AWS CLI nommés.	Pour le compte créateur et pour chaque compte client, créez un profil nommé AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, voir Configurer le AWS CLI dans le centre de ressources AWS pour la mise en route.	DevOps ingénieur
Pour cloner le référentiel.	Entrez la commande suivante. Cela clone le référentiel cross-account-ami-monitoring-terraform-samples à l'aide de SSH. GitHub `git clone git@github.com:aws-samples/cross-account-ami-monitoring-terraform-samples.git`	DevOps ingénieur
Mettez à jour le fichier provider.tf.	1. Entrez la commande suivante pour accéder au `terraform` dossier du référentiel cloné. `cd cross-account-ami-monitoring/terraform` 2. Ouvrez le fichier `provider.tf` .	DevOps ingénieur

Tâche	Description	Compétences requises
	3. Mettez à jour les configurations du AWS fournisseur Terraform pour le compte créateur et le compte consommateur comme suit : • Pour `alias`, entrez un nom pour la configuration du fournisseur. • Pour `region`, entrez la cible sur Région AWS laquelle vous souhaitez déployer cette solution. • Pour `profile`, entrez le profil AWS CLI nommé pour accéder au compte. 4. Si vous configurez plusieurs comptes client, créez un profil pour chaque compte client supplémentaire. 5. Enregistrez et fermez le fichier `provider.tf` . Pour plus d'informations sur la configuration des fournisseurs, consultez la section Configurations de fournisseurs multiples dans la documentation Terraform.	

Tâche	Description	Compétences requises
Mettez à jour le fichier terraform.tfvars.	1. Ouvrez le fichier `terraform.tfvars` . 2. Dans le `account_email_mapping` paramètre, configurez les alertes pour le compte créateur et le compte consommateur comme suit : • Pour `account`, entrez l'identifiant du compte. • Pour `email`, entrez l'adresse e-mail à laquelle vous souhaitez envoyer les alertes. Vous ne pouvez saisir qu'une seule adresse e-mail pour chaque compte. 3. Si vous configurez plusieurs comptes client, entrez un compte et une adresse e-mail pour chaque compte client supplémentaire. 4. Enregistrez et fermez le fichier `terraform.tfvars` .	DevOps ingénieur

Tâche	Description	Compétences requises
Mettez à jour le fichier main.tf.	Effectuez ces étapes uniquement si vous déployez cette solution sur plusieurs comptes client. Si vous déployez cette solution sur un seul compte client, aucune modification de ce fichier n'est nécessaire. 1. Ouvrez le fichier `main.tf`. 2. Pour chaque compte client supplémentaire, créez un nouveau module basé sur le `consumer_account_A` module du modèle. Pour chaque compte client, pour`provider`, la valeur doit correspondre à l'alias que vous avez saisi dans le `provider.tf` fichier. 3. Enregistrez et fermez le fichier `main.tf`.	DevOps ingénieur

Déployez la solution à l'aide de Terraform

Tâche	Description	Compétences requises
Déployez la solution.	Dans la CLI Terraform, entrez les commandes suivantes pour déployer les AWS ressources dans les comptes de créateur et de consommateur :	DevOps ingénieur

Tâche	Description	Compétences requises

	1. Entrez la commande suivante pour initialiser Terraform.
	`terraform init`
	2. Entrez la commande suivante pour valider les configurations Terraform.
	`terraform validate`
	3. Entrez la commande suivante pour créer un plan d'exécution Terraform.
	`terraform plan`
	4. Passez en revue les modifications de configuration dans le plan Terraform et confirmez que vous souhaitez implémenter ces modifications.
	5. Entrez la commande suivante pour déployer les ressources.
	`terraform apply`	

Tâche	Description	Compétences requises
Vérifiez l'identité de l'adresse e-mail.	Lorsque vous avez déployé le plan Terraform, Terraform a créé une identité d'adresse e-mail pour chaque compte client dans Amazon SES. Avant que les notifications puissent être envoyées à cette adresse e-mail, vous devez vérifier l'adresse e-mail. Pour obtenir des instructions, consultez Vérifier l'identité d'une adresse e-mail dans la documentation Amazon SES.	AWS général

Valider le déploiement des ressources

Tâche	Description	Compétences requises
Validez le déploiement dans le compte du créateur.	1. Connectez-vous au compte du créateur. 2. Dans la barre de navigation, confirmez que vous visualisez la cible Région AWS. Si vous vous trouvez dans une autre région, choisissez le nom de la région actuellement affichée, puis choisissez la région cible. 3. Ouvrez la console DynamoDB. 4. Dans le volet de navigation, choisissez Tables.	DevOps ingénieur

Tâche	Description	Compétences requises
	5. Dans la liste des tables, vérifiez que la `AmiShare` table est présente. 6. Ouvrez la console Lambda. 7. Dans le volet de navigation, choisissez Fonctions. 8. Dans la liste des fonctions, vérifiez que la `ami-share` fonction est présente. 9. Ouvrez la console IAM. 10. Dans le panneau de navigation, choisissez Roles (Rôles). 11. Dans la liste des rôles, vérifiez que le `external-ddb-role` rôle est présent. 12. Ouvrez la EventBridge console. 13. Dans le volet de navigation, choisissez Règles. 14. Dans la liste des règles, vérifiez que la `modify_image_attribute_event` règle est présente. 15. Ouvrez la console Amazon SES. 16. Dans le volet de navigation, choisissez Verified Identities. 17. Dans la liste des identités, vérifiez qu'une adresse	

Tâche	Description	Compétences requises
	e-mail a été enregistrée et vérifiée pour chaque compte client.	

Tâche	Description	Compétences requises
Validez le déploiement dans le compte client.	1. Connectez-vous au compte client. 2. Dans la barre de navigation, confirmez que vous visualisez la cible Région AWS. Si vous vous trouvez dans une autre région, choisissez le nom de la région actuellement affichée, puis choisissez la région cible. 3. Ouvrez la console DynamoDB. 4. Dans le volet de navigation, choisissez Tables. 5. Dans la liste des tables, vérifiez que la `Mapping` table est présente. 6. Ouvrez la console Lambda. 7. Dans le volet de navigation, choisissez Fonctions. 8. Dans la liste des fonctions, vérifiez que les `ami-deregister-function` fonctions `ami-usage-function` et sont présentes. 9. Ouvrez la EventBridge console. 10. Dans le volet de navigation, choisissez Règles.	DevOps ingénieur

Tâche	Description	Compétences requises
	11. Dans la liste des règles, vérifiez que les `ami_deregister_events` règles `ami_usage_events` et sont présentes.	

Valider la surveillance

Tâche	Description	Compétences requises
Créez une AMI dans le compte du créateur.	1. Dans le compte du créateur, créez une AMI privée. Pour obtenir des instructions, consultez Créer une AMI à partir d'une EC2 instance Amazon. 2. Partagez la nouvelle AMI avec l'un des comptes clients. Pour obtenir des instructions, voir Partager une AMI avec des personnes spécifiques Comptes AWS.	DevOps ingénieur
Utilisez l'AMI dans le compte client.	Dans le compte client, utilisez l'AMI partagée pour créer une EC2 instance Amazon ou un modèle de lancement. Pour obtenir des instructions, consultez How do I launch an Amazon EC2 instance from a custom AMI (AWS Re:Post Knowledge Center) ou Create	DevOps ingénieur

Tâche	Description	Compétences requises
	a launch template for an Auto Scaling group (documentation Amazon EC2 Auto Scaling).	
Validez la surveillance et les alertes.	1. Connectez-vous au compte du créateur. 2. Ouvrez la EC2 console Amazon. 3. Dans le panneau de navigation, sélectionnez AMIs. 4. Sélectionnez l'AMI dans la liste, puis choisisse z Actions, Modifier les autorisations de l'AMI. 5. Dans la section Comptes partagés, sélectionnez le compte client, puis choisissez Supprimer la sélection. 6. Sélectionnez Enregistrer les modifications. 7. Vérifiez que l'adresse e-mail cible que vous avez définie pour le compte client reçoit une notification indiquant que le partage a été annulé pour l'AMI.	DevOps ingénieur

(Facultatif) Arrêter la surveillance partagée AMIs

Tâche	Description	Compétences requises
Supprimez les ressources.	1. Entrez la commande suivante pour supprimer les ressources déployées selon ce modèle et arrêter la surveillance partagée AMIs. `terraform destroy` 2. Confirmez la `destroy` commande en entrant`yes`.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
Je n'ai pas reçu d'alerte par e-mail.	Il peut y avoir plusieurs raisons pour lesquelle s l'e-mail d'Amazon SES n'a pas été envoyé. Vérifiez les éléments suivants : 1. Dans la section Epics, utilisez l'épopée de validation du déploiement des ressource s pour confirmer que l'infrastructure a été correctement provisionnée dans l'ensemble. Comptes AWS 2. Validez les événements de la fonction Lambda dans Amazon CloudWatch Logs. Pour obtenir des instructions, consultez la section Utilisation de la CloudWatch console dans la documentation Lambda. Vérifiez qu'il n'y a aucun problème d'autorisation, tel qu'un refus explicite dans les politique s basées sur l'identité ou les ressources.

Problème	Solution
	Pour plus d'informations, consultez la section Logique d'évaluation des politiques dans la documentation IAM. 3. Dans Amazon SES, vérifiez que le statut de l'identité de l'adresse e-mail est vérifié. Pour plus d'informations, consultez la section Vérification de l'identité d'une adresse e-mail.

Ressources connexes

AWS documentation

- Création de fonctions Lambda avec Python (documentation Lambda)
- Création d'une AMI (EC2 documentation Amazon)
- Partager une AMI avec un utilisateur spécifique Comptes AWS (EC2 documentation Amazon)
- Désenregistrer votre AMI (documentation Amazon EC2)

Documentation Terraform

- Installez Terraform
- Configuration du backend Terraform
- Fournisseur AWS Terraform
- Téléchargement du binaire Terraform

Configurez des alertes pour les fermetures de comptes programmatiques dans AWS Organizations

Créée par Richard Milner-Watts (AWS), Debojit Bhadra (AWS) et Manav Yadav (AWS)

Récapitulatif

L'CloseAccount API pour AWS Organizations vous permet de fermer les comptes des membres d'une organisation par programmation, sans avoir à vous connecter au compte avec des informations d'identification root. L'RemoveAccountFromOrganization API extrait un compte d'une organisation dans AWS Organizations pour en faire un compte autonome.

Cela augmente APIs potentiellement le nombre d'opérateurs autorisés à fermer ou supprimer un compte AWS. Tous les utilisateurs qui ont accès à l'organisation via AWS Identity and Access Management (IAM) dans le compte de gestion AWS Organizations peuvent les APIs appeler. L'accès n'est donc pas limité au propriétaire de l'adresse e-mail racine du compte associée à tout dispositif d'authentification multifactorielle (MFA) associé.

Ce modèle implémente des alertes lorsque les `CloseAccount` et `RemoveAccountFromOrganization` APIs sont appelés, afin que vous puissiez surveiller ces activités. Pour les alertes, il utilise une rubrique Amazon Simple Notification Service (Amazon SNS). Vous pouvez également configurer les notifications Slack via un webhook.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une organisation dans AWS Organizations
- Accès au compte de gestion de l'organisation, sous la racine de l'organisation, pour créer les ressources nécessaires

Limites

- Comme décrit dans le guide de référence de l'API AWS Organizations, l'`CloseAccount`API permet de fermer seulement 10 % des comptes de membres actifs sur une période continue de 30 jours.

- Lorsqu'un compte AWS est fermé, son statut passe à SUSPENDU. Pendant 90 jours après cette transition de statut, AWS Support peut rouvrir le compte. Après 90 jours, le compte est définitivement supprimé.
- Utilisateurs ayant accès au compte de gestion AWS Organizations et APIs pouvant également être autorisés à désactiver ces alertes. Si le principal problème est un comportement malveillant plutôt qu'une suppression accidentelle, envisagez de protéger les ressources créées par ce modèle avec une limite d'autorisations IAM.
- L'API appelle `CloseAccount` et `RemoveAccountFromOrganization` est traitée dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`). Par conséquent, vous devez déployer cette solution `us-east-1` afin d'observer les événements.

Architecture

Pile technologique cible

- AWS Organizations
- AWS CloudTrail
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Architecture cible

Le schéma suivant montre l'architecture de la solution pour ce modèle.

1. AWS Organizations traite une `RemoveAccountFromOrganization` demande d'`CloseAccountor`.
2. Amazon EventBridge est intégré à AWS CloudTrail pour transmettre ces événements au bus d'événements par défaut.
3. Une EventBridge règle Amazon personnalisée correspond aux demandes d'AWS Organizations et appelle une fonction AWS Lambda.
4. La fonction Lambda envoie un message à une rubrique SNS, à laquelle les utilisateurs peuvent s'abonner pour recevoir des alertes par e-mail ou poursuivre le traitement.

5. Si les notifications Slack sont activées, la fonction Lambda envoie un message à un webhook Slack.

Outils

Services AWS

- AWS CloudFormation fournit un moyen de modéliser un ensemble de ressources AWS et tierces connexes, de les fournir rapidement et de manière cohérente, et de les gérer tout au long de leur cycle de vie, en traitant l'infrastructure comme du code.
- Amazon EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. EventBridge reçoit un événement, un indicateur d'un changement d'environnement, et applique une règle pour acheminer l'événement vers une cible. Les règles associent les événements aux cibles en fonction de la structure de l'événement, appelée schéma d'événements, ou d'un calendrier.
- AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, passant de quelques requêtes par jour à des milliers par seconde. Vous payez uniquement pour le temps de calcul consommé. Aucun frais n'est facturé si votre code n'est pas en cours d'exécution.
- AWS Organizations vous aide à gérer et à gouverner de manière centralisée votre environnement à mesure que vous développez et adaptez vos ressources AWS. AWS Organizations vous permet de créer par programmation de nouveaux comptes AWS et d'allouer des ressources, de regrouper des comptes pour organiser vos flux de travail, d'appliquer des politiques aux comptes ou aux groupes à des fins de gouvernance et de simplifier la facturation en utilisant un mode de paiement unique pour tous vos comptes.
- AWS CloudTrail surveille et enregistre l'activité des comptes dans l'ensemble de votre infrastructure AWS, et vous permet de contrôler les actions de stockage, d'analyse et de correction.
- Amazon Simple Notification Service (Amazon SNS) est un service de messagerie entièrement géré pour les communications (A2A) application-to-application application-to-person et (A2P).

Autres outils

- La bibliothèque AWS Lambda Powertools for Python est un ensemble d'utilitaires fournissant des fonctionnalités de suivi, de journalisation, de métriques et de gestion des événements pour les fonctions Lambda.

Code

Le code de ce modèle se trouve dans le référentiel GitHub AWS Account Closer Notifier.

La solution inclut un CloudFormation modèle qui déploie l'architecture de ce modèle. Il utilise la bibliothèque AWS Lambda Powertools for Python pour assurer la journalisation et le suivi.

Épopées

Déployer l'architecture

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle pour la pile de solutions.	Le CloudFormation modèle de ce modèle se trouve dans la branche principale du GitHub référentiel. Il déploie les rôles IAM, les EventBridge règles, les fonctions Lambda et la rubrique SNS. Pour lancer le modèle, procédez comme suit : 1. Clonez le GitHub référentiel pour obtenir une copie du code de la solution. 2. Ouvrez la console de gestion AWS pour le compte de gestion AWS Organizations. 3. Choisissez la région USA Est (Virginie du Nord`us-east-1`) (), puis ouvrez la CloudFormation console. 4. Créez la pile en utilisant le `account-closure-notifier.yml` modèle	Administrateur AWS

Tâche	Description	Compétences requises
	et en spécifiant les valeurs suivantes : • Nom de la pile : `aws-account-closure-notifier-stack` • `ResourcePrefix` paramètre : `aws-account-closure-notifier` • `SlackNotification` paramètre : si des notifications Slack sont requises, remplacez ce paramètre par. `true` • `SlackWebhookEndpoint` paramètre : si des notifications Slack sont requises, spécifiez l'URL du webhook. Pour plus d'informations sur le lancement d'une CloudFormation pile, consultez la documentation AWS.	

Tâche	Description	Compétences requises
Vérifiez que la solution a été lancée avec succès.	1. Attendez que la CloudFormation pile atteigne le statut CREATE_COMPLETE. 2. Ouvrez la EventBridge console dans `us-east-1` . 3. Vérifiez qu'une nouvelle règle portant ce nom a été créée `aws-account-closure-notifier-event-rule` .	Administrateur AWS

Tâche	Description	Compétences requises
Abonnez-vous à la rubrique SNS.	(Facultatif) Si vous souhaitez vous abonner à la rubrique SNS : 1. Ouvrez la console Amazon SNS et `us-east-1` recherchez le sujet nommé. `aws-account-closure-notifier-sns-topic` 2. Choisissez le nom de la rubrique, puis choisissez Créer un abonnement. 3. Pour Protocole, choisissez E-mail. 4. Pour Endpoint, spécifiez l'adresse e-mail qui doit recevoir la notification, puis choisissez Créer un abonnement. 5. Consultez votre boîte de réception pour y trouver un message provenant d'AWS Notifications. Utilisez le lien contenu dans cet e-mail pour confirmer l'abonnement. Pour plus d'informations sur la configuration des notifications SNS, consultez la documentation Amazon SNS.	Administrateur AWS

Vérifiez la solution

Tâche	Description	Compétences requises
Envoyez un événement de test au bus d'événements par défaut.	Le GitHub référentiel fournit un exemple d'événement que vous pouvez envoyer au bus d'événements EventBridge par défaut à des fins de test. La EventBridge règle réagit également aux événement s qui utilisent la source d'événements personnal iséeaccount.closure.notifier . **Note** Vous ne pouvez pas utiliser la source de l' CloudTrail événement pour envoyer cet événement, car il n'est pas possible d'envoyer un événement en tant que service AWS. Pour envoyer un événement de test : 1. Ouvrez la EventBridge console dansus-east-1 . 2. Dans le volet de navigatio n, sous Bus, choisisse z Bus d'événements,	Administrateur AWS

Tâche	Description	Compétences requises
	puis sélectionnez le bus d'événements par défaut. 3. Choisissez Envoyer des événements. 4. Dans Source de l'événement, entrez `account.closure.notifier` . 5. Pour Type de détails, entrez `AWS API Call via CloudTrail` . 6. Pour les détails de l'événement, copiez et collez le contenu de `tests/dummy-event.json` depuis le GitHub référentiel dans la zone de texte. 7. Choisissez Envoyer pour lancer le flux de notification.	
Vérifiez que la notification par e-mail a bien été reçue.	Consultez la boîte aux lettres qui s'est abonnée à la rubrique SNS pour les notifications. Vous devriez recevoir un e-mail contenant les détails du compte qui a été fermé et du principal qui a effectué l'appel d'API.	Administrateur AWS

Tâche	Description	Compétences requises
Vérifiez que la notification Slack a bien été reçue.	(Facultatif) Si vous avez spécifié une URL de webhook pour le `SlackWebhookEndpoint` paramètre lorsque vous avez déployé le CloudFormation modèle, vérifiez le canal Slack mappé au webhook. Il doit afficher un message contenant les détails du compte fermé et du principal qui a effectué l'appel d'API.	Administrateur AWS

Ressources connexes

- CloseAccount action (référence d'API AWS Organizations)
- RemoveAccountFromOrganization action (référence d'API AWS Organizations)
- Outils puissants AWS Lambda pour Python

Afficher les détails des instantanés EBS pour votre compte AWS ou votre organisation

Créée par Arun Chandapillai (AWS) et Parag Nagwekar (AWS)

Récapitulatif

Ce modèle décrit comment générer automatiquement un rapport à la demande de tous les instantanés Amazon Elastic Block Store (Amazon EBS) enregistrés dans votre compte Amazon Web Services (AWS) ou dans votre unité organisationnelle (UO) dans AWS Organizations.

Amazon EBS est un easy-to-use service de stockage par blocs évolutif et performant conçu pour Amazon Elastic Compute Cloud (Amazon EC2). Un volume EBS fournit un stockage durable et persistant que vous pouvez associer à vos EC2 instances. Vous pouvez utiliser les volumes EBS comme stockage principal pour vos données et effectuer une point-in-time sauvegarde de vos volumes EBS en créant un instantané. Vous pouvez utiliser la console de gestion AWS ou l'interface de ligne de commande AWS (AWS CLI) pour afficher les détails de instantanés EBS spécifiques. Ce modèle fournit un moyen programmatique de récupérer des informations sur tous les instantanés EBS de votre compte AWS ou de votre unité d'organisation.

Vous pouvez utiliser le script fourni par ce modèle pour générer un fichier de valeurs séparées par des virgules (CSV) contenant les informations suivantes sur chaque instantané : ID de compte, ID d'instantané, ID et taille du volume, date à laquelle l'instantané a été pris, ID d'instance et description. Si vos instantanés EBS sont balisés, le rapport inclut également les attributs du propriétaire et de l'équipe.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- AWS CLI version 2 installée et configurée
- Rôle AWS Identity and Access Management (IAM) doté des autorisations appropriées (autorisations d'accès pour un compte spécifique ou pour tous les comptes d'une unité d'organisation si vous prévoyez d'exécuter le script depuis AWS Organizations)

Architecture

Le schéma suivant montre le flux de travail de script qui génère un rapport à la demande sur les instantanés EBS répartis sur plusieurs comptes AWS d'une unité d'organisation.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- Amazon Elastic Block Store (Amazon EBS) fournit des volumes de stockage au niveau des blocs à utiliser avec les instances. EC2
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Organizations est un service de gestion de comptes qui vous aide à consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.

Code

Le code de l'exemple d'application utilisé dans ce modèle est disponible sur GitHub, dans le aws-ebs-snapshots-awsorganizationsréférentiel. Suivez les instructions de la section suivante pour utiliser les fichiers d'exemple.

Épopées

Téléchargez le script

Tâche	Description	Compétences requises
Téléchargez le script Python.	Téléchargez le script GetSnapshotDetailsAllAccountsOU.py depuis le GitHub dépôt.	AWS général

Obtenir les détails des instantanés EBS pour un compte AWS

Tâche	Description	Compétences requises

Exécutez le script python.	Exécutez la commande :
	`python3 getsnapsh otinfo.py --file <output-file>.csv --region <region-name>`
	où `<output-file>` fait référence au fichier de sortie CSV dans lequel vous souhaitez obtenir des informations sur les instantanés EBS placés, et `<region-name>` indique la région AWS dans laquelle les instantanés sont stockés. Par exemple :
	`python3 getsnapsh otinfo.py --file snapshots.csv --region us-east-1`
		AWS général

Obtenez les détails d'un instantané EBS pour une organisation

Tâche	Description	Compétences requises
Exécutez le script python.	Exécutez la commande : `python3 getsnapsh otinfo.py --file <output-file>.csv --role <IAM-role> --region <region-name>`	AWS général

Tâche	Description	Compétences requises
	où `<output-file>` fait référence au fichier de sortie CSV dans lequel vous souhaitez obtenir des informations sur les instantanés EBS placés, `<IAM-role>` est un rôle qui fournit des autorisations pour accéder à AWS Organizations et `<region-name>` correspond à la région AWS dans laquelle les instantanés sont stockés. Par exemple : `python3 getsnapshotinfo.py --file snapshots.csv --role <IAM role> --region us-west-2`	

Ressources connexes

- Documentation Amazon EBS
- Actions Amazon EBS
- Référence d'API Amazon EBS
- Améliorer les performances d'Amazon EBS
- Ressources Amazon EBS
- Tarification instantanée d'EBS

Informations supplémentaires

Types de snapshots EBS

Amazon EBS fournit trois types de snapshots, en fonction de la propriété et de l'accès :

- Vous êtes le propriétaire : par défaut, vous êtes le seul à pouvoir créer des volumes à partir des instantanés que vous possédez.
- Instantanés publics : vous pouvez partager des instantanés publiquement avec tous les autres comptes AWS. Pour créer un instantané public, vous modifiez les autorisations associées à un instantané afin de le partager avec les comptes AWS que vous spécifiez. Les utilisateurs que vous autoriserez pourront ensuite utiliser les instantanés que vous partagez en créant leurs propres volumes EBS, sans affecter votre instantané d'origine. Vous pouvez également mettre vos instantanés non chiffrés à la disposition de tous les utilisateurs d'AWS. Toutefois, pour des raisons de sécurité, vous ne pouvez pas rendre vos instantanés chiffrés accessibles au public. Les instantanés publics présentent un risque de sécurité important en raison de la possibilité d'exposer des données personnelles et sensibles. Nous vous déconseillons vivement de partager vos instantanés EBS avec tous les comptes AWS. Pour plus d'informations sur le partage de snapshots, consultez la documentation AWS.
- Instantanés privés : vous pouvez partager des instantanés en privé avec les comptes AWS individuels que vous spécifiez. Pour partager l'instantané en privé avec des comptes AWS spécifiques, suivez les instructions de la documentation AWS et choisissez Privé pour le paramètre des autorisations. Les utilisateurs qui bénéficient de votre autorisation peuvent utiliser les instantanés que vous partagez pour créer leurs propres volumes EBS, tandis que votre instantané d'origine reste inchangé.

Aperçus et procédures

Le tableau suivant fournit des liens vers des informations supplémentaires sur les instantanés EBS, notamment sur la manière de réduire les coûts de volume EBS en recherchant et en supprimant les instantanés inutilisés, et d'archiver les instantanés rarement consultés qui ne nécessitent pas de récupération fréquente ou rapide.

Pour plus d'informations sur	See
Les instantanés, leurs fonctionnalités et leurs limites	Créez des instantanés Amazon EBS
Comment créer un instantané	Console : créer un instantané CLI AWS : commande create-snapshot Par exemple :

```
aws ec2 create-snapshot --volume-id
 vol-1234567890abcdef0 --description
 " volume snapshot"
```

Supprimer des instantanés (informations générales)	Supprimer un instantané Amazon EBS
Comment supprimer un instantané	Console : Supprimer un instantané CLI AWS : commande delete-snapshot Par exemple :

```
aws ec2 delete-snapshot --snapshot-id
 snap-1234567890abcdef0
```

Archivage des instantanés (informations générales)	Archiver les instantanés Amazon EBS Archive des instantanés Amazon EBS (article de blog)
Comment archiver un instantané	Console : archiver un instantané CLI AWS : modify-snapshot-tier commande
Comment récupérer un instantané archivé	Console : restauration d'un instantané archivé CLI AWS : restore-snapshot-tier commande
Tarification instantanée	Tarification Amazon EBS

FAQ

Quelle est la durée minimale d'archivage ?

La période d’archivage minimale est de 90 jours.

Combien de temps faudrait-il pour restaurer un instantané archivé ?

La restauration d’un instantané archivé du niveau d’archivage au niveau standard peut prendre jusqu’à 72 heures, en fonction de la taille de l’instantané.

Les instantanés archivés sont-ils des instantanés complets ?

Les instantanés archivés sont toujours des instantanés complets.

Quels instantanés un utilisateur peut-il archiver ?

Vous ne pouvez archiver que les instantanés dont vous êtes propriétaire dans votre compte.

Pouvez-vous archiver un instantané du volume de l'appareil racine d'une Amazon Machine Image (AMI) enregistrée ?

Non, vous ne pouvez pas archiver un instantané du volume du périphérique racine d'une AMI enregistrée.

Quelles sont les considérations de sécurité liées au partage d'un instantané ?

Lorsque vous partagez un instantané, vous permettez à d'autres utilisateurs d'accéder à toutes les données qu'il contient. Partagez des instantanés uniquement avec les personnes à qui vous confiez vos données.

Comment partager un instantané avec une autre région AWS ?

Les instantanés sont limités à la région dans laquelle ils ont été créés. Pour partager un instantané avec une autre région, copiez l’instantané dans cette région, puis partagez la copie.

Pouvez-vous partager des instantanés chiffrés ?

Vous ne pouvez pas partager des instantanés chiffrés avec la clé gérée par AWS par défaut. Vous pouvez partager des instantanés chiffrés à l'aide d'une clé gérée par le client uniquement. Lorsque vous partagez un instantané chiffré, vous devez également partager la clé gérée par le client qui a été utilisée pour chiffrer l'instantané.

Qu'en est-il des instantanés non chiffrés ?

Vous pouvez partager des instantanés non chiffrés publiquement.

Plus de modèles

- Automatisez la création de comptes à l'aide de l'accélérateur Landing Zone sur AWS
- Automatisez AWS les opérations d'infrastructure en utilisant Amazon Bedrock
- Automatisez l'évaluation des ressources AWS
- Inventaire automatique AWS des ressources sur plusieurs comptes et régions
- Automatisez le déploiement du portefeuille et des produits AWS Service Catalog à l'aide d'AWS CDK
- Automatisez la gestion dynamique du pipeline pour le déploiement de solutions de correctifs dans les environnements Gitflow en utilisant et AWS Service CatalogAWS CodePipeline
- Automatisez l'ingestion et la visualisation des métriques personnalisées Amazon MWAA sur Amazon Managed Grafana à l'aide de Terraform
- Automatisez les analyses de sécurité pour les charges de travail entre comptes à l'aide d'Amazon Inspector et AWS Security Hub
- Associez automatiquement une politique gérée par AWS pour Systems Manager aux profils d' EC2 instance à l'aide de Cloud Custodian et d'AWS CDK
- Chiffrez automatiquement les volumes Amazon EBS existants et nouveaux
- Centralisez la surveillance à l'aide d'Amazon CloudWatch Observability Access Manager
- Vérifiez la présence de balises obligatoires dans les EC2 instances au lancement
- Nettoyez les ressources de AWS Account Factory for Terraform (AFT) en toute sécurité après la perte du fichier d'état
- Configuration de la journalisation et de la surveillance des événements de sécurité dans votre AWS IoT environnement
- Créez une définition de tâche Amazon ECS et montez un système de fichiers sur des EC2 instances à l'aide d'Amazon EFS
- Créez des règles AWS Config personnalisées à l'aide AWS CloudFormation Guard de politiques
- Personnalisez les noms de rôles par défaut en utilisant des AWS CDK aspects et des trappes d'échappement
- Supprimez les volumes Amazon EBS inutilisés en utilisant AWS Config et AWS Systems Manager
- Déployez et gérez AWS Control Tower les contrôles en utilisant AWS CDK et CloudFormation
- Déployez et gérez les AWS Control Tower contrôles à l'aide de Terraform

- Déployez du code dans plusieurs régions AWS à l'aide d'AWS CodePipeline CodeCommit, AWS et AWS CodeBuild
- Activez Amazon de GuardDuty manière conditionnelle à l'aide de modèles AWS CloudFormation
- Exportez un rapport sur les identités d'AWS IAM Identity Center et leurs attributions en utilisant PowerShell
- Générez un CloudFormation modèle AWS contenant les règles gérées par AWS Config à l'aide de Troposphere
- Donnez aux instances de SageMaker bloc-notes un accès temporaire à un CodeCommit référentiel dans un autre compte AWS
- Intégrez le contrôleur universel Stonebranch à la modernisation du mainframe AWS
- Lancez un CodeBuild projet sur des comptes AWS à l'aide de Step Functions et d'une fonction proxy Lambda
- Migrer les certificats SSL Windows vers un Application Load Balancer à l'aide d'ACM
- Surveiller l'activité de l'utilisateur root IAM
- Optimisez les déploiements multicomptes sans serveur en utilisant les flux de travail et AWS CDK Actions GitHub
- Effectuez des actions personnalisées à partir d' CodeCommit événements AWS
- Préservez l'espace IP routable dans les conceptions VPC multi-comptes pour les sous-réseaux autres que les charges de travail
- Fournissez des rôles IAM avec le moindre privilège en déployant une solution de distribution automatique de rôles
- Enregistrez plusieurs comptes AWS avec une seule adresse e-mail à l'aide d'Amazon SES
- Supprimez EC2 les entrées Amazon Comptes AWSAWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Supprimez EC2 les entrées Amazon dans le même Compte AWS formulaire AWS Managed Microsoft AD en utilisant l' AWS Lambda automatisation
- Rotation des informations d'identification de base de données sans redémarrer les conteneurs
- Exécutez des charges de travail planifiées et pilotées par des événements à grande échelle avec AWS Fargate
- Envoyer des notifications pour une instance de base de données Amazon RDS for SQL Server à l'aide d'un serveur SMTP sur site et de Database Mail
- Configurer un tableau de bord de surveillance Grafana pour AWS ParallelCluster

- Configurez une journalisation centralisée à l'échelle de l'entreprise à l'aide de Terraform
- Marquez automatiquement les pièces jointes à Transit Gateway à l'aide d'AWS Organizations
- Utilisez les requêtes BMC Discovery pour extraire les données de migration afin de planifier la migration
- Vérifiez les meilleures pratiques opérationnelles pour la norme PCI DSS 4.0 en utilisant AWS Config
- Visualisez les rapports d'identification IAM pour tous les comptes AWS à l'aide d'Amazon QuickSight

Messagerie et communications

Rubriques

- Automatisez la configuration de RabbitMQ dans Amazon MQ
- Améliorez la qualité des appels sur les postes de travail des agents dans les centres de contact Amazon Connect
- Plus de modèles

Automatisez la configuration de RabbitMQ dans Amazon MQ

Créée par Yogesh Bhatia (AWS) et Afroz Khan (AWS)

Récapitulatif

Amazon MQ est un service géré de courtage de messages compatible avec de nombreux courtiers de messages populaires. L'utilisation d'Amazon MQ avec RabbitMQ fournit un cluster RabbitMQ robuste géré dans le cloud Amazon Web Services (AWS) avec plusieurs courtiers et options de configuration. Amazon MQ fournit une infrastructure hautement disponible, sécurisée et évolutive, et peut traiter facilement un grand nombre de messages par seconde. Plusieurs applications peuvent utiliser l'infrastructure avec différents hôtes virtuels, files d'attente et échanges. Cependant, la gestion de ces options de configuration ou la création manuelle de l'infrastructure peuvent demander du temps et des efforts. Ce modèle décrit un moyen de gérer les configurations de RabbitMQ en une seule étape, via un seul fichier. Vous pouvez intégrer le code fourni avec ce modèle dans n'importe quel outil d'intégration continue (CI) tel que Jenkins ou Bamboo.

Vous pouvez utiliser ce modèle pour configurer n'importe quel cluster RabbitMQ. Tout ce dont elle a besoin, c'est d'une connectivité au cluster. Bien qu'il existe de nombreuses autres manières de gérer les configurations de RabbitMQ, cette solution crée des configurations d'applications complètes en une seule étape, ce qui vous permet de gérer facilement les files d'attente et autres détails.

Conditions préalables et limitations

Prérequis

- Interface de ligne de commande AWS (AWS CLI) installée et configurée pour pointer vers votre compte AWS (pour obtenir des instructions, consultez la documentation de l'AWS CLI)
- Ansible est installé, vous pouvez donc exécuter des playbooks pour créer la configuration
- rabbitmqadmin installé (pour les instructions, consultez la documentation de RabbitMQ)
- Un cluster RabbitMQ dans Amazon MQ, créé à partir de statistiques Amazon saines CloudWatch

Exigences supplémentaires

- Assurez-vous de créer les configurations pour les hôtes virtuels et les utilisateurs séparément et non dans le cadre de JSON.
- Assurez-vous que le JSON de configuration fait partie du référentiel et qu'il est contrôlé par version.

- La version de la CLI rabbitmqadmin doit être identique à celle du serveur RabbitMQ. La meilleure option est donc de télécharger la CLI depuis la console RabbitMQ.
- Dans le cadre du pipeline, assurez-vous que la syntaxe JSON est validée avant chaque exécution.

Versions du produit

- Version 2.0 de l'interface de ligne de commande AWS
- Version 2.9.13 d'Ansible
- rabbitmqadmin version 3.9.13 (doit être identique à la version du serveur RabbitMQ)

Architecture

Pile technologique source

- Un cluster RabbitMQ exécuté sur une machine virtuelle (VM) locale existante ou sur un cluster Kubernetes (sur site ou dans le cloud)

Pile technologique cible

- Configurations automatisées de RabbitMQ sur Amazon MQ pour RabbitMQ

Architecture cible

Il existe de nombreuses façons de configurer RabbitMQ. Ce modèle utilise la fonctionnalité de configuration d'importation, dans laquelle un seul fichier JSON contient toutes les configurations. Ce fichier applique tous les paramètres et peut être géré par un système de contrôle de version tel que Bitbucket ou Git. Ce modèle utilise Ansible pour implémenter la configuration via la CLI rabbitmqadmin.

Outils

Outils

- rabbitmqadmin est un outil de ligne de commande pour l'API HTTP de RabbitMQ. Il est utilisé pour gérer et surveiller les nœuds et les clusters RabbitMQ.

- Ansible est un outil open source permettant d'automatiser les applications et l'infrastructure informatique.
- L'AWS CLI vous permet d'interagir avec les services AWS à l'aide de commandes dans un shell de ligne de commande.

Services AWS

- Amazon MQ est un service géré de courtage de messages qui facilite la configuration et le fonctionnement des courtiers de messages dans le cloud.
- AWS vous CloudFormation aide à configurer votre infrastructure AWS et à accélérer le provisionnement du cloud grâce à l'infrastructure sous forme de code.

Code

Le fichier de configuration JSON utilisé dans ce modèle et un exemple de playbook Ansible sont fournis en pièce jointe.

Épopées

Créez votre infrastructure AWS

Tâche	Description	Compétences requises
Créez un cluster RabbitMQ sur AWS.	Si vous ne possédez pas encore de cluster RabbitMQ, vous pouvez utiliser AWS CloudFormation pour créer la pile sur AWS. Vous pouvez également utiliser le module Cloudformation d'Ansible pour créer la pile. Avec cette dernière approche, vous pouvez utiliser Ansible pour les deux tâches : créer l'infrastructure RabbitMQ et gérer les configurations.	AWS CloudFormation, Ansible

Création de la configuration Amazon MQ pour RabbitMQ

Tâche	Description	Compétences requises
Créez un fichier de propriétés.	Téléchargez le fichier de configuration JSON (`rabbitmqconfig.jso n`) dans la pièce jointe ou exportez-le depuis la console RabbitMQ. Modifiez-le pour configurer les files d'attente, les échanges et les liaisons. Ce fichier de configuration illustre les éléments suivants : - Crée deux files d'attente : `sample-queue1` et `sample-queue2` - Crée deux échanges : `sample-exchange1` et `sample-exchange2` - Implémente la liaison entre les files d'attente et les échanges Ces configurations sont effectuées sous l'hôte virtuel root (/), comme l'exige rabbitmqadmin.	JSON
Récupérez les détails de l'infrastructure Amazon MQ pour RabbitMQ.	Récupérez les informations suivantes concernant l'infrast ructure RabbitMQ sur AWS : • Nom de l'agent • Hôte RabbitMQ	CLI AWS, Amazon MQ

Tâche	Description	Compétences requises
	• Nom d'utilisateur RabbitMQ (l'utilisateur administrateur créé lors de la création du cluster) • Mot de passe RabbitMQ Vous pouvez utiliser l'AWS Management Console ou l'AWS CLI pour récupérer ces informations. Ces informations permettent au playbook Ansible de se connecter à votre compte AWS et d'utiliser le cluster RabbitMQ pour exécuter des commandes. **Important** L'ordinateur qui exécute le playbook Ansible doit être en mesure d'accéder à votre compte AWS, et l'interface de ligne de commande AWS doit déjà être configurée, comme décrit dans la section Conditions préalables.	

Tâche	Description	Compétences requises

Créez le fichier hosts_var.	Créez le `hosts_var` fichier pour Ansible et assurez-vous que toutes les variables sont définies dans le fichier. Envisagez d'utiliser Ansible Vault pour stocker le mot de passe. Vous pouvez configurer le `hosts_var` fichier comme suit (remplacez les astérisques par vos informations) :
	`RABBITMQ_HOST: "**********.mq.us-east-2.amazonaws.com"`
	`RABBITMQ_VHOST: "/"`
	`RABBITMQ_USERNAME: "admin"`
	`RABBITMQ_PASSWORD: "*******"`
		Ansible

Tâche	Description	Compétences requises
Créez un playbook Ansible.	Pour un exemple de playbook, voir `ansible-rabbit-config.yaml` la pièce jointe. Téléchargez et enregistrez ce fichier. Le playbook Ansible importe et gère toutes les configurations RabbitMQ, telles que les files d'attente, les échanges et les liaisons, dont les applications ont besoin. Suivez les meilleures pratiques relatives aux playbooks Ansible, telles que la sécurisation des mots de passe. Utilisez Ansible Vault pour le chiffrement du mot de passe et récupérez le mot de passe RabbitMQ dans le fichier chiffré.	Ansible

Déploiement de la configuration

Tâche	Description	Compétences requises
Lancez le playbook.	Lancez le playbook Ansible que vous avez créé dans l'épopée précédente. `ansible-playbook ansible-rabbit-config.yaml`	RabbitMQ, Amazon MQ, Ansible

Tâche	Description	Compétences requises
	Vous pouvez vérifier les nouvelles configurations sur la console RabbitMQ.	

Ressources connexes

- Migration de RabbitMQ vers Amazon MQ (article de blog AWS)
- Outil de ligne de commande de gestion (documentation RabbitMQ)
- Création ou suppression d'une CloudFormation pile AWS (documentation Ansible)
- Migration d'applications basées sur des messages vers Amazon MQ pour RabbitMQ (article de blog AWS)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Améliorez la qualité des appels sur les postes de travail des agents dans les centres de contact Amazon Connect

Créée par Ernest Ozdoba (AWS)

Récapitulatif

Les problèmes de qualité des appels sont parmi les problèmes les plus difficiles à résoudre dans les centres de contact. Pour éviter les problèmes de qualité vocale et les procédures de dépannage complexes, vous devez optimiser l'environnement de travail et les paramètres du poste de travail de vos agents. Ce modèle décrit les techniques d'optimisation de la qualité vocale pour les postes de travail des agents dans les centres de contact Amazon Connect. Il fournit des recommandations dans les domaines suivants :

- Ajustements de l'environnement de travail. L'environnement des agents n'affecte pas la façon dont la voix est transmise sur le réseau, mais il a un effet sur la qualité des appels.
- Paramètres du poste de travail de l'agent. Les configurations matérielles et réseau des postes de travail des centres de contact ont des effets significatifs sur la qualité des appels.
- Réglages du navigateur. Les agents utilisent un navigateur Web pour accéder au site Web du panneau de contrôle des contacts Amazon Connect (CCP) et communiquer avec les clients. Les paramètres du navigateur peuvent donc affecter la qualité des appels.

Les composants suivants peuvent également affecter la qualité des appels, mais ils ne relèvent pas du champ d'application du poste de travail et ne sont pas couverts par ce modèle :

- Flux de trafic vers le cloud Amazon Web Services (AWS) via AWS Direct Connect, un VPN à tunnel complet ou un VPN à tunnel partagé
- État du réseau lorsque vous travaillez à l'intérieur ou à l'extérieur du siège social
- Connectivité au réseau téléphonique public commuté (PSTN)
- L'appareil et l'opérateur de téléphonie du client
- Configuration de l'infrastructure de bureau virtuel (VDI)

Pour plus d'informations concernant ces domaines, consultez la section Problèmes courants liés au panneau de configuration des contacts (CCP) et utilisez l'utilitaire de test Endpoint dans la documentation Amazon Connect.

Conditions préalables et limitations

Prérequis

- Les casques et les postes de travail doivent être conformes aux exigences spécifiées dans le guide de l'administrateur Amazon Connect.

Limites

- Les techniques d'optimisation de ce modèle s'appliquent à la qualité vocale douce du téléphone. Ils ne s'appliquent pas lorsque vous configurez l'Amazon Connect CCP en mode téléphone de bureau. Toutefois, vous pouvez utiliser le mode téléphone de bureau si la configuration de votre téléphone logiciel ne fournit pas une qualité vocale acceptable pour l'appel.

Versions du produit

- Pour connaître les navigateurs et les versions pris en charge, consultez le guide de l'administrateur Amazon Connect.

Architecture

Ce modèle est indépendant de l'architecture car il cible les paramètres du poste de travail de l'agent. Comme le montre le schéma suivant, le chemin vocal entre l'agent et le client est affecté par le casque, le navigateur, le système d'exploitation, le matériel du poste de travail et le réseau de l'agent.

Dans les centres de contact Amazon Connect, la connectivité audio de l'utilisateur est établie avec WebRTC. La voix est codée avec le codec audio interactif Opus et cryptée avec le protocole de transport sécurisé en temps réel (SRTP) en transit. D'autres architectures réseau sont possibles, notamment les réseaux VPN, WAN/LAN privés et ISP.

Outils

- Utilitaire de test Amazon Connect Endpoint : cet utilitaire vérifie la connectivité réseau et les paramètres du navigateur.
- Éditeurs de configuration du navigateur pour les paramètres WebRTC :
  - Pour Firefox : about:config
  - Pour Chrome : chrome : //flags

- Analyseur de journaux CCP — Cet outil vous aide à analyser les journaux CCP à des fins de dépannage.

Épopées

Ajuster l'environnement de travail

Tâche	Description	Compétences requises
Réduisez le bruit de fond.	Évitez les environnements bruyants. Si cela n'est pas possible, optimisez l'environnement à l'aide de ces conseils d'insonorisation : • Absorbez le bruit en utilisant des surfaces insonorisantes telles que des rideaux, des tapis et des tissus d'ameublement. • Bloquez le bruit en installant des barrières entre les bureaux. • Envisagez une solution de suppression active du bruit (ANC) telle qu'un générateur de bruit blanc pour favoriser la concentration et garantir l'intimité, ou utilisez des casques antibruit. • Empêchez les échos lors de vos appels. Les grands espaces vides peuvent créer des effets d'écho ou amplifier les bruits. Le fait de recouvrir les	Agent, directeur

Tâche	Description	Compétences requises
	surfaces susceptibles de faire rebondir les sons aidera à réduire les échos.	

Optimisation des paramètres du poste de travail de

Tâche	Description	Compétences requises
Choisissez le bon casque.	• Si l'environnement est bruyant, optez pour un casque stéréo. Le fait de diriger le son vers les deux oreilles aide les agents à mieux se concentrer et à mieux entendre le client, et réduit le bruit global en réduisant la probabilité que les agents élèvent la voix. • Évitez d'utiliser des haut-parleurs ou le système audio intégré à l'ordinateur. Pour une qualité optimale, utilisez un casque filaire dédié aux centres d'appels. Les casques sans fil sont pratiques, mais ils peuvent être une source de retard audio supplémentaire et de réduction de la qualité audio en raison des interférences radio et du transcodage.	Agent, directeur
Utilisez le casque comme prévu.	• Activez les fonctionnalités de suppression active du	Agent

Tâche	Description	Compétences requises
	bruit et d'amélioration de la voix de votre casque si elles sont disponibles. Recherchez des paramètres tels que l'ANC ou l'ANR. Pour obtenir des instructions sur l'activation de ces paramètres, consultez le manuel d'utilisation de votre casque. • Réglez votre microphone pour pouvoir y parler directement. La meilleure position pour votre microphone est juste en dessous de votre menton. Un placement correct peut faire une différence de 10 décibels (dB) dans le niveau sonore. La plupart des casques vous permettent de faire pivoter ou de plier le bras du microphone (perche). Il est donc important de le maintenir au bon endroit lorsque vous parlez. • Certains casques sont équipés de plusieurs microphones et de fonctionnalités avancées telles que la formation de faisceaux vocaux, qui permet de capturer la parole sans bruit. Pour vous assurer que	

Tâche	Description	Compétences requises
	vous utilisez le microphon e principal comme prévu par le fabricant, consultez le manuel d'utilisation de votre appareil.	
Vérifiez les ressources du poste de travail.	Assurez-vous que les ordinateurs de vos agents sont performants. S'ils utilisent des applications tierces consommant des ressource s, il est possible que leurs ordinateurs ne répondent pas à la configuration matériell e minimale requise pour exécuter CCP. Si les agents rencontrent des problèmes de qualité des appels, assurez-vous qu'ils disposent de suffisamment de puissance de traitement (CPU), d'espace disque, de bande passante réseau et de mémoire pour CCP. Les agents doivent fermer toutes les applications et tous les onglets inutiles afin d'améliorer les performan ces du CCP et la qualité des appels.	Administrateur

Tâche	Description	Compétences requises
Configurez les paramètres audio du système d'exploitation.	Les paramètres par défaut pour le niveau du microphone et l'amplification fonctionnent généralement correctement. Si vous trouvez que la voix sortante est faible ou que le microphone capte trop, il peut être utile de régler ces paramètres. Les paramètres du microphone se trouvent dans la configuration audio du système de votre ordinateur (son, entrée sous macOS, propriétés du microphone sous Windows). Vous pouvez accéder aux paramètres avancés susceptibles d'affecter la qualité vocale via des outils système ou des applications tierces. Voici certains des paramètres que vous pouvez vérifier : • Fréquence d'échantillonnage : cette valeur détermine le nombre de fois que le son est sondé par seconde. Le réglage par défaut est généralement de 44 ou 48 kilohertz (kHz). La valeur optimale pour Amazon Connect est de 48 kHz. Vous pouvez utiliser les paramètres de votre navigateur pour	Agent, administrateur

Tâche	Description	Compétences requises
	remplacer la valeur par défaut. Pour plus d'informations, consultez la section de résolution des problèmes du manuel Amazon Connect Administrator Guide. • Gain : cette valeur détermine dans quelle mesure le microphone amplifie le son. Si vous augmentez le gain, votre microphone risque de capter davantage de bruit de fond. • Profondeur de bits — Cette valeur de résolution numérique décrit le nombre de niveaux d'amplitude du son reconnus. Plus la profondeur de bits est élevée, plus le son de la voix est doux. Cependant, de nombreux réseaux téléphoniques traditionnels utilisent la norme PCM (Pulse-Code Modulation), qui ne prend en charge qu'une résolution de 8 bits. • Seuil ouvert — Il s'agit de l'amplitude sonore minimale captée par un microphone. Si vous rencontrez des problèmes de qualité vocale, essayez de rétablir les	

Tâche	Description	Compétences requises
	paramètres par défaut de ces valeurs avant de poursuivre vos recherches. Pour plus d'informations sur ces paramètres et sur d'autres paramètres réglables , consultez le manuel de votre appareil.	

Tâche	Description	Compétences requises
Utilisez un réseau filaire.	Généralement, l'Etherne t filaire a une latence plus faible, il est donc plus facile de fournir la qualité de transmiss ion constante requise pour la transmission de données vocales. Nous recommand ons une bande passante de 100 Ko par appel au minimum. • Si les agents travaillent à domicile, nous recommand ons une connexion filaire via une connexion sans fil. Cela ne devrait pas prendre plus de 150 millisecondes pour entendre le client. Vous pouvez accéder au test de latence d'Amazon Connect depuis l'utilitaire de test Amazon Connect Endpoint. Toutefois, cet utilitaire mesure le délai entre le navigateur et les régions Amazon Connect, et non les clients. La recommand ation de délai unidirect ionnel de 150 millisecondes empêche l'agent et le client de discuter entre eux. La valeur est mesurée de bout en bout, et chaque élément ajoute un délai, y compris la partie de l'appel entre la	Administrateur réseau, agent

Tâche	Description	Compétences requises
	région Amazon Connect et le client. • Si les agents travaillent depuis le bureau, le Wi-Fi d'entreprise est acceptable tant que les paramètres se situent dans la plage recommandée et que le trafic RTP (Real-Time Transport Protocol) est priorisé.	
Mettez à jour les pilotes matériels.	Lorsque vous utilisez un casque USB ou un autre type de casque doté de son propre microprogramme, nous vous recommandons de le mettre à jour avec la dernière version. Les casques simples qui utilisent un port auxiliaire utilisent le périphérique audio intégré de l'ordinateur. Assurez-vous donc que le pilote matériel du système d'exploitation est à jour. Dans de rares cas, une mise à jour du pilote audio peut provoquer des problèmes audio et vous devrez peut-être l'annuler. Pour plus d'informations sur la modification des versions du microprogramme et du pilote, consultez le manuel de votre appareil.	Administrateur

Tâche	Description	Compétences requises
Évitez les hubs USB et les dongles.	Lorsque vous connectez votre casque, évitez les périphéri ques supplémentaires tels que les dongles, les convertisseurs de type port, les hubs et les rallonges. Ces appareils peuvent affecter la qualité des appels. Connectez plutôt votre appareil directement au port de votre ordinateur.	Agent

Tâche	Description	Compétences requises
Consultez les journaux CCP.	Le CCP Log Parser permet de vérifier facilement les journaux des applications. 1. Téléchargez les journaux CCP après un appel. 2. Ouvrez le CCP Log Parser. 3. Glissez et déposez le fichier journal pour le télécharger à des fins d'analyse. 4. Lorsque le journal a été analysé, l'onglet Snapshots & Logs est sélectionné par défaut. Cliquez sur l'onglet Métriques situé à côté pour consulter les informations. 5. Dans la section WebRTC Metrics - audio_input, vérifiez les points suivants : • Le graphique du niveau audio, pour voir si le niveau audio reçu est supérieur à 0. Cela indique qu'un signal audio a été reçu de votre interlocuteur. • Le graphe des paquets pour tous les paquets perdus. Si ce graphique montre des augmentat ions significatives, contactez votre équipe de support informatique.	Agent (compétences avancées)

Tâche	Description	Compétences requises
	6. Dans la section WebRTC Metrics - audio_output, vérifiez les points suivants : • Le graphique du niveau audio, pour confirmer que le son a été envoyé depuis votre appareil. • Le graphe des paquets. Si vous constatez un pic de perte de paquets, signalez-le à votre équipe de support informatique. • Le graphique Jitter Buffer et RTT. Les valeurs de temps aller-retour (RTT) supérieures à 300 affecteront l'expérience d'appel. Signalez-les à votre équipe de support informatique.	

Optimisation des paramètres du navigateur

Tâche	Description	Compétences requises
Restaurez les paramètres WebRTC par défaut.	Le WebRTC doit être activé pour passer des appels téléphoniques informels avec CCP. Nous vous recommandons de conserver les paramètres par défaut pour les fonctionnalités liées au WebRTC.	Administrateur

Tâche	Description	Compétences requises
	• Dans Chrome, vous pouvez définir des drapeaux en accédant à l'URL chrome : // flags. Tapez WebRTC dans le champ de recherche pour trouver les paramètre s susceptibles d'interférer avec le CCP, puis définisse z-les sur Default. • Dans Firefox, tapez about:config dans la barre d'adresse, puis tapez WebRTC dans le champ de recherche de la page de configuration. Les paramètres autres que ceux par défaut apparaissent en gras et peuvent être modifiés sur Par défaut.	
Désactivez les extensions de navigateur lors du dépannage.	Certaines extensions de navigateur peuvent affecter la qualité des appels ou même empêcher les appels de se connecter correctement. Utilisez la fenêtre de navigatio n privée ou le mode privé de votre navigateur et désactivez toutes les extensions. Si cela résout le problème, passez en revue les extensions de votre navigateur et recherchez les modules complémentaires suspects, ou désactivez-les individuellement.	Agent, administrateur

Tâche	Description	Compétences requises
Vérifiez le taux d'échantillonnage du navigateur.	Vérifiez que l'entrée de votre microphone est réglée sur la fréquence d'échantillonnage optimale de 48 kHz. Pour obtenir des instructions, consultez le guide de l'administrateur Amazon Connect.	Agent, administrateur

Ressources connexes

Si vous avez suivi les étapes décrites dans ce modèle mais que vous rencontrez toujours des problèmes de qualité des appels, consultez les ressources suivantes pour obtenir des conseils de résolution des problèmes.

- Passez en revue les problèmes courants du panneau de configuration des contacts (CCP).
- Vérifiez la connexion avec l'utilitaire de test Endpoint.
- Suivez le guide de dépannage pour tout autre problème.

Si votre dépannage et vos ajustements ne résolvent pas le problème de qualité des appels, la cause première est peut-être externe à votre poste de travail. Pour un dépannage plus approfondi, contactez votre équipe de support informatique.

Plus de modèles

- Décomposez les monolithes en microservices en utilisant le CQRS et le sourcing d'événements
- Déployez une ChatOps solution pour gérer les résultats du scan SAST en utilisant Amazon Q Developer dans les applications de chat, les actions personnalisées et AWS CloudFormation
- Intégrez Amazon API Gateway à Amazon SQS pour gérer le REST asynchrone APIs
- Enregistrez plusieurs comptes AWS avec une seule adresse e-mail à l'aide d'Amazon SES
- Exécutez des charges de travail basées sur les messages à grande échelle à l'aide d'AWS Fargate
- Simplifiez le développement et le déploiement des robots Amazon Lex à l'aide d'un flux de travail automatisé

Sécurité, identité et conformité

Rubriques

- Accès Services AWS depuis une application ASP.NET Core à l'aide des pools d'identités Amazon Cognito
- Authentifier Microsoft SQL Server sur Amazon à EC2 l'aide d'AWS Directory Service
- Automatisez la réponse aux incidents et la criminalistique
- Automatisez la correction des résultats AWS Security Hub standard
- Automatisez les analyses de sécurité pour les charges de travail entre comptes à l'aide d'Amazon Inspector et AWS Security Hub
- Auditez automatiquement les groupes de AWS sécurité qui autorisent l'accès depuis des adresses IP publiques
- Réactivez automatiquement AWS à l'aide CloudTrail d'une règle de correction personnalisée dans AWS Config
- Corriger automatiquement les instances et clusters de base de données Amazon RDS non chiffrés
- Faites automatiquement pivoter les clés d'accès utilisateur IAM à grande échelle avec AWS Organizations et AWS Secrets Manager
- Validez et déployez automatiquement les politiques et les rôles IAM dans un compte AWS à l'aide d' CodePipelineIAM Access Analyzer et de macros AWS CloudFormation
- Intégration bidirectionnelle au logiciel AWS Security Hub Jira
- Créez un pipeline pour les images de conteneurs renforcées à l'aide d' EC2 Image Builder et de Terraform
- Centralisez la gestion des clés d'accès IAM dans AWS Organizations à l'aide de Terraform
- Consultez une CloudFront distribution Amazon pour la journalisation des accès, les versions HTTPS et TLS
- Vérifiez les entrées du réseau à hôte unique dans les règles d'entrée du groupe de sécurité pour et IPv4 IPv6
- Choisissez un flux d'authentification Amazon Cognito pour les applications d'entreprise
- Créez des règles AWS Config personnalisées à l'aide AWS CloudFormation Guard de politiques
- Créez un rapport consolidé des découvertes de sécurité de Prowler à partir de plusieurs Comptes AWS
- Supprimez les volumes Amazon EBS inutilisés en utilisant AWS Config et AWS Systems Manager

- Déployez et gérez AWS Control Tower les contrôles en utilisant AWS CDK et CloudFormation
- Déployez et gérez les AWS Control Tower contrôles à l'aide de Terraform
- Déployez un pipeline qui détecte simultanément les problèmes de sécurité dans plusieurs livrables de code
- Déployez des contrôles d'accès basés sur des attributs de détection pour les sous-réseaux publics en utilisant AWS Config
- Déployez des contrôles d'accès préventifs basés sur les attributs pour les sous-réseaux publics
- Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform
- Détectez les instances de base de données Amazon RDS et Aurora dont les certificats CA expirent
- Générez dynamiquement une politique IAM avec IAM Access Analyzer à l'aide de Step Functions
- Activez Amazon de GuardDuty manière conditionnelle à l'aide de modèles AWS CloudFormation
- Activez le chiffrement transparent des données dans Amazon RDS for SQL Server
- Assurez-vous que les équilibreurs de charge AWS utilisent des protocoles d'écoute sécurisés (HTTPS, SSL/TLS)
- Assurez-vous que le chiffrement des données Amazon EMR au repos est activé au lancement
- Assurez-vous qu'un profil IAM est associé à une instance EC2
- Assurez-vous qu'un cluster Amazon Redshift est chiffré lors de sa création
- Exportez un rapport sur les identités d'AWS IAM Identity Center et leurs attributions en utilisant PowerShell
- Surveiller et corriger la suppression planifiée des clés AWS KMS
- Identifiez les compartiments Amazon S3 publics à l'aide AWS Organizations de Security Hub
- Ingérez et analysez les journaux de sécurité AWS dans Microsoft Sentinel
- Gérez AWS Organizations les politiques sous forme de code en utilisant AWS CodePipeline Amazon Bedrock
- Gérez les ensembles AWS IAM Identity Center d'autorisations sous forme de code en utilisant AWS CodePipeline
- Gérez les informations d'identification à l'aide d'AWS Secrets Manager
- Surveiller les ElastiCache clusters pour les groupes de sécurité
- Surveillez les clusters Amazon EMR pour le chiffrement en transit lors du lancement
- Surveillez les ElastiCache clusters Amazon pour le chiffrement au repos
- Surveillez les paires de clés d' EC2 instance à l'aide d'AWS Config

- Surveiller l'activité de l'utilisateur root IAM
- Envoyer une notification lorsqu'un utilisateur IAM est créé
- Empêchez l'accès à Internet au niveau du compte en utilisant une politique de contrôle des services
- Limitez l'accès en fonction de l'adresse IP ou de la géolocalisation en utilisant AWS WAF
- Analysez les référentiels Git pour détecter les informations sensibles et les problèmes de sécurité à l'aide de git-secrets
- Envoyer des alertes depuis AWS Network Firewall vers un canal Slack
- Simplifiez la gestion des certificats privés en utilisant AWS Private CA et AWS RAM
- Désactiver les contrôles standard de sécurité sur tous les comptes membres du Security Hub dans un environnement multi-comptes
- Mettez à jour les informations d'identification de l'AWS CLI depuis AWS IAM Identity Center en utilisant PowerShell
- Utiliser AWS Config pour surveiller les configurations de sécurité d'Amazon Redshift
- Utilisez Network Firewall pour capturer les noms de domaine DNS à partir de l'indication du nom du serveur pour le trafic sortant
- Utilisez Terraform pour activer automatiquement Amazon GuardDuty pour une organisation
- Vérifiez les meilleures pratiques opérationnelles pour la norme PCI DSS 4.0 en utilisant AWS Config
- Vérifiez que les nouveaux clusters Amazon Redshift ont besoin de points de terminaison SSL
- Vérifiez que les nouveaux clusters Amazon Redshift sont lancés dans un VPC
- Plus de modèles

Accès Services AWS depuis une application ASP.NET Core à l'aide des pools d'identités Amazon Cognito

Créée par Bibhuti Sahu (AWS) et Marcelo Barbosa (AWS)

Récapitulatif

Ce modèle explique comment configurer les groupes d'utilisateurs et les groupes d'identités Amazon Cognito, puis permettre à une application ASP.NET Core d'accéder aux AWS ressources après une authentification réussie.

Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour vos applications Web et mobiles. Les deux principaux composants d'Amazon Cognito sont les groupes d'utilisateurs et les groupes d'identités.

Un groupe d'utilisateurs est un répertoire d'utilisateurs dans Amazon Cognito. Avec un groupe d'utilisateurs, vos utilisateurs peuvent se connecter à votre application web ou mobile via Amazon Cognito. Vos utilisateurs peuvent également se connecter via des fournisseurs d'identité sociale tels que Google, Facebook, Amazon ou Apple, et via des fournisseurs d'identité SAML.

Les groupes d'identités Amazon Cognito (identités fédérées) vous permettent de créer des identités uniques pour vos utilisateurs et de les fédérer avec des fournisseurs d'identité. Avec un pool d'identités, vous pouvez obtenir des informations d' AWS identification temporaires à privilèges limités pour accéder à d'autres. Services AWS Avant de commencer à utiliser votre nouveau pool d'identités Amazon Cognito, vous devez attribuer un ou plusieurs rôles AWS Identity and Access Management (IAM) afin de déterminer le niveau d'accès que vous souhaitez accorder aux utilisateurs de votre application à vos ressources. AWS Les groupes d'identités définissent deux types d'identités : les identités authentifiées et celles qui ne le sont pas. Chaque type d'identité peut se voir attribuer son propre rôle dans IAM. Les identités authentifiées appartiennent aux utilisateurs authentifiés par un fournisseur de connexion public (groupes d'utilisateurs Amazon Cognito, Facebook, Google, SAML ou tout autre fournisseur OpenID Connect) ou par un fournisseur de développement (votre propre processus d'authentification principal), tandis que les identités non authentifiées appartiennent généralement aux utilisateurs invités. Lorsqu'Amazon Cognito reçoit une demande d'utilisateur, le service détermine si la demande est authentifiée ou non, détermine quel rôle est associé à ce type d'authentification, puis utilise la politique associée à ce rôle pour répondre à la demande.

Conditions préalables et limitations

Prérequis

- Et Compte AWS avec les autorisations Amazon Cognito et IAM
- Accès aux AWS ressources que vous souhaitez utiliser
- ASP.NET Core 2.0.0 ou version ultérieure

Architecture

Pile technologique

- Amazon Cognito
- Noyau ASP.NET

Architecture cible

Outils

Outils SDKs, et Services AWS

- Visual Studio ou Visual Studio Code
- Amazon. AspNetCore.Identity.Cognito (1.0.4) — paquet NuGet
- AWSSDK.S3 (3.3.110.32) — paquet NuGet
- Amazon Cognito

Code

Le fichier .zip joint contient des exemples de fichiers illustrant les éléments suivants :

- Comment récupérer un jeton d'accès pour l'utilisateur connecté
- Comment échanger un jeton d'accès contre des AWS informations d'identification
- Comment accéder au service Amazon Simple Storage Service (Amazon S3) avec des informations d'identification AWS

Rôle IAM pour les identités authentifiées

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mobileanalytics:PutEvents",
        "cognito-sync:*",
        "cognito-identity:*",
        "s3:ListAllMyBuckets*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Épopées

Création d'un groupe d'utilisateurs Amazon Cognito

Tâche	Description	Compétences requises
Créez un groupe d'utilisateurs.	1. Connectez-vous à la console Amazon Cognito AWS Management Console et ouvrez-la. 2. Choisissez Gérer les groupes d'utilisateurs. 3. Dans l'angle supérieur droit de la page, choisisse z Créer un groupe d'utilisa teurs. 4. Donnez un nom à votre groupe d'utilisateurs, choisissez Revoir les paramètres par défaut, puis Create pool. 5. Notez l'ID de groupe.	Developer

Tâche	Description	Compétences requises
Ajoutez un client d'application.	Vous pouvez créer une application pour utiliser les pages Web intégrées pour l'inscription et la connexion de vos utilisateurs. 1. Dans la barre de navigation située sur le côté gauche de la page du groupe d'utilisateurs, choisissez Clients d'applications sous Paramètres généraux, puis choisissez Ajouter un client d'application. 2. Donnez un nom à votre application, puis choisissez Create app client. 3. Notez l'ID du client de l'application et le secret du client (choisissez Afficher les détails pour voir le secret du client).	Developer

Créer un groupe d’identités Amazon Cognito

Tâche	Description	Compétences requises
Créer un groupe d'identités .	1. Sur la console Amazon Cognito, choisissez Manage Identity Pools, puis Create new identity pool. 2. Entrez un nom pour le pool d'identités.	Developer

Tâche	Description	Compétences requises
	3. Si vous souhaitez activer les identités non authentifiées, sélectionnez cette option dans la section Identités non authentifiées. 4. Dans la section Fournisseurs d'authentification, configurez le pool d'identités Amazon Cognito en définissant l'ID du groupe d'utilisateurs et l'ID du client de l'application, puis choisissez Create Pool.	
Attribuez des rôles IAM au pool d'identités.	Vous pouvez modifier les rôles IAM pour les utilisateurs authentifiés et non authentifiés, ou conserver les valeurs par défaut, puis choisir Autoriser. Pour ce modèle, nous modifierons le rôle IAM authentifié et fournirons l'accès à. `s3:ListAllMyBuckets` Pour un exemple de code, consultez le rôle IAM fourni plus haut dans la section Outils.	Developer

Tâche	Description	Compétences requises
Copiez l'ID du pool d'identités.	Lorsque vous sélectionnez Autoriser à l'étape précédente, la page Getting started with Amazon Cognito s'affiche. Sur cette page, vous pouvez soit copier l'ID du pool d'identités depuis la section Obtenir les informations d'identification AWS, soit choisir Modifier le pool d'identités en haut à droite et copier l'ID du pool d'identités sur l'écran qui s'affiche.	Developer

Configurez votre exemple d'application

Tâche	Description	Compétences requises
Clonez l'exemple d'application Web ASP.NET Core.	1. Clonez l'exemple d'application Web .NET Core à partir de https://github.com/aws/aws-aspnet-cognito-identity-provider.git. 2. Accédez au `samples` dossier et ouvrez la solution. Dans ce projet, vous allez configurer le `appsettings.json` fichier et ajouter une nouvelle page qui affichera tous les compartiments S3 une fois la connexion réussie.	Developer

Tâche	Description	Compétences requises
Ajoutez des dépendances.	Ajoutez une NuGet dépendance pour `Amazon.AspNetCore.Identity.Cognito` à votre application ASP.NET Core.	Developer
Ajoutez les clés et les valeurs de configuration à`appsettings.json` .	Incluez le code du `appsettings.json` fichier joint dans votre `appsettings.json` fichier, puis remplacez les espaces réservés par les valeurs des étapes précédentes.	Developer
Créez un nouvel utilisateur et connectez-vous.	Créez un nouvel utilisateur dans le groupe d'utilisateurs Amazon Cognito et vérifiez qu'il existe sous Utilisateurs et groupes dans le groupe d'utilisateurs.	Developer
Créez une nouvelle page Razor intitulée`MyS3Buckets` .	Ajoutez une nouvelle page ASP.NET Core Razor à votre exemple d'application et remplacez le contenu de `MyS3Bucket.cshtml` et `MyS3Bucket.cshtml.cs` depuis l'exemple ci-joint. Ajoutez la nouvelle page MyS3bucket sous le menu de navigation de la `_Layout.cshtml` page.	Developer

Résolution des problèmes

Problème	Solution
Après avoir ouvert l'exemple d'application depuis le GitHub référentiel, une erreur s'affiche lorsque vous essayez d'ajouter le NuGet package au projet Samples.	Dans le `src` dossier, veillez à supprimer du `Samples.sln` fichier la référence au `Amazon.AspNetCore.Identity.Cognito` projet. Vous pouvez ensuite ajouter le NuGet package au projet Samples sans aucun problème.

Ressources connexes

- Amazon Cognito
- Groupes d'utilisateurs Amazon Cognito
- Groupes d'identités Amazon Cognito
- Exemples de politiques d'accès
- GitHub - Fournisseur d'identité AWS ASP.NET Cognito

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Authentifier Microsoft SQL Server sur Amazon à EC2 l'aide d'AWS Directory Service

Créée par Jagadish Kantubugata (AWS) et Oludahun Bade Ajidahun (AWS)

Récapitulatif

Ce modèle décrit comment créer un répertoire AWS Directory Service et l'utiliser pour authentifier Microsoft SQL Server sur une instance Amazon Elastic Compute Cloud (Amazon EC2).

AWS Directory Service propose plusieurs manières d'utiliser Amazon Cloud Directory et Microsoft Active Directory (AD) avec d'autres services AWS. Les annuaires stockent des informations sur les utilisateurs, les groupes et les appareils, et les administrateurs les utilisent pour gérer l'accès aux informations et aux ressources. AWS Directory Service propose plusieurs choix d'annuaires aux utilisateurs qui souhaitent utiliser leurs applications Microsoft AD ou LDAP (Lightweight Directory Access Protocol) existantes dans le cloud. Il offre également ces mêmes possibilités pour les développeurs qui ont besoin d'un annuaire pour gérer des utilisateurs, des groupes, des appareils et des accès.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un cloud privé virtuel (VPC) avec au moins deux sous-réseaux privés et deux sous-réseaux publics
- Un rôle AWS Identity and Access Management (IAM) permettant d'associer le serveur au domaine

Architecture

Pile technologique source

- La source peut être un Active Directory local

Pile technologique cible

- AWS Directory Service pour Microsoft Active Directory (AWS Managed Microsoft AD)

Architecture cible

Outils

- SQL Server Management Studio (SSMS) est un outil de gestion de Microsoft SQL Server, y compris l'accès, la configuration et l'administration des composants de SQL Server.

Épopées

Configuration d'un répertoire

Tâche	Description	Compétences requises
Sélectionnez AWS Managed Microsoft AD comme type de répertoire.	Sur la console AWS Directory Service, choisissez Directories, Set up directory, AWS Managed Microsoft AD, Next.	DevOps
Sélectionnez l'édition.	Parmi les éditions disponibles pour AWS Managed Microsoft AD, choisissez Standard Edition.	DevOps
Spécifiez le nom DNS du répertoire.	Utilisez un nom de domaine complet. Ce nom se résout uniquement à l'intérieur du VPC. Il n'a pas besoin d'être publiquement résolu.	DevOps
Définir le mot de passe de l’administrateur	Définissez le mot de passe de l'utilisateur administratif par défaut, nommé Admin.	DevOps
Choisissez le VPC et les sous-réseaux.	Choisissez le VPC qui contiendra votre répertoire et les sous-réseaux des contrôleurs de domaine. Si	DevOps

Tâche	Description	Compétences requises
	vous ne possédez pas de VPC avec au moins deux sous-réseaux, vous devez en créer un.	
Vérifiez et lancez le répertoire.	Consultez les informations relatives à l'édition et au prix de l'annuaire, puis choisissez Créer un répertoire.	DevOps

Lancer une EC2 instance pour SQL Server dans le domaine

Tâche	Description	Compétences requises
Sélectionnez une AMI pour SQL Server.	Les étapes de cette épopée relient en toute simplicité une EC2 instance Windows à votre répertoire Microsoft AD géré par AWS. Sur la EC2 console Amazon, choisissez Launch instance, puis sélectionnez l'Amazon Machine Image (AMI) appropriée pour SQL Server.	DevOps, DBA
Configurez les détails d'instance.	Configurez l'instance Windows pour répondre à vos exigences en matière de SQL Server.	DevOps, DBA
Sélectionnez le nom de la paire de clés.	Sélectionnez une paire de clés, puis lancez l'instance.	DevOps, DBA

Tâche	Description	Compétences requises
Ajoutez un réseau.	Vous pouvez choisir le VPC dans lequel votre répertoire a été créé.	DevOps, DBA
Sélectionnez un rôle IAM.	Dans les paramètres avancés, sélectionnez un profil IAM auquel sont `AmazonSSM DirectoryServiceAccess` associées `AmazonSSM ManagedInstanceCore` les politiques gérées par AWS.	DevOps, DBA
Ajoutez un sous-réseau.	Choisissez l'un des sous-réseaux publics de votre VPC. Tout le trafic externe du sous-réseau que vous choisissez doit être acheminé vers une passerelle Internet. Sinon, vous ne pourrez pas vous connecter à l'instance à distance.	DevOps, DBA
Choisissez votre domaine.	Choisissez le domaine que vous avez créé dans la liste du répertoire de jointure des domaines.	DevOps, DBA
Lancez l'instance.	Choisissez Launch instance (Lancer une instance).	DBA

Authentifier SQL Server à l'aide du Directory Service

Tâche	Description	Compétences requises
Connectez-vous en tant qu'administrateur Windows.	Connectez-vous à l' EC2 instance Windows à l'aide des informations d'identification de l'administrateur Windows.	DBA
Connectez-vous à SQL Server.	Lancez SQL Server Management Studio (SSMS) et connectez-vous à SQL Server à l'aide de la méthode d'authentification Windows.	DBA
Créez un identifiant pour l'utilisateur de l'annuaire.	Dans SSMS, choisissez Security, puis choisissez New Login.	DBA
Recherchez un nom de connexion.	Cliquez sur le bouton de recherche situé à côté de la zone de texte de connexion.	DBA
Sélectionnez un lieu.	Dans la boîte de dialogue Sélectionner un utilisateur ou un groupe, choisissez Emplacements.	DBA
Entrez les informations d'identification réseau.	Entrez les informations d'identification réseau complètes que vous avez utilisées lors de la création du service d'annuaire ; par exemple :`test.com\admin` .	DBA
Sélectionnez l'annuaire.	Choisissez le nom du répertoire AWS, puis cliquez sur OK.	DBA

Tâche	Description	Compétences requises
Sélectionnez un nom d'objet.	Sélectionnez l'utilisateur pour lequel vous souhaitez créer l'identifiant. Sélectionnez l'emplacement, choisisse z l'intégralité du répertoire, recherchez l'utilisateur et ajoutez le nom d'utilisateur.	DBA
Connectez-vous à l'instance SQL Server.	Connectez-vous à l' EC2 instance Windows pour SQL Server à l'aide de vos informations d'identification de domaine.	DBA
Connectez-vous à SQL Server en tant qu'utilisateur du domaine.	Lancez SSMS et connectez -vous au moteur de base de données à l'aide de la méthode d'authentification Windows.	DBA

Ressources connexes

- Documentation d'AWS Directory Service (site Web AWS)
- Créez votre répertoire Microsoft AD géré par AWS (documentation AWS Directory Service)
- Rejoignez facilement une EC2 instance Windows (documentation AWS Directory Service)
- Microsoft SQL Server sur AWS (site Web AWS)
- Documentation SSMS (site Web de Microsoft)
- Création d'un identifiant dans SQL Server (documentation SQL Server)

Automatisez la réponse aux incidents et la criminalistique

Créée par Lucas Kauffman (AWS) et Tomek Jakubowski (AWS)

Récapitulatif

Ce modèle déploie un ensemble de processus qui utilisent des AWS Lambda fonctions pour fournir les éléments suivants :

- Un moyen de lancer le processus de réponse aux incidents avec un minimum de connaissances
- Processus automatisés et reproductibles conformes au Guide de réponse aux incidents AWS de sécurité
- Séparation des comptes pour exécuter les étapes d'automatisation, stocker les artefacts et créer des environnements de criminalistique

Le cadre de réponse automatisée aux incidents et de criminalistique suit un processus d'investigation numérique standard comprenant les phases suivantes :

1. Maîtrise
2. Acquisition
3. Examen
4. Analyse

Vous pouvez effectuer des recherches sur des données statiques (par exemple, de la mémoire acquise ou des images de disque) et sur des données dynamiques qui sont actives mais sur des systèmes séparés.

Pour plus de détails, consultez la section Informations supplémentaires.

Conditions préalables et limitations

Prérequis

- Deux Comptes AWS :
  - Compte de sécurité, qui peut être un compte existant, mais qui est de préférence nouveau
  - Compte Forensics, de préférence neuf

- AWS Organizations configurer
- Dans les comptes des membres des Organisations :
  - Le rôle Amazon Elastic Compute Cloud (Amazon EC2) doit disposer d'un accès Get and List à Amazon Simple Storage Service (Amazon S3) et être accessible par. AWS Systems Manager Nous vous recommandons d'utiliser le rôle `AmazonSSMManagedInstanceCore` AWS géré. Notez que ce rôle sera automatiquement attaché à l' EC2 instance Amazon lorsque la réponse aux incidents sera initiée. Une fois la réponse terminée, AWS Identity and Access Management (IAM) supprimera tous les droits relatifs à l'instance.
  - Points de terminaison du cloud privé virtuel (VPC) dans le compte AWS membre et dans la réponse et l'analyse des incidents. VPCs Ces points de terminaison sont : S3 Gateway, EC2 Messages, SSM et SSM Messages.
- AWS Command Line Interface (AWS CLI) installé sur les EC2 instances Amazon. Si les EC2 instances Amazon ne sont pas AWS CLI installées, un accès à Internet sera nécessaire pour que l'instantané du disque et l'acquisition de mémoire fonctionnent. Dans ce cas, les scripts se connecteront à Internet pour télécharger les fichiers AWS CLI d'installation et les installeront sur les instances.

Limites

- Ce cadre ne vise pas à générer des artefacts pouvant être considérés comme des preuves électroniques, susceptibles d'être soumises devant les tribunaux.
- Actuellement, ce modèle ne prend en charge que les instances basées sur Linux exécutées sur une architecture x86.

Architecture

Architecture cible

Outre le compte membre, l'environnement cible comprend deux comptes principaux : un compte Security et un compte Forensics. Deux comptes sont utilisés pour les raisons suivantes :

- Pour les séparer de tous les autres comptes clients afin de réduire le rayon d'explosion en cas d'échec d'une analyse médico-légale
- Pour aider à garantir l'isolation et la protection de l'intégrité des artefacts analysés
- Pour préserver la confidentialité de l'enquête

- Pour éviter les situations dans lesquelles les acteurs de la menace auraient utilisé toutes les ressources immédiatement disponibles pour votre compromission Compte AWS en atteignant les quotas de service et en vous empêchant ainsi d'instancier une EC2 instance Amazon pour effectuer des investigations.

En outre, le fait de disposer de comptes de sécurité et de criminalistique distincts permet de créer des rôles distincts : un intervenant chargé de recueillir les preuves et un enquêteur chargé de les analyser. Chaque rôle aurait accès à son compte distinct.

Le schéma suivant montre uniquement l'interaction entre les comptes. Les détails de chaque compte sont présentés dans les diagrammes suivants, et un schéma complet est joint en annexe.

Le schéma suivant montre le compte du membre.

1. Un événement est envoyé à la rubrique Slack (Amazon Simple Notification Service (Amazon SNS).

Le schéma suivant montre le compte de sécurité.

2. La rubrique Amazon SNS du compte de sécurité lance les événements Forensics.

Le schéma suivant montre le compte Forensics.

Le compte Security est l'endroit où les deux principaux AWS Step Functions flux de travail sont créés pour la mémoire et l'acquisition d'images sur disque. Une fois les flux de travail exécutés, ils accèdent au compte membre qui contient les EC2 instances Amazon impliquées dans un incident, et ils lancent un ensemble de fonctions Lambda qui collecteront un vidage de mémoire ou un vidage de disque. Ces artefacts sont ensuite stockés dans le compte Forensics.

Le compte Forensics conservera les artefacts collectés par le flux de travail Step Functions dans le compartiment Amazon S3 des artefacts d'analyse. Le compte Forensics disposera également d'un pipeline Amazon EC2 Image Builder qui crée une Amazon Machine Image (AMI) d'une instance Forensics. Actuellement, l'image est basée sur la station de travail SANS SIFT.

Le processus de création utilise le VPC de maintenance, qui est connecté à Internet. L'image peut être utilisée ultérieurement pour faire tourner l' EC2 instance Amazon afin d'analyser les artefacts collectés dans le VPC d'analyse.

Le VPC d'analyse n'est pas connecté à Internet. Par défaut, le modèle crée trois sous-réseaux d'analyse privés. Vous pouvez créer jusqu'à 200 sous-réseaux, ce qui correspond au quota du nombre de sous-réseaux dans un VPC, mais ces sous-réseaux doivent être ajoutés aux points de terminaison du VPC pour automatiser l'exécution des commandes dans ceux-ci. AWS Systems Manager Session Manager

Du point de vue des meilleures pratiques, nous vous recommandons d'utiliser AWS CloudTrail et AWS Config de faire ce qui suit :

- Suivez les modifications apportées à votre compte Forensics
- Surveiller l'accès et l'intégrité des artefacts stockés et analysés

Flux de travail

Le schéma suivant montre les étapes clés d'un flux de travail qui inclut le processus et l'arbre de décision, depuis le moment où une instance est compromise jusqu'à son analyse et son confinement.

1. La `SecurityIncidentStatus` balise a-t-elle été définie avec la valeur Analyser ? Dans l'affirmative, procédez comme suit :
   a. Joignez les profils IAM appropriés pour AWS Systems Manager et Amazon S3.
   b. Envoyez un message Amazon SNS à la file d'attente Amazon SNS dans Slack.
   c. Envoyez un message Amazon SNS à la file d'attente. `SecurityIncident`
   d. Appelez la machine d'état Memory and Disk Acquisition.
2. La mémoire et le disque ont-ils été acquis ? Si ce n'est pas le cas, il y a une erreur.
3. Marquez l' EC2 instance Amazon avec le `Contain` tag.
4. Associez le rôle IAM et le groupe de sécurité pour isoler complètement l'instance.

Automatisation et évolutivité

L'objectif de ce modèle est de fournir une solution évolutive pour répondre aux incidents et effectuer des analyses sur plusieurs comptes au sein d'une même AWS Organizations organisation.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS Command Line Interface (AWS CLI) est un outil open source permettant d'interagir Services AWS via des commandes dans votre interface de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.

Code

Pour le code et les conseils spécifiques de mise en œuvre et d'utilisation, consultez le référentiel GitHub Automated Incident Response and Forensics Framework.

Épopées

Déployer les CloudFormation modèles

Tâche	Description	Compétences requises
Déployez CloudFormation des modèles.	Les CloudFormation modèles sont marqués de 1 à 7, le premier mot du nom du script indiquant dans quel compte le modèle doit être déployé. Notez que l'ordre de lancement des CloudForm ation modèles est important. • `1-forensic-AnalysisVPCnS3Buckets.yaml` : Déployé dans le compte Forensics. Il crée les compartiments Amazon S3 et le VPC d'analyse, puis il s'active. CloudTrail • `2-forensic-MaintenanceVPCnEC2ImageBuilderPipeline.yaml` : Déploie le VPC de maintenance et le pipeline de création d'images sur la base de SANS SIFT. • `3-security_IR-Disk_Mem_automation.yaml` : Déploie les fonctions du compte de sécurité qui permettent l'acquisition de disques et de mémoire.	Administrateur AWS

Tâche	Description	Compétences requises
	• `4-security_LiME_Volatility_Factory.yaml` : Lance une fonction de construction pour commencer à créer les modules de mémoire en fonction de l'AMI IDs donnée. Notez que les AMI IDs sont différentes d'un endroit à l'autre Régions AWS. Chaque fois que vous avez besoin de nouveaux modules de mémoire, vous pouvez réexécuter ce script avec la nouvelle AMI IDs. Envisagez de l'intégrer à vos pipelines de création d'AMI Golden Image (s'ils sont utilisés dans votre environnement). • `5-member-IR-automation.yaml` : crée la fonction d'automatisation de la réponse aux incidents des membres, qui lance le processus de réponse aux incidents. Il permet de partager les volumes Amazon Elastic Block Store (Amazon EBS) entre les comptes, de les publier automatiquement sur les canaux Slack pendant le processus de réponse aux incidents, de lancer le	

Tâche	Description	Compétences requises
	processus de criminalistique et d'isoler les instances une fois le processus terminé. • `6-forensic-artifact-s3-policies.yaml` : Une fois que tous les scripts ont été déployés, ce script fixe les autorisations requises pour toutes les interactions entre comptes. • `7-security-IR-vpc.yaml` : Configure un VPC utilisé pour le traitement du volume de réponse aux incidents. Pour lancer le cadre de réponse aux incidents pour une EC2 instance Amazon spécifique, créez une balise avec la clé `SecurityIncidentStatus` et la valeur`Analyze`. Cela lancera la fonction Lambda du membre qui lancera automatiquement l'isolation et l'acquisition de mémoire ainsi que l'acquisition de disques.	

Tâche	Description	Compétences requises
Faites fonctionner le framework.	La fonction Lambda rebalisera également l'actif à la fin (ou en cas de panne) avec. `Contain` Cela initie le confinement, qui isole complètement l'instanc e avec un groupe de sécurité sans entrant/sortant et avec un rôle IAM qui interdit tout accès. Suivez les étapes indiquées dans le GitHub référentiel.	Administrateur AWS

Déployez des actions Security Hub personnalisées

Tâche	Description	Compétences requises
Déployez les actions personnalisées du Security Hub à l'aide d'un CloudForm ation modèle.	Pour créer une action personnalisée afin de pouvoir utiliser la liste déroulante de Security Hub, déployez le `Modules/SecurityHu b Custom Actions/S ecurityHubCustomAc tions.yaml` CloudForm ation modèle. Modifiez ensuite le `IRAutomation` rôle dans chacun des comptes membres pour permettre à la fonction Lambda qui exécute l'action d'assumer le `IRAutomat ion` rôle. Pour plus d'informa tions, consultez le GitHub référentiel.	Administrateur AWS

Ressources connexes

- AWS Guide de réponse aux incidents de sécurité

Informations supplémentaires

En utilisant cet environnement, une équipe du centre des opérations de sécurité (SOC) peut améliorer son processus de réponse aux incidents de sécurité en procédant comme suit :

- Avoir la capacité d'effectuer des analyses dans un environnement séparé afin d'éviter la compromission accidentelle des ressources de production
- Disposer d'un processus standardisé, reproductible et automatisé pour le confinement et l'analyse.
- Donner à tout propriétaire ou administrateur de compte la possibilité de lancer le processus de réponse aux incidents avec un minimum de connaissances sur l'utilisation des balises
- Disposer d'un environnement propre et normalisé pour effectuer l'analyse des incidents et la criminalistique sans le bruit d'un environnement plus vaste
- Capacité à créer plusieurs environnements d'analyse en parallèle
- Concentrer les ressources du SOC sur la réponse aux incidents plutôt que sur la maintenance et la documentation d'un environnement de criminalistique dans le cloud
- Passer d'un processus manuel à un processus automatisé pour atteindre l'évolutivité
- Utilisation CloudFormation de modèles pour des raisons de cohérence et pour éviter les tâches répétitives

De plus, vous évitez d'utiliser une infrastructure persistante et vous payez pour les ressources lorsque vous en avez besoin.

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Automatisez la correction des résultats AWS Security Hub standard

Créée par Chandini Penmetsa (AWS) et Aromal Raj Jayarajan (AWS)

Récapitulatif

Avec AWS Security Hub, vous pouvez activer la vérification des meilleures pratiques standard, telles que les suivantes :

- AWS Bonnes pratiques fondamentales en matière de sécurité
- Indice de référence AWS des fondations du CIS
- Norme de sécurité des données de l’industrie des cartes de paiement (PCI DSS)

Chacune de ces normes comporte des contrôles prédéfinis. Security Hub vérifie le contrôle d'une donnée Compte AWS et publie les résultats.

AWS Security Hub envoie tous les résultats à Amazon EventBridge par défaut. Ce modèle fournit un contrôle de sécurité qui déploie une EventBridge règle pour identifier les résultats standard des meilleures pratiques de sécurité AWS fondamentales. La règle identifie les résultats suivants concernant le dimensionnement automatique, les clouds privés virtuels (VPCs), Amazon Elastic Block Store (Amazon EBS) et Amazon Relational Database Service (Amazon RDS AWS), conformément à la norme des meilleures pratiques de sécurité fondamentales :

- [AutoScaling.1] Les groupes Auto Scaling associés à un équilibreur de charge doivent utiliser des contrôles de santé de l'équilibreur de charge
- [EC2.2] Le groupe de sécurité VPC par défaut ne doit pas autoriser le trafic entrant et sortant
- [EC2.6] La journalisation des flux VPC doit être activée dans tous VPCs
- [EC2.7] Le chiffrement par défaut d'EBS doit être activé
- [RDS.1] Les instantanés RDS doivent être privés
- [RDS.6] Une surveillance améliorée doit être configurée pour les instances de base de données et les clusters RDS
- [RDS.7] La protection contre la suppression des clusters RDS doit être activée

La EventBridge règle transmet ces résultats à une AWS Lambda fonction qui les corrige. La fonction Lambda envoie ensuite une notification contenant des informations de correction à une rubrique Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Adresse e-mail à laquelle vous souhaitez recevoir la notification de correction
- Security Hub et AWS Config activé à l' Région AWS endroit où vous souhaitez déployer le contrôle
- Un bucket Amazon Simple Storage Service (Amazon S3) situé dans la même région que le contrôle pour télécharger le code AWS Lambda

Limites

- Ce contrôle de sécurité corrige automatiquement les nouvelles découvertes signalées après le déploiement du contrôle de sécurité. Pour corriger les résultats existants, sélectionnez-les manuellement sur la console Security Hub. Ensuite, sous Actions, sélectionnez l'action AFSBPRemedypersonnalisée créée dans le cadre du déploiement par AWS CloudFormation.
- Ce contrôle de sécurité est régional et doit être déployé dans le pays Régions AWS que vous avez l'intention de surveiller.
- Pour la solution EC2 1.6, pour activer les journaux de flux VPC, un groupe de journaux CloudWatch Amazon Logs sera créé `/VpcFlowLogs/vpc_id` au format. S'il existe un groupe de journaux portant le même nom, le groupe de journaux existant sera utilisé.
- Pour la solution EC2 1.7, pour activer le chiffrement par défaut d'Amazon EBS, la clé default AWS Key Management Service (AWS KMS) est utilisée. Cette modification empêche l'utilisation de certaines instances qui ne prennent pas en charge le chiffrement.

Architecture

Pile technologique cible

- fonction Lambda
- Rubrique Amazon SNS
- EventBridge règle
- AWS Identity and Access Management Rôles (IAM) pour la fonction Lambda, les journaux de flux VPC et la surveillance améliorée d'Amazon RDS

Architecture cible

Automatisation et mise à l'échelle

Si vous l'utilisez AWS Organizations, vous pouvez l'utiliser AWS CloudFormation StackSetspour déployer ce modèle sur plusieurs comptes que vous souhaitez qu'il surveille.

Outils

- AWS CloudFormationest un service qui vous aide à modéliser et à configurer AWS des ressources en utilisant l'infrastructure sous forme de code.
- Amazon EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications logicielles en tant que service (SaaS) Services AWS, et achemine ces données vers des cibles telles que les fonctions Lambda.
- AWS Lambdaprend en charge l'exécution de code sans provisionner ni gérer de serveurs.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif que vous pouvez utiliser pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Bonnes pratiques

- Neuf AWS Security Hub bonnes pratiques
- AWS Norme sur les meilleures pratiques de sécurité fondamentales

Épopées

Déployez le contrôle de sécurité

Tâche	Description	Compétences requises
Définissez le compartiment Amazon S3.	Sur la console Amazon S3, choisissez ou créez un compartiment Amazon S3 avec un nom unique qui ne contient pas de barres obliques. Le nom d'un compartiment Amazon S3 est unique au monde et l'espace de noms est partagé par tous Comptes AWS. Votre compartiment Amazon S3 doit se trouver dans la même région que les résultats du Security Hub en cours d'évaluation.	Architecte du cloud
Téléchargez le code Lambda dans le compartiment Amazon S3.	Téléchargez le fichier .zip de code Lambda fourni dans la section « Pièces jointes » dans le compartiment Amazon S3 défini.	Architecte du cloud
Déployez le AWS CloudForm ation modèle.	Déployez le AWS CloudForm ation modèle fourni en pièce jointe à ce modèle. Dans l'épopée suivante, indiquez les valeurs des paramètres.	Architecte du cloud

Complétez les paramètres dans le AWS CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment Amazon S3.	Entrez le nom du compartiment Amazon S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud
Fournissez le préfixe Amazon S3.	Indiquez l'emplacement du fichier .zip du code Lambda dans votre compartiment Amazon S3, sans barres obliques (par exemple,). `<directory>/<file-name>.zip`	Architecte du cloud
Indiquez l'ARN de la rubrique Amazon SNS.	Si vous souhaitez utiliser une rubrique Amazon SNS existante pour les notifications de correction, indiquez le nom de ressource Amazon (ARN) de la rubrique Amazon SNS. Si vous souhaitez utiliser une nouvelle rubrique Amazon SNS, conservez la valeur `None` (valeur par défaut).	Architecte du cloud
Indiquez une adresse e-mail.	Indiquez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications de correction (nécessaire uniquement lorsque vous souhaitez AWS CloudFormation créer la rubrique Amazon SNS).	Architecte du cloud

Tâche	Description	Compétences requises
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événement s d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud
Fournissez l'ARN du rôle IAM pour les journaux de flux VPC.	Indiquez l'ARN du rôle IAM à utiliser pour les journaux de flux VPC. Si vous entrez`None`, AWS CloudFormation crée un rôle IAM et l'utilise.	Architecte du cloud
Fournissez l'ARN du rôle IAM pour Amazon RDS Enhanced Monitoring.	Indiquez l'ARN du rôle IAM à utiliser pour Amazon RDS Enhanced Monitoring. Si vous entrez`None`, AWS CloudForm ation crée un rôle IAM et l'utilise.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'abonnement Amazon SNS.	Lorsque le modèle est déployé avec succès, si une nouvelle rubrique Amazon SNS a été	Architecte du cloud

Tâche	Description	Compétences requises
	créée, un message d'abonnement est envoyé à l'adresse e-mail que vous avez fournie. Pour recevoir des notifications de correction, vous devez confirmer cet e-mail d'abonnement.	

Ressources connexes

- Création d'une pile sur la AWS CloudFormation console
- AWS Lambda website
- AWS Security Hub documentation

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Automatisez les analyses de sécurité pour les charges de travail entre comptes à l'aide d'Amazon Inspector et AWS Security Hub

Créée par Ramya Pulipaka (AWS) et Mikesh Khanal (AWS)

Récapitulatif

Ce modèle décrit comment détecter automatiquement les vulnérabilités dans les charges de travail entre comptes sur le cloud Amazon Web Services (AWS).

Le modèle permet de créer un calendrier pour les scans basés sur l'hôte des instances Amazon Elastic Compute Cloud EC2 (Amazon) groupées par balises ou pour les scans Amazon Inspector basés sur le réseau. Une AWS CloudFormation pile déploie toutes les AWS ressources et tous les services nécessaires dans votre Comptes AWS environnement.

Les résultats d'Amazon Inspector sont exportés vers AWS Security Hub et fournissent des informations sur les vulnérabilités de vos comptes Régions AWS, de vos clouds privés virtuels (VPCs) et de vos EC2 instances Amazon. Vous pouvez recevoir ces résultats par e-mail ou créer une rubrique Amazon Simple Notification Service (Amazon SNS) qui utilise un point de terminaison HTTP pour envoyer les résultats aux outils de billetterie, aux logiciels de gestion des informations et des événements de sécurité (SIEM) ou à d'autres solutions de sécurité tierces.

Conditions préalables et limitations

Prérequis

- Active Comptes AWS qui héberge des charges de travail entre comptes, y compris un compte d'audit central.
- Adresse e-mail existante pour recevoir les notifications par e-mail d'Amazon SNS.
- Point de terminaison HTTP existant utilisé par les outils de billetterie, les logiciels SIEM ou d'autres solutions de sécurité tierces.
- Security Hub, activé et configuré. Vous pouvez utiliser ce modèle sans Security Hub, mais nous vous recommandons d'utiliser Security Hub en raison des informations qu'il génère. Pour plus d'informations, consultez la section Configuration de Security Hub dans la documentation du Security Hub.
- Un agent Amazon Inspector doit être installé sur chaque EC2 instance que vous souhaitez scanner. Vous pouvez installer l'agent Amazon Inspector sur plusieurs EC2 instances à l'aide d'AWS Systems Manager Run Command.

Compétences

- Expérience d'utilisation `self-managed` et `service-managed` autorisations pour les stack sets in CloudFormation. Si vous souhaitez utiliser `self-managed` les autorisations pour déployer des instances de stack sur des comptes spécifiques dans des régions spécifiques, vous devez créer les rôles AWS Identity and Access Management (IAM) requis. Si vous souhaitez utiliser `service-managed` des autorisations pour déployer des instances de stack sur des comptes gérés par AWS Organizations des régions spécifiques, vous n'avez pas besoin de créer les rôles IAM requis. Pour plus d'informations, consultez la section Création d'un ensemble de piles dans la CloudFormation documentation.

Limites

- Si aucune balise n'est appliquée aux EC2 instances Amazon d'un compte, Amazon Inspector analyse toutes les instances de ce compte.
- Les ensembles de CloudFormation piles et le `onboard-audit-account.yaml` fichier (joint) doivent être déployés dans la même région.
- L'approche de ce modèle peut évoluer en deçà du quota de publication de 30 000 transactions par seconde (TPS) pour un sujet Amazon SNS dans la région USA Est (Virginie du Nord) `us-east-1` (), bien que les limites varient d'une région à l'autre. Pour évoluer plus efficacement et éviter les pertes de données, nous vous recommandons d'utiliser Amazon Simple Queue Service (Amazon SQS) avant la rubrique Amazon SNS.

Architecture

Le schéma suivant illustre le flux de travail permettant de scanner automatiquement EC2 les instances Amazon.

Le flux de travail se compose des étapes suivantes :

1. Une EventBridge règle Amazon utilise une expression cron pour s'auto-initier selon un calendrier spécifique et lance Amazon Inspector.
2. Amazon Inspector analyse les EC2 instances Amazon étiquetées dans le compte.
3. Amazon Inspector envoie les résultats à Security Hub, qui génère des informations pour le flux de travail, la priorisation et les mesures correctives.

4. Amazon Inspector envoie également le statut de l'évaluation à une rubrique Amazon SNS du compte d'audit. Une AWS Lambda fonction est invoquée si un `findings reported` événement est publié dans la rubrique Amazon SNS.
5. La fonction Lambda récupère, formate et envoie les résultats à une autre rubrique Amazon SNS du compte d'audit.
6. Les résultats sont envoyés aux adresses e-mail abonnées à la rubrique Amazon SNS. Les informations complètes et les recommandations sont envoyées au format JSON au point de terminaison HTTP abonné.

Outils

- AWS CloudFormationvous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications.
- AWS CloudFormation StackSetsétend les fonctionnalités des piles en vous permettant de créer, de mettre à jour ou de supprimer des piles sur plusieurs comptes et régions en une seule opération.
- AWS Control Towercrée une couche d'abstraction ou d'orchestration qui combine et intègre les fonctionnalités de plusieurs autres Services AWS, notamment AWS Organizations.
- Amazon EventBridge est un service de bus d'événements sans serveur qui permet de connecter facilement vos applications à des données provenant de diverses sources.
- AWS Lambdaest un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs.
- AWS Security Hubvous fournit une vue complète de votre état de sécurité dans AWS et vous aide à vérifier que votre environnement est conforme aux normes du secteur de la sécurité et aux meilleures pratiques.
- Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages aux abonnés par les éditeurs.

Épopées

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle dans le compte d'audit.	Téléchargez et enregistrez le `onboard-audit-account.yaml` fichier (joint) sur un chemin local sur votre ordinateur. Connectez-vous à votre compte d'audit, ouvrez la CloudFormation console, puis choisissez Create stack. AWS Management Console Choisissez Préparer le modèle dans la section Conditions préalables, puis sélectionnez Le modèle est prêt. Choisissez la source du modèle dans la section Spécifier le modèle, puis choisissez Le modèle est prêt. Téléchargez le `onboard-audit-account.yaml` fichier, puis configurez les options restantes en fonction de vos besoins. Assurez-vous de configurer les paramètres d'entrée suivants : • `DestinationEmailAddress` — Entrez une	Développeur, ingénieur en sécurité

Tâche	Description	Compétences requises
	adresse e-mail pour recevoir les résultats. • `HTTPEndpoint` — Fournissez un point de terminaison HTTP pour vos outils de billetterie ou de SIEM. **Note** Vous pouvez également déployer le CloudFormation modèle en utilisant AWS Command Line Interface (AWS CLI). Pour plus d'informations à ce sujet, consultez la section Création d'une pile dans la CloudFormation documentation.	
Confirmez l'abonnement Amazon SNS.	Ouvrez votre boîte e-mail et choisissez Confirmer l'abonnement dans l'e-mail que vous recevez d'Amazon SNS. Cela ouvre une fenêtre de navigateur Web et affiche la confirmation de l'abonnement.	Développeur, ingénieur en sécurité

Créez des ensembles de CloudFormation piles pour automatiser le calendrier de scan d'Amazon Inspector

Tâche	Description	Compétences requises
Créez des ensembles de piles dans le compte d'audit.	Téléchargez le `vulnerability-management-program.yaml` fichier (joint) sur un chemin local de votre ordinateur. Sur la CloudFormation console, choisissez Afficher les stacksets, puis Create. StackSet Choisissez Le modèle est prêt, choisissez Télécharger un fichier modèle, puis téléchargez le **`vulnerability-management-program.yaml`** fichier. Si vous souhaitez utiliser `self-managed` des autorisations, suivez les instructions de la section Créer un ensemble de piles avec des autorisations autogérées dans la CloudFormation documentation. Cela crée des ensembles de piles dans des comptes individuels. Si vous souhaitez utiliser des `service-managed` autorisations, suivez les instructions de la section	Développeur, ingénieur en sécurité

Tâche	Description	Compétences requises
	Créer un ensemble de piles avec des autorisations gérées par les services dans la CloudFormation documentation. Cela crée des ensembles de piles dans l'ensemble de votre organisation ou dans des unités organisationnelles spécifiques (OUs). Assurez-vous que les paramètres d'entrée suivants sont configurés pour vos ensembles de piles : • `AssessmentSchedule` — Le calendrier d' EventBridge utilisation des expressions cron. • `Duration`— La durée de l'évaluation Amazon Inspector exécutée en secondes. • `CentralSNSTopicArn` — Le nom de ressource Amazon (ARN) pour la rubrique principale d'Amazon SNS. • `Tagkey`— La clé de balise associée au groupe de ressources. • `Tagvalue`— La valeur de balise associée au groupe de ressources.	

Tâche	Description	Compétences requises
	Si vous souhaitez scanner des EC2 instances Amazon dans le compte d'audit, vous devez exécuter le `vulnerability-management-program.yaml` fichier sous forme de CloudFormation pile dans le compte d'audit.	
Validez la solution.	Vérifiez que vous recevez les résultats par e-mail ou par point de terminaison HTTP selon le calendrier que vous avez spécifié pour Amazon Inspector.	Développeur, ingénieur en sécurité

Ressources connexes

- Élargissez vos tests de vulnérabilité en matière de sécurité avec Amazon Inspector (article de AWS blog)
- Corriger automatiquement les résultats de sécurité d'Amazon Inspector (article de AWS blog)
- Comment simplifier la configuration de l'évaluation de la sécurité à l'aide EC2 d' AWS Systems Manager Amazon et d'Amazon Inspector (article de AWS blog)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Auditez automatiquement les groupes de AWS sécurité qui autorisent l'accès depuis des adresses IP publiques

Créée par Eugene Shifer (AWS) et Stephen DiCato (AWS)

Récapitulatif

En tant que meilleure pratique en matière de sécurité, il est essentiel de limiter l'exposition des AWS ressources à ce qui est absolument nécessaire. Par exemple, les serveurs Web destinés au grand public doivent autoriser l'accès entrant depuis Internet, mais l'accès aux autres charges de travail doit être limité à des réseaux spécifiques afin de réduire les risques inutiles. Les groupes de sécurité dans Amazon Virtual Private Cloud (Amazon VPC) constituent un contrôle efficace pour vous aider à limiter l'accès aux ressources. Cependant, l'évaluation des groupes de sécurité peut s'avérer une tâche fastidieuse, en particulier dans les architectures multi-comptes. AWS Config les règles et les AWS Security Hub contrôles peuvent vous aider à identifier les groupes de sécurité qui autorisent l'accès depuis l'Internet public (0.0.0.0/0) à des protocoles de communication réseau spécifiques, tels que Secure Shell (SSH), HTTP, HTTPS et le protocole RDP (Windows Remote Desktop Protocol). Toutefois, ces règles et contrôles ne sont pas applicables si les services s'exécutent sur des ports non standard ou si l'accès est limité à certaines adresses IP publiques. Par exemple, cela peut se produire lorsqu'un service Web est associé au port TCP 8443 au lieu du port TCP standard 443. Cela peut également se produire lorsque les développeurs ont accès au serveur depuis leur réseau domestique, par exemple à des fins de test.

Pour résoudre ce problème, vous pouvez utiliser la solution d'infrastructure en tant que code (IaC) fournie dans ce modèle pour identifier les groupes de sécurité qui autorisent l'accès à partir de toute adresse IP non privée (non conforme à la RFC 1918) à n'importe quelle charge de travail au sein de votre entreprise ou de votre Compte AWS organisation. AWS Le AWS CloudFormationmodèle fournit une AWS Config règle personnalisée, une AWS Lambdafonction et les autorisations nécessaires. Vous pouvez le déployer sous la forme d'une pile dans un seul compte ou d'une pile dans l'ensemble de l'organisation, gérée via AWS Organizations.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Expérience d'utilisation GitHub

- Si vous effectuez un déploiement en un seul Compte AWS :
  - Autorisations pour créer des CloudFormation piles
  - AWS Config configuré dans le compte cible
  - (Facultatif) Security Hub configuré dans le compte cible
- Si vous effectuez un déploiement au sein d'une AWS organisation :
  - Autorisations pour créer des ensembles de CloudFormation piles
  - Security Hub configuré avec AWS Organizations intégration
  - AWS Config configurer dans les comptes sur lesquels vous déployez cette solution
  - Désignez un Compte AWS administrateur délégué pour AWS Config Land Security Hub

Limites

- Si vous effectuez un déploiement sur un compte individuel sur lequel Security Hub n'est pas activé, vous pouvez l'utiliser AWS Config pour évaluer les résultats.
- Si vous effectuez un déploiement dans une organisation qui ne dispose pas d'un administrateur délégué pour AWS Config Security Hub, vous devez vous connecter aux comptes des membres individuels pour consulter les résultats.
- Si vous avez l' AWS Control Tower habitude de gérer et de gouverner les comptes de votre organisation, déployez l'iAc selon ce modèle en utilisant Customizations for AWS Control Tower (CfCT). L'utilisation de la CloudFormation console créerait une dérive de AWS Control Tower configuration et obligerait à réinscrire les unités organisationnelles (OUs) ou les comptes gérés.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité par région, voir Services AWS par région. Pour des points de terminaison spécifiques, consultez la page Points de terminaison et quotas du service, puis choisissez le lien vers le service.

Architecture

Déploiement chez un individu Compte AWS

Le schéma d'architecture suivant montre le déploiement des AWS ressources au sein d'une même architecture Compte AWS. Vous approvisionnez les ressources à l'aide d'un CloudFormation modèle directement via la CloudFormation console. Si Security Hub est activé, vous pouvez consulter les résultats dans Security Hub AWS Config ou dans Security Hub. Si Security Hub n'est pas activé, vous pouvez afficher les résultats uniquement dans AWS Config.

Le schéma suivant illustre le flux de travail suivant :

1. Vous créez une CloudFormation pile. Cela déploie une fonction Lambda et AWS Config une règle. La règle et la fonction sont configurées avec les autorisations AWS Identity and Access Management (IAM) requises pour publier des évaluations de ressources dans AWS Config des journaux.
2. La AWS Config règle fonctionne en mode d'évaluation détective et invoque la fonction Lambda toutes les 24 heures.
3. La fonction Lambda évalue les groupes de sécurité et envoie des mises à jour à. AWS Config
4. Security Hub reçoit tous les AWS Config résultats.
5. Vous pouvez consulter les résultats dans Security Hub ou dans AWS Config, selon les services que vous avez configurés dans le compte.

Déploiement au AWS sein d'une organisation

Le schéma suivant montre le déploiement du modèle sur plusieurs comptes gérés via AWS Organizations et AWS Control Tower. Vous déployez le CloudFormation modèle via CfCT. Les résultats de l'évaluation sont centralisés dans Security Hub, dans le compte administrateur délégué. La section du diagramme consacrée au AWS CodePipeline flux de travail montre les étapes d'arrière-plan qui se produisent lors du déploiement de CfCT.

Le schéma suivant illustre le flux de travail suivant :

1. Dans le compte de gestion, vous chargez un fichier compressé (ZIP) du modèle iAC dans un bucket Amazon Simple Storage Service (Amazon S3) déployé par CfCT.
2. Le pipeline CFct décompresse le fichier, exécute les vérifications cfn-nag (GitHub) et déploie le modèle sous forme de stack set. CloudFormation
3. En fonction de la configuration que vous spécifiez dans le fichier manifeste CFct, CloudFormation StackSets déploie les piles dans des comptes individuels ou spécifiées. OUs Cela déploie une fonction Lambda et AWS Config une règle dans les comptes cibles. La règle et la fonction sont configurées avec les autorisations IAM requises pour publier des évaluations de ressources dans AWS Config des journaux.
4. La AWS Config règle fonctionne en mode d'évaluation détective et invoque la fonction Lambda toutes les 24 heures.
5. La fonction Lambda évalue les groupes de sécurité et envoie des mises à jour à. AWS Config

6. AWS Config transmet tous les résultats à Security Hub.
7. Les résultats du Security Hub sont agrégés dans le compte d'administrateur délégué.
8. Vous pouvez consulter les résultats agrégés dans Security Hub dans le compte d'administrateur délégué.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.
- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps. Une AWS Config règle définit vos paramètres de configuration idéaux pour une ressource et AWS Config permet d'évaluer si vos AWS ressources sont conformes aux conditions de la règle.
- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives. Les personnalisations pour AWS Control Tower (CfCT) vous aident à personnaliser votre zone AWS Control Tower d'atterrissage et à respecter les AWS meilleures pratiques. Les personnalisations de cette solution sont mises en œuvre par le biais CloudFormation de modèles et de politiques de contrôle des AWS Organizations services (SCPs).
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.

Autres outils

- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Détecter les groupes de sécurité vulnérables.

Bonnes pratiques

Nous vous recommandons de suivre les meilleures pratiques décrites dans les ressources suivantes :

- Bonnes pratiques pour les unités organisationnelles dotées de AWS Organizations(blog AWS sur les opérations et les migrations dans le cloud)
- Conseils pour établir une base initiale à l'aide de AWS Control Tower on AWS (bibliothèque de AWS solutions)
- Conseils pour créer et modifier AWS Control Tower des ressources (AWS Control Tower documentation)
- Considérations relatives au déploiement du CfCT (AWS Control Tower documentation)
- Appliquer les autorisations du moindre privilège (documentation IAM)

Épopées

Passez en revue le CloudFormation modèle

Tâche	Description	Compétences requises
Déterminez votre stratégie de déploiement.	Passez en revue la solution et le code afin de détermine r la stratégie de déploieme nt adaptée à votre AWS environnement. Déterminez si vous effectuez le déploiement dans un seul compte ou dans une AWS organisation.	Propriétaire de l'application, General AWS
Pour cloner le référentiel.	Entrez la commande suivante pour cloner le référentiel Detect vulnerable security groups :	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/detect-public-security-groups.git`	
Validez la version de Python.	1. Accédez au répertoire de premier niveau du référentiel cloné : `cd detect-public-security-groups` 2. Ouvrez Security-Group-Public-Assessment.yaml. 3. Dans la `SgPublicAccessCheckLambdaFunction` ressource, vérifiez que la version de Python est compatible avec votre cible Régions AWS. Par défaut, cette fonction utilise Python 3.12. Pour plus d'informations, consultez la section AWS Lambda Ajout du support pour Python 3.12. Si nécessaire, mettez à jour la version de Python. 4. Enregistrez et fermez Security-Group-Public-Assessment.yaml.	Administrateur AWS, développeur d'applications

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Déployez le CloudFormation modèle dans votre AWS environnement. Effectuez l'une des actions suivantes : • Si vous effectuez un déploiement sur un modèle unique Compte AWS, suivez les instructions de la section Création d'une pile. • Si vous effectuez un déploiement dans une organisation qui n'est pas gérée par AWS Control Tower, suivez les instructi ons de la section Créer un stack set. • Si vous effectuez un déploiement dans une organisation gérée par AWS Control Tower, consultez les instructions de la section Créez vos propres personnalisations.	Développeur d'applications, administrateur AWS, AWS général
Vérifier le déploiement.	Dans la CloudFormation console, vérifiez que la pile ou l'ensemble de piles a été déployé avec succès.	Administrateur AWS, propriéta ire de l'application

Passez en revue les résultats

Tâche	Description	Compétences requises
Consultez les résultats des AWS Config règles.	Dans Security Hub, procédez comme suit pour afficher la liste des résultats individuels : 1. Ouvrez la console Security Hub. 2. Dans le volet de navigation, choisissez Conclusions. 3. Dans la zone Ajouter des filtres, ajoutez les filtres suivants : • Le statut de conformité est `FAILED` • Le titre est `SgPublicAccessCheck` 4. Choisissez Appliquer. Dans Security Hub, procédez comme suit pour afficher la liste des résultats totaux regroupés par Compte AWS : 1. Ouvrez la console Security Hub. 2. Dans le panneau de navigation, choisissez Insights. 3. Choisissez Create insight (Créer une information).	Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
	4. Pour sélectionner l'attribut de regroupement pour l'aperçu : a. Choisissez le champ de recherche pour afficher les options de filtre. b. Choisissez Group by (Regrouper par). c. Sélectionnez AwsAccountId. d. Choisissez Appliquer. 5. Dans la zone Ajouter des filtres, ajoutez les filtres suivants : • Le titre est `SgPublicAccessCheck` • Le statut de conformité est `FAILED` 6. Choisissez Create insight (Créer une information). 7. Entrez un nom d'aperçu, puis choisissez Créer un aperçu. Dans AWS Config, pour consulter la liste des résultats, suivez les instructions de la section Affichage des informations de conformité et des résultats d'évaluation de la AWS Config documentation.	

Résolution des problèmes

Problème	Solution
La création ou la suppression de l'ensemble de CloudFormation piles échoue.	Lorsqu'il AWS Control Tower est déployé, il applique les garde-fous nécessaires et prend le contrôle des AWS Config agrégateurs et des règles. Cela inclut la prévention de toute modification directe par le biais de CloudForm ation. Pour déployer ou supprimer correctement ce CloudFormation modèle, y compris toutes les ressources associées, vous devez utiliser CfCT.
CfCT ne parvient pas à supprimer le CloudFormation modèle.	Si le CloudFormation modèle persiste même après avoir apporté les modifications nécessaires au fichier manifeste et supprimé les fichiers modèles, vérifiez que le fichier manifeste contient le `enable_stack_set_d eletion` paramètre et que la valeur est définie sur`false`. Pour plus d'informations, consultez Supprimer un ensemble de piles dans la documentation CfCT.

Ressources connexes

- AWS Config Règles personnalisées (AWS Config documentation)

Réactivez automatiquement AWS à l'aide CloudTrail d'une règle de correction personnalisée dans AWS Config

Créée par Manigandan Shri (AWS)

Récapitulatif

La visibilité de l'activité de votre compte Amazon Web Services (AWS) est une bonne pratique opérationnelle et de sécurité importante. AWS vous CloudTrail aide à gérer la gouvernance, la conformité, ainsi que l'audit des opérations et des risques de votre compte.

Pour garantir que cela CloudTrail reste activé dans votre compte, AWS Config fournit la règle `cloudtrail-enabled` gérée. Si elle CloudTrail est désactivée, la `cloudtrail-enabled` règle la réactive automatiquement à l'aide de la correction automatique.

Toutefois, vous devez vous assurer de suivre les meilleures pratiques en matière de sécurité CloudTrail si vous utilisez la correction automatique. Ces bonnes pratiques incluent l'activation CloudTrail dans toutes les régions AWS, la journalisation des charges de travail de lecture et d'écriture, l'activation d'informations et le chiffrement des fichiers journaux avec un chiffrement côté serveur à l'aide des clés gérées par AWS Key Management Service (AWS KMS) (SSE-KMS).

Ce modèle vous aide à suivre ces bonnes pratiques en matière de sécurité en fournissant une action corrective personnalisée pour la réactiver automatiquement CloudTrail dans votre compte.

> **Important**
>
> Nous vous recommandons d'utiliser des politiques de contrôle des services (SCPs) pour empêcher toute altération. CloudTrail Pour plus d'informations à ce sujet, consultez la section Empêcher toute altération avec AWS de la CloudTrail section Comment utiliser AWS Organizations pour simplifier la sécurité à grande échelle sur le blog de sécurité AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Autorisations pour créer un runbook AWS Systems Manager Automation

- Un historique existant pour votre compte

Limites

Ce modèle ne prend pas en charge les actions suivantes :

- Configuration d'une clé de préfixe Amazon Simple Storage Service (Amazon S3) pour l'emplacement de stockage
- Publication sur une rubrique Amazon Simple Notification Service (Amazon SNS)
- Configuration d'Amazon CloudWatch Logs pour surveiller vos CloudTrail journaux

Architecture

Pile technologique

- AWS Config
- CloudTrail
- Systems Manager
- Systems Manager Automation

Outils

- AWS Config fournit une vue détaillée de la configuration des ressources AWS de votre compte.
- AWS vous CloudTrail aide à activer la gouvernance, la conformité et l'audit opérationnel et des risques de votre compte.
- AWS Key Management Service (AWS KMS) est un service de chiffrement et de gestion des clés.
- AWS Systems Manager vous aide à visualiser et à contrôler votre infrastructure sur AWS.
- AWS Systems Manager Automation simplifie les tâches courantes de maintenance et de déploiement des instances Amazon Elastic Compute Cloud (Amazon EC2) et des autres ressources AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Code

Le fichier cloudtrail-remediation-action.yml (joint) vous permet de créer un runbook Systems Manager Automation à configurer et à réactiver en CloudTrail utilisant les meilleures pratiques de sécurité.

Épopées

Configuration CloudTrail

Tâche	Description	Compétences requises
Créez un compartiment S3.	Connectez-vous à l'AWS Management Console, ouvrez la console Amazon S3, puis créez un compartiment S3 pour stocker les CloudTrail journaux. Pour plus d'informations, consultez la section Créer un compartiment S3 dans la documentation Amazon S3.	Administrateur de systèmes
Ajoutez une politique de compartiment pour CloudTrail permettre de fournir des fichiers journaux au compartiment S3.	CloudTrail doit disposer des autorisations requises pour transmettre les fichiers journaux à votre compartiment S3. Sur la console Amazon S3, choisissez le compartiment S3 que vous avez créé précédemment, puis sélectionnez Permissions. Créez une politique de compartiment S3 à l'aide de la politique CloudTrail de compartiment Amazon S3 figurant dans la CloudTrail documentation.	Administrateur de systèmes

Tâche	Description	Compétences requises
	Pour savoir comment ajouter une politique à un compartiment S3, consultez la section Ajout d'une politique de compartiment à l'aide de la console Amazon S3 dans la documentation Amazon S3. **⚠ Important** Si vous avez spécifié un préfixe lorsque vous avez créé votre parcours dans CloudTrail, assurez-vous de l'inclure dans la politique du compartiment S3. Le préfixe est un ajout facultatif à la clé d'objet S3 qui crée une organisation semblable à un dossier dans votre compartiment S3. Pour plus d'informations à ce sujet, consultez la section Création d'un parcours dans la CloudTrail documentation.	

Tâche	Description	Compétences requises
Créer une clé KMS.	Créez une clé AWS KMS CloudTrail pour chiffrer les objets avant de les ajouter au compartiment S3. Pour obtenir de l'aide concernant cet article, consultez la section Chiffrement des fichiers CloudTrail journaux à l'aide des clés gérées par AWS KMS (SSE-KMS) dans la documentation. CloudTrail	Administrateur de systèmes
Ajoutez une politique clé à la clé KMS.	Joignez une politique de clé KMS CloudTrail pour autoriser l'utilisation de la clé KMS. Pour obtenir de l'aide concernant cet article, consultez la section Chiffrement des fichiers CloudTrail journaux avec des clés gérées par AWS KMS (SSE-KMS) dans la documentation. CloudTrail ⚠ Important CloudTrail ne nécessite pas d'`Decrypt`autorisation.	Administrateur de systèmes

Tâche	Description	Compétences requises
Runbook Create AssumeRole for Systems Manager	Créez un `AssumeRole` pour Systems Manager Automation pour exécuter le runbook. Pour obtenir des instructions et plus d'informations à ce sujet, consultez la section Configuration de l'automatisation dans la documentation de Systems Manager.	Administrateur de systèmes

Créez et testez le runbook Systems Manager Automation

Tâche	Description	Compétences requises
Créez le runbook Systems Manager Automation.	Utilisez le `cloudtrail-remediation-action.yml` fichier (joint) pour créer le runbook Systems Manager Automation. Pour plus d'informations à ce sujet, consultez les documents Creating Systems Manager dans la documentation de Systems Manager.	Administrateur de systèmes
Testez le runbook.	Sur la console Systems Manager, testez le runbook Systems Manager Automation que vous avez créé précédemment. Pour plus d'informations à ce sujet, consultez la section Exécuter une automatisation simple	Administrateur de systèmes

Tâche	Description	Compétences requises
	dans la documentation de Systems Manager.	

Configurer la règle de correction automatique dans AWS Config

Tâche	Description	Compétences requises
Ajoutez la règle CloudTrail activée.	Sur la console AWS Config, choisissez Rules, puis Add rule. Sur la page Ajouter une règle, choisissez Ajouter une règle personnalisée. Sur la page Configurer la règle, entrez un nom et une description, puis ajoutez la `cloudtrail-enabled` règle. Pour plus d'informations, consultez la section Gestion de vos règles AWS Config dans la documentation AWS Config.	Administrateur de systèmes
Ajoutez l'action de correction automatique.	Dans la liste déroulante Actions, choisissez Gérer les mesures correctives. Choisissez Auto remediation, puis choisissez le runbook Systems Manager que vous avez créé précédemment. Les paramètres d'entrée requis sont les CloudTrail suivants : • `CloudTrailName`	Administrateur de systèmes

Tâche	Description	Compétences requises
	• `CloudTrailS3BucketName` • `CloudTrailKmsKeyId` • `AssumeRole` (facultatif) Les paramètres d'entrée suivants sont définis sur true par défaut : • `IsMultiRegionTrail` • `IsOrganizationTrail` • `IncludeGlobalServiceEvents` • `EnableLogFileValidation` Conservez les valeurs par défaut du paramètre Rate Limits et du paramètre Resource ID. Choisissez Enregistrer. Pour plus d'informations, consultez la section Corriger les ressources AWS non conformes à l'aide des règles AWS Config dans la documentation AWS Config.	

Tâche	Description	Compétences requises
Testez la règle de correction automatique.	Pour tester la règle de correction automatique, ouvrez la CloudTrail console, choisissez Trails, puis choisissez le trail. Choisisse z Arrêter la journalisation pour désactiver la journalis ation du parcours. Lorsque vous êtes invité à confirmer, choisissez Arrêter la journalis ation. CloudTrail arrête l'activit é d'enregistrement pour ce sentier. Suivez les instructions de la section Évaluation de vos ressources dans la documenta tion AWS Config pour vous assurer que cette option CloudTrail a été automatiq uement réactivée.	Administrateur de systèmes

Ressources connexes

Configuration CloudTrail

- Création d'un compartiment S3
- Politique relative aux compartiments Amazon S3 pour CloudTrail
- Ajouter une politique de compartiment à l'aide de la console Amazon S3
- Création d’un journal de suivi
- Configuration de l'automatisation
- Chiffrement des fichiers CloudTrail journaux avec les clés gérées par AWS KMS (SSE-KMS)

Créez et testez le runbook Systems Manager Automation

- Création de documents Systems Manager
- Exécution d'une automatisation simple

Configurer la règle de correction automatique dans AWS Config

- Gestion de vos règles AWS Config
- Corriger les ressources AWS non conformes à l'aide des règles AWS Config

Ressources supplémentaires

- AWS CloudTrail - Bonnes pratiques en matière de sécurité
- Commencer à utiliser AWS Systems Manager
- Commencer à utiliser AWS Config
- Commencer à utiliser AWS CloudTrail

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Corriger automatiquement les instances et clusters de base de données Amazon RDS non chiffrés

Créée par Ajay Rawat (AWS) et Josh Joy (AWS)

Récapitulatif

Ce modèle décrit comment corriger automatiquement les instances de base de données et les clusters Amazon Relational Database Service (Amazon RDS) non chiffrés sur Amazon Web Services (AWS) en utilisant des clés AWS Config, AWS Systems Manager runbooks et (). AWS Key Management Service AWS KMS

Les instances de base de données RDS chiffrées fournissent une couche supplémentaire de protection des données en protégeant vos données contre tout accès non autorisé au stockage sous-jacent. Vous pouvez utiliser le chiffrement Amazon RDS pour renforcer la protection des données de vos applications déployées dans le AWS Cloud et pour satisfaire aux exigences de conformité relatives au chiffrement au repos. Vous pouvez activer le chiffrement pour une instance de base de données RDS lorsque vous la créez, mais pas après sa création. Toutefois, vous pouvez ajouter le chiffrement à une instance de base de données RDS non chiffrée en créant un instantané de votre instance de base de données, puis en créant une copie chiffrée de cet instantané. Vous pouvez ensuite restaurer une instance de base de données à partir de l'instantané chiffré pour obtenir une copie chiffrée de votre instance de base de données d'origine.

Ce modèle est utilisé AWS Config Rules pour évaluer les instances et les clusters de base de données RDS. Il applique la correction en utilisant AWS Systems Manager des runbooks, qui définissent les actions à effectuer sur les ressources Amazon RDS non conformes, AWS KMS et des clés pour chiffrer les instantanés de base de données. Il applique ensuite les politiques de contrôle des services (SCPs) pour empêcher la création de nouvelles instances de base de données et de nouveaux clusters sans chiffrement.

Le code de ce modèle est fourni dans GitHub.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Fichiers du référentiel de code GitHub source pour ce modèle téléchargés sur votre ordinateur

- Une instance ou un cluster de base de données RDS non chiffré
- Une AWS KMS clé existante pour chiffrer les instances et les clusters de base de données RDS
- Accès pour mettre à jour la politique de ressources clés KMS
- AWS Config activé dans votre Compte AWS (voir Getting Started with AWS Config dans la AWS documentation)

Limites

- Vous pouvez activer le chiffrement pour une instance de base de données RDS uniquement lorsque vous la créez, et non une fois qu'elle a été créée.
- Vous ne pouvez pas avoir un réplica en lecture chiffré d'une instance de base de données non chiffrée ni un réplica en lecture non chiffré d'une instance de base de données chiffrée.
- Vous ne pouvez pas restaurer un instantané non chiffré ou une sauvegarde non chiffrée vers une instance de base de données chiffrée.
- Le chiffrement Amazon RDS est disponible pour la plupart des classes d'instance de base de données. Pour obtenir la liste des exceptions, consultez la section Chiffrement des ressources Amazon RDS dans la documentation Amazon RDS.
- Pour copier un instantané chiffré de l'un Région AWS à l'autre, vous devez spécifier la clé KMS dans la destination Région AWS. Cela est dû au fait que les clés KMS sont spécifiques à Région AWS celle dans laquelle elles ont été créées.
- L'instantané source reste chiffré pendant tout le processus de copie. Amazon RDS utilise le chiffrement des enveloppes pour protéger les données pendant le processus de copie. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la AWS KMS documentation.
- Vous ne pouvez pas déchiffrer une instance de base de données chiffrée. Toutefois, vous pouvez exporter des données depuis une instance de base de données chiffrée et les importer dans une instance de base de données non chiffrée.
- Vous ne devez supprimer une clé KMS que lorsque vous êtes certain de ne plus avoir besoin de l'utiliser. En cas de doute, pensez à désactiver la clé KMS au lieu de la supprimer. Vous pouvez réactiver une clé KMS désactivée si vous devez la réutiliser ultérieurement, mais vous ne pouvez pas récupérer une clé KMS supprimée.
- Si vous choisissez de ne pas conserver les sauvegardes automatisées, les sauvegardes automatiques qui se trouvent dans le même emplacement Région AWS que l'instance de base de données sont supprimées. Elles ne sont pas récupérables après la suppression de l'instance de base de données.

- Vos sauvegardes automatisées sont conservées pendant la période de rétention définie sur l'instance de base de données au moment où vous la supprimez. Cette période de conservation définie intervient que vous choisissiez ou non de créer un instantané de bases de données final.
- Si la correction automatique est activée, cette solution chiffre toutes les bases de données qui possèdent la même clé KMS.

Architecture

Le schéma suivant illustre l'architecture de la mise AWS CloudFormation en œuvre. Notez que vous pouvez également implémenter ce modèle en utilisant le AWS Cloud Development Kit (AWS CDK).

Outils

Outils

- AWS CloudFormationvous aide à configurer automatiquement vos AWS ressources. Il vous permet d'utiliser un fichier modèle pour créer et supprimer un ensemble de ressources en une seule unité (une pile).
- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel permettant de définir votre infrastructure cloud en code et de la provisionner à l'aide de langages de programmation familiers.

Services et fonctionnalités AWS

- AWS Configassure le suivi de la configuration de vos AWS ressources et de leurs relations avec vos autres ressources. Il peut également évaluer la conformité de ces AWS ressources. Ce service utilise des règles qui peuvent être configurées pour évaluer les AWS ressources par rapport aux configurations souhaitées. Vous pouvez utiliser un ensemble de règles AWS Config gérées pour les scénarios de conformité courants ou créer vos propres règles pour des scénarios personnalisés. Lorsqu'une AWS ressource s'avère non conforme, vous pouvez spécifier une action corrective par le biais d'un AWS Systems Manager runbook et éventuellement envoyer une alerte via une rubrique Amazon Simple Notification Service (Amazon SNS). En d'autres termes, vous pouvez associer des actions de correction AWS Config Rules et choisir de les exécuter automatiquement pour traiter les ressources non conformes sans intervention manuelle. Si une ressource n'est toujours pas conforme après la correction automatique, vous pouvez définir la règle pour réessayer la correction automatique.

- Amazon Relational Database Service (Amazon RDS) facilite la configuration, l'exploitation et le dimensionnement d'une base de données relationnelle dans le cloud. L'élément de base d'Amazon RDS est l'instance de base de données, qui est un environnement de base de données isolé dans le AWS Cloud. Amazon RDS propose une sélection de types d'instances optimisés pour s'adapter aux différents cas d'utilisation des bases de données relationnelles. Les types d'instances comprennent différentes combinaisons de capacité de processeur, de mémoire, de stockage et de réseau et vous permettent de choisir la combinaison de ressources appropriée pour votre base de données. Chaque type d'instance inclut plusieurs tailles d'instance, ce qui vous permet d'adapter votre base de données aux exigences de votre charge de travail cible.
- AWS Key Management Service (AWS KMS) est un service géré qui vous permet de créer et de contrôler facilement AWS KMS keys, et qui crypte vos données. Une clé KMS est une représentation logique d'une clé racine. La clé KMS inclut des métadonnées, telles que l'ID de clé, la date de création, la description et l'état de la clé.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- Les politiques de contrôle des services (SCPs) permettent de contrôler de manière centralisée les autorisations maximales disponibles pour tous les comptes de votre organisation. SCPs vous aider à garantir que vos comptes respectent les directives de contrôle d'accès de votre organisation. SCPs n'affectent pas les utilisateurs ni les rôles dans le compte de gestion. Elles affectent uniquement les comptes membres de votre organisation. Nous vous recommandons vivement de ne pas vous attacher SCPs à la racine de votre organisation sans avoir testé de manière approfondie l'impact de la politique sur les comptes. Créez plutôt une unité organisationnelle (UO) dans laquelle vous pouvez déplacer vos comptes un par un, ou du moins en petit nombre, afin de ne pas empêcher les utilisateurs d'accéder par inadvertance à des services clés.

Code

Le code source et les modèles de ce modèle sont disponibles dans un GitHub référentiel. Le modèle propose deux options d'implémentation : vous pouvez déployer un AWS CloudFormation modèle pour créer le rôle de correction qui chiffre les instances de base de données et les clusters RDS, ou utiliser le. AWS CDK Le référentiel comporte des dossiers distincts pour ces deux options.

La section Epics fournit des step-by-step instructions pour déployer le CloudFormation modèle. Si vous souhaitez utiliser le AWS CDK, suivez les instructions figurant dans le `README.md` fichier du GitHub référentiel.

Bonnes pratiques

- Activez le chiffrement des données au repos et en transit.
- Activez AWS Config dans tous les comptes et Régions AWS.
- Enregistrez les modifications de configuration apportées à tous les types de ressources.
- Effectuer une rotation régulière des informations d'identification IAM.
- Tirez parti du balisage pour AWS Config faciliter la gestion, la recherche et le filtrage des ressources.

Épopées

Création du rôle de correction IAM et du runbook Systems Manager

Tâche	Description	Compétences requises
Téléchargez le CloudFormation modèle.	Téléchargez le `unencrypted-to-encrypted-rds.template.json` fichier depuis le GitHub référentiel.	DevOps ingénieur
Créez la CloudFormation pile.	1. Connectez-vous à la CloudFormation console AWS Management Console et ouvrez-la. 2. Lancez le `unencrypted-to-encrypted-rds.template.json` modèle pour créer une nouvelle pile. Pour plus d'informations sur le déploiement de modèles, consultez la AWS CloudFormation documentation.	DevOps ingénieur

Tâche	Description	Compétences requises
Passez en revue CloudForm ation les paramètres et les valeurs.	1. Passez en revue les détails de la pile et mettez à jour les valeurs en fonction des exigences de votre environnement. 2. Choisissez Create stack pour déployer le modèle.	DevOps ingénieur
Passez en revue les ressource s.	Lorsque la pile a été créée, son statut passe à CREATE_COMPLETE. Passez en revue les ressource s créées (rôle IAM, manuel d'exécution de Systems Manager) dans la CloudForm ation console.	DevOps ingénieur

Mettre à jour la politique AWS KMS clé

Tâche	Description	Compétences requises
Mettez à jour votre politique relative aux clés KMS.	1. Assurez-vous que l'alias de clé `alias/RDS EncryptionAtRestKM SAlias` existe. 2. La déclaration de politique clé doit inclure le rôle de correction de l'IAM. (Vérifiez les ressources créées par le CloudFormation modèle que vous avez déployé dans l'épopée précédente.) 3. Dans la politique clé suivante, mettez à jour	DevOps ingénieur

Tâche	Description	Compétences requises
	les parties en gras pour qu'elles correspondent à votre compte et au rôle IAM créé. `{ "Sid": "Allow access through RDS for all principals in the account that are authorized to use RDS", "Effect": "Allow", "Principal": { "AWS": "arn:aws:iam:: <your-AWS-account-ID>”:role/<your-IAM-remediation-role>" }, "Action": ["kms:Encrypt", "kms:Decrypt", "kms:ReEncrypt*", "kms:GenerateDataKey*", "kms:CreateGrant", "kms:ListGrants", "kms:DescribeKey"], "Resource": "*", "Condition": { "StringEquals": {`	

Tâche	Description	Compétences requises

	<pre>"kms:ViaS
	ervice": "rds.us-e
	ast-1.amazonaws.com",
	"kms:Call
	erAccount": "<your-AW
	S-account-ID>"
	}
	}
	}</pre>	

Identifiez et corrigez les ressources non conformes

Tâche	Description	Compétences requises
Afficher les ressources non conformes.	1. Pour afficher la liste des ressources non conformes, ouvrez la AWS Config console. 2. Dans le volet de navigation, choisissez Rules, puis choisissez la `rds-storage-encrypted` règle. Les ressources non conformes répertoriées dans la AWS Config console seront des instances et non des clusters. L'automatisation de la correction chiffre les instances et les clusters, et crée soit une nouvelle instance chiffrée, soit un cluster nouvellement créé. Veillez toutefois à ne pas corriger simultanément	DevOps ingénieur

Tâche	Description	Compétences requises
	plusieurs instances appartenant au même cluster. Avant de corriger des instances ou des volumes de base de données RDS, assurez-vous que l'instance de base de données RDS n'est pas utilisée. Vérifiez qu'aucune opération d'écriture n'est en cours pendant la création de l'instantané, afin de vous assurer que celui-ci contient les données d'origine. Envisagez d'imposer une fenêtre de maintenance pendant laquelle la correction s'exécutera.	

Tâche	Description	Compétences requises
Corrigez les ressources non conformes.	1. Lorsque vous êtes prêt et que la fenêtre de maintenance est active, choisissez la ressource à corriger, puis choisissez Corriger. La colonne État de l'action doit désormais afficher l'exécution de l'action en file d'attente. 2. Consultez la progression et le statut de la correction dans Systems Manager. Ouvrez la console Systems Manager. Dans le volet de navigation, choisissez Automation, puis sélectionnez l'ID d'exécution de l'automatisation correspondante pour afficher plus de détails.	DevOps ingénieur

Tâche	Description	Compétences requises
Vérifiez que l'instance de base de données RDS est disponible.	Une fois l'automatisation terminée, l'instance de base de données RDS nouvellement chiffrée sera disponible. L'instance de base de données RDS cryptée aura le préfixe `encrypted` suivi du nom d'origine. Par exemple, si le nom de l'instance de base de données RDS non chiffrée était`database-1` , l'instance de base de données RDS nouvellement chiffrée le serait. `encrypted-database-1`	DevOps ingénieur
Mettez fin à l'instance non chiffrée.	Une fois la correction terminée et la nouvelle ressource chiffrée validée, vous pouvez mettre fin à l'instance non chiffrée. Assurez-vous de vérifier que la ressource nouvellement chiffrée correspond à la ressource non chiffrée avant de mettre fin à toute ressource.	DevOps ingénieur

Faire appliquer SCPs

Tâche	Description	Compétences requises
Faire appliquer SCPs.	Appliquez SCPs pour empêcher la création d'instances et de clusters de base de données sans chiffrement à	Ingénieur de sécurité

Tâche	Description	Compétences requises
	l'avenir. Utilisez le `rds_encrypted.json` fichier fourni dans le GitHub référentiel à cette fin et suivez les instructions de la AWS documentation.	

Ressources connexes

Références

- Configuration AWS Config
- AWS Config règles personnalisées
- AWS KMS concepts
- AWS Systems Manager documents
- Politiques de contrôle des services

Outils

- AWS CloudFormation
- AWS Cloud Development Kit (AWS CDK)

Guides et modèles

- Réactivation automatique à AWS CloudTrail l'aide d'une règle de correction personnalisée dans AWS Config

Informations supplémentaires

Comment AWS Config fonctionne ?

Lorsque vous l'utilisez AWS Config, il découvre d'abord les AWS ressources prises en charge qui existent dans votre compte et génère un élément de configuration pour chaque ressource. AWS Config génère également des éléments de configuration lorsque la configuration d'une ressource

change, et il conserve des enregistrements historiques des éléments de configuration de vos ressources depuis le démarrage de l'enregistreur de configuration. Par défaut, AWS Config crée des éléments de configuration pour chaque ressource prise en charge dans le Région AWS. Si vous ne souhaitez pas AWS Config créer d'éléments de configuration pour toutes les ressources prises en charge, vous pouvez spécifier les types de ressources que vous souhaitez suivre.

Comment sont-ils AWS Config et AWS Config Rules liés à AWS Security Hub ?

AWS Security Hub est un service de sécurité et de conformité qui fournit une gestion de la posture de sécurité et de conformité en tant que service. Il utilise AWS Config et AWS Config Rules comme principal mécanisme pour évaluer la configuration des AWS ressources. AWS Config Rules peut également être utilisé pour évaluer directement la configuration des ressources. Autres Services AWS, tels AWS Control Tower et AWS Firewall Managerégalement utilisés AWS Config Rules.

Faites automatiquement pivoter les clés d'accès utilisateur IAM à grande échelle avec AWS Organizations et AWS Secrets Manager

Créée par Tracy Hickey (AWS), Gaurav Verma (AWS), Laura Seletos (AWS), Michael Davie (AWS) et Arvind Patel (AWS)

Récapitulatif

> **Important**
>
> En tant que bonne pratique, AWS vous recommande d'utiliser des rôles AWS Identity and Access Management (IAM) plutôt que des utilisateurs IAM dotés d'informations d'identif ication à long terme, telles que des clés d'accès. L'approche décrite dans ce modèle est destinée uniquement aux implémentations existantes qui nécessitent des informati ons d'identification d'API AWS de longue durée. Pour ces implémentations, nous vous recommandons tout de même d'envisager des options d'utilisation d'informations d'identif ication à court terme, telles que l'utilisation de profils d'instance Amazon Elastic Compute Cloud (Amazon EC2) ou d'IAM Roles Anywhere. L'approche décrite dans cet article concerne uniquement les cas où vous ne pouvez pas passer immédiatement à l'utilisa tion d'informations d'identification à court terme et où vous avez besoin d'une rotation des informations d'identification à long terme selon un calendrier. Avec cette approche, vous êtes responsable de la mise à jour périodique du code ou de la configuration de votre ancienne application afin d'utiliser les informations d'identification d'API modifiées.

Les clés d'accès sont des informations d'identification à long terme pour un utilisateur IAM. La rotation régulière de vos informations d'identification IAM permet d'empêcher un ensemble compromis de clés d'accès IAM d'accéder aux composants de votre compte AWS. La rotation des informations d'identification IAM est également un élément important des meilleures pratiques de sécurité en matière d'IAM.

Ce modèle vous permet de faire pivoter automatiquement les clés d'accès IAM à l'aide de CloudFormation modèles AWS, qui sont fournis dans le référentiel de rotation des clés GitHub IAM.

Le modèle prend en charge le déploiement dans un ou plusieurs comptes. Si vous utilisez AWS Organizations, cette solution identifie tous les comptes AWS IDs au sein de votre organisation et évolue dynamiquement à mesure que des comptes sont supprimés ou que de nouveaux comptes

sont créés. La fonction AWS Lambda centralisée utilise un rôle IAM supposé pour exécuter localement les fonctions de rotation sur plusieurs comptes que vous sélectionnez.

- Les nouvelles clés d'accès IAM sont générées lorsque les clés d'accès existantes datent de 90 jours.
- Les nouvelles clés d'accès sont stockées en tant que secret dans AWS Secrets Manager. Une politique basée sur les ressources permet uniquement au principal IAM spécifié d'accéder au secret et de le récupérer. Si vous choisissez de stocker les clés dans le compte de gestion, les clés de tous les comptes sont stockées dans le compte de gestion.
- L'adresse e-mail attribuée au propriétaire du compte AWS où les nouvelles clés d'accès ont été créées reçoit une notification.
- Les clés d'accès précédentes sont désactivées à 100 jours, puis supprimées à 110 jours.
- Une notification par e-mail centralisée est envoyée au propriétaire du compte AWS.

Les fonctions Lambda et Amazon exécutent CloudWatch automatiquement ces actions. Vous pouvez ensuite récupérer la nouvelle paire de clés d'accès et la remplacer dans votre code ou dans vos applications. Les périodes de rotation, de suppression et de désactivation peuvent être personnalisées.

Conditions préalables et limitations

- Au moins un compte AWS actif.
- AWS Organizations, configuré et configuré (voir le didacticiel).
- Autorisations pour interroger AWS Organizations depuis votre compte de gestion. Pour plus d'informations, consultez AWS Organizations and service-linked roles dans la documentation AWS Organizations.
- Un responsable IAM autorisé à lancer le CloudFormation modèle AWS et les ressources associées. Pour plus d'informations, consultez la section Accorder des autorisations autogérées dans la CloudFormation documentation AWS.
- Un compartiment Amazon Simple Storage Service (Amazon S3) existant pour déployer les ressources.
- Amazon Simple Email Service (Amazon SES) a quitté le sandbox. Pour plus d'informations, consultez la section Sortir du sandbox d'Amazon SES dans la documentation Amazon SES.
- Si vous choisissez d'exécuter Lambda dans un cloud privé virtuel (VPC), les ressources suivantes doivent être créées avant d'exécuter le modèle principal : CloudFormation

  - Un VPC.
  - Un sous-réseau
  - Points de terminaison pour Amazon SES, AWS Systems Manager, AWS Security Token Service (AWS STS), Amazon S3 et AWS Secrets Manager. (Vous pouvez exécuter le modèle de point de terminaison fourni dans le référentiel de rotation des clés GitHub IAM pour créer ces points de terminaison.)
- L'utilisateur et le mot de passe SMTP (Simple Mail Transfer Protocol) stockés dans les paramètres d'AWS Systems Manager (paramètres SSM). Les paramètres doivent correspondre aux paramètres du CloudFormation modèle principal.

Architecture

Pile technologique

- Amazon CloudWatch
- Amazon EventBridge
- IAM
- AWS Lambda
- AWS Organizations
- Amazon S3

Architecture

Les diagrammes suivants montrent les composants et les flux de travail de ce modèle. La solution prend en charge deux scénarios de stockage des informations d'identification : dans un compte membre et dans le compte de gestion.

Option 1 : Stocker les informations d'identification dans un compte membre

Option 2 : Stocker les informations d'identification dans le compte de gestion

Les diagrammes montrent le flux de travail suivant :

1. Un EventBridge événement lance une fonction `account_inventory` Lambda toutes les 24 heures.

2. Cette fonction Lambda interroge AWS Organizations pour obtenir la liste de tous les comptes IDs, noms de comptes et e-mails relatifs aux comptes AWS.
3. La fonction `account_inventory` Lambda lance une fonction `access_key_auto_rotation` Lambda pour chaque ID de compte AWS et lui transmet les métadonnées pour un traitement supplémentaire.
4. La fonction `access_key_auto_rotation` Lambda utilise un rôle IAM supposé pour accéder à l'ID de compte AWS. Le script Lambda exécute un audit de tous les utilisateurs et de leurs clés d'accès IAM dans le compte.
5. Si l'âge de la clé d'accès IAM n'a pas dépassé le seuil des meilleures pratiques, la fonction Lambda n'entreprend aucune autre action.
6. Si l'âge de la clé d'accès IAM dépasse le seuil des meilleures pratiques, la fonction `access_key_auto_rotation` Lambda détermine l'action de rotation à effectuer.
7. Lorsqu'une action est requise, la fonction `access_key_auto_rotation` Lambda crée et met à jour un secret dans AWS Secrets Manager si une nouvelle clé est générée. Une politique basée sur les ressources est également créée pour autoriser uniquement le principal IAM spécifié à accéder au secret et à le récupérer. Dans le cas de l'option 1, les informations d'identification sont stockées dans Secrets Manager du compte correspondant. Dans le cas de l'option 2 (si l'`StoreSecretsInCentralAccount`indicateur est défini sur True), les informations d'identification sont stockées dans Secrets Manager du compte de gestion.
8. Une fonction `notifier` Lambda est lancée pour informer le propriétaire du compte de l'activité de rotation. Cette fonction reçoit l'ID du compte AWS, le nom du compte, l'adresse e-mail du compte et les actions de rotation effectuées.
9. La fonction `notifier` Lambda interroge le compartiment S3 de déploiement pour un modèle d'e-mail et le met à jour dynamiquement avec les métadonnées d'activité pertinentes. L'e-mail est ensuite envoyé à l'adresse e-mail du propriétaire du compte.

Remarques :

- Cette solution prend en charge la résilience dans plusieurs zones de disponibilité. Cependant, il ne prend pas en charge la résilience dans plusieurs régions AWS. Pour bénéficier d'une assistance dans plusieurs régions, vous pouvez déployer la solution dans la deuxième région et désactiver la EventBridge règle de rotation des clés. Vous pouvez ensuite activer la règle lorsque vous souhaitez exécuter la solution dans la deuxième région.
- Vous pouvez exécuter cette solution en mode audit. En mode audit, les clés d'accès IAM ne sont pas modifiées, mais un e-mail est envoyé pour informer les utilisateurs. Pour

exécuter la solution en mode audit, définissez l'`DryRunFlag`indicateur sur True lorsque vous exécutez le modèle de rotation des clés ou dans la variable d'environnement de la fonction `access_key_auto_rotation` Lambda.

Automatisation et mise à l'échelle

Les CloudFormation modèles qui automatisent cette solution sont fournis dans le référentiel de rotation des clés GitHub IAM et répertoriés dans la section Code. Dans AWS Organizations, vous pouvez l'utiliser CloudFormation StackSetspour déployer le `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` CloudFormation modèle sur plusieurs comptes au lieu de déployer la solution individuellement sur chaque compte membre.

Outils

Services AWS

- Amazon vous CloudWatch aide à surveiller les indicateurs de vos ressources AWS et des applications que vous exécutez sur AWS en temps réel.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizations est un service de gestion de comptes qui vous aide à consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Amazon Simple Email Service (Amazon SES) vous permet d'envoyer et de recevoir des e-mails en utilisant vos propres adresses e-mail et domaines.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.
- Les points de terminaison Amazon VPC fournissent une interface permettant de se connecter aux services fournis par AWS PrivateLink, y compris de nombreux services AWS. Pour chaque sous-réseau que vous spécifiez à partir de votre VPC, une interface réseau de point de terminaison est créée dans le sous-réseau et une adresse IP privée est attribuée à partir de la plage d'adresses du sous-réseau.

Code

Les CloudFormation modèles AWS, les scripts Python et la documentation du runbook requis sont disponibles dans le référentiel de rotation des clés GitHub IAM. Les modèles sont déployés comme suit.

Modèle	Déployer dans	Remarques
`ASA-iam-key-auto-rotation-and-notifier-solution.yaml`	Compte de déploiement	Il s'agit du modèle principal de la solution.
`ASA-iam-key-auto-rotation-iam-assumed-roles.yaml`	Comptes à un ou plusieurs membres pour lesquels vous souhaitez alterner les informations d'identification	Vous pouvez utiliser des ensembles de CloudFormation piles pour déployer ce modèle sur plusieurs comptes.
`ASA-iam-key-auto-rotation-list-accounts-role.yaml`	Compte central/de gestion	Utilisez ce modèle pour tenir un inventaire des comptes dans AWS Organizations.
`ASA-iam-key-auto-rotation-vpc-endpoints.yaml`	Compte de déploiement	Utilisez ce modèle pour automatiser la création de points de terminaison uniquement si vous souhaitez exécuter les fonctions Lambda dans un VPC (définissez `RunLambdaInVPC` le

paramètre sur True dans le modèle principal).

Épopées

Configurez la solution

Tâche	Description	Compétences requises
Choisissez votre compartiment S3 de déploiement.	Connectez-vous à l'AWS Management Console pour votre compte, ouvrez la console Amazon S3, puis choisissez le compartiment S3 pour votre déploiement. Si vous souhaitez implément er la solution pour plusieurs comptes dans AWS Organizat ions, connectez-vous au compte de gestion de votre organisation.	Architecte du cloud
Pour cloner le référentiel.	Clonez le référentiel de rotation des clés GitHub IAM sur votre bureau local.	Architecte du cloud
Téléchargez les fichiers dans le compartiment S3.	Téléchargez les fichiers clonés dans votre compartiment S3. Utilisez la structure de dossiers par défaut suivante pour copier et coller tous les fichiers et répertoires clonés : `asa/asa-iam-rotation`	Architecte du cloud

Tâche	Description	Compétences requises
	Note Vous pouvez personnaliser cette structure de dossiers dans les CloudForm ation modèles.	
Modifiez le modèle d'e-mail.	Modifiez le modèle d'`iam-auto-key-rotation-enforcement.html` e-mail (situé dans le `template` dossier) en fonction de vos besoins. Remplacez `[Department Name Here]` à la fin du modèle par le nom de votre département.	Architecte du cloud

Déployez la solution

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle pour la rotation des clés.	1. Lancez le `ASA-iam-key-auto-rotation-and-notifier-solution.yaml` modèle dans le compte de déploiement. Pour plus d'informations, consultez la section Sélection d'un modèle de pile dans la CloudFormation documentation. 2. Spécifiez les valeurs des paramètres, notamment :	Architecte du cloud

Tâche	Description	Compétences requises
	• CloudFormation Nom du compartiment S3 (`S3BucketName`) : nom du compartiment S3 de déploiement qui contient votre code Lambda. • CloudFormation Préfixe du compartiment S3 (`S3BucketPrefix`) : préfixe du compartiment S3. • Nom de rôle IAM supposé (**`IAMRoleName`**) : nom de rôle que la fonction `key-rotation` Lambda adoptera pour faire pivoter les clés. • Nom du rôle d'exécution IAM (`ExecutionRoleName`) : nom du rôle d'exécution IAM utilisé par la fonction Lambda`key-rotation`. • Nom du rôle d'exécution de l'inventaire (`InventoryExecutionRoleName`) : nom du rôle d'exécution IAM utilisé par la fonction `account_inventory` Lambda.	

Tâche	Description	Compétences requises
	• Indicateur Dry Run (mode audit) (`DryRunFlag`) : défini sur True pour activer le mode audit (par défaut). Réglez la valeur sur False pour activer le mode d'application. • Compte pour répertorier les comptes de l'organisation (`OrgListAccount`) : ID de compte du compte central/de gestion qui sera utilisé pour répertorier les comptes de l'organisation. • Nom du rôle des comptes de liste (`OrgListRole`) : nom du rôle qui sera utilisé pour répertorier les comptes de l'organisation. • Drapeau Secrets Store pour le compte central (`StoreSecretsInCentralAccount`) : défini sur True pour stocker les secrets dans le compte central. Définissez cette valeur sur False pour enregistrer les secrets dans le compte correspondant.	

Tâche	Description	Compétences requises
	• Régions dans lesquelles répliquer les informations d'identification (`CredentialReplicationRegions`) : régions AWS dans lesquelles vous souhaitez répliquer les informations d'identification (Secrets Manager), séparées par des virgules ; par exemple,. `us-east-2,us-west-1,us-west-2` Ignorez la région dans laquelle vous créez la pile. • Exécuter Lambda dans un VPC (`RunLambdaInVpc`) : défini sur True pour exécuter des fonctions Lambda dans un VPC spécifié. Vous devez créer des points de terminaison VPC et associer une passerelle NAT au sous-réseau qui contient la fonction Lambda. Pour plus d'informations, consultez l'article Re:Post qui traite de cette option. • ID VPC pour les fonctions Lambda ()**`VpcId`**, CIDR	

Tâche	Description	Compétences requises
	VPC pour la règle du groupe de sécurité () et identifiant de sous-rése au pour les fonctions Lambda () **`SubnetId`** : fournissez des informati ons sur le VPC**`VpcCidr`**, le CIDR et le sous-rése au si vous définissez sur True. **`RunLambda InVpc`** • Adresse e-mail de l'administrateur (`AdminEmai lAddress`) : adresse e-mail valide à laquelle envoyer des notifications. • ID d'organisation AWS (`AWSOrgID`) : identifiant unique de votre organisat ion. Cet identifiant commence par `o-` et est suivi de 10 à 32 lettres minuscules ou chiffres. • Nom du fichier du modèle d'e-mail [Mode audit] (`EmailTemp lateAudit`) et [Mode d'applica tion] (`EmailTemp lateEnforce`) : nom du fichier du modèle HTML d'e-mail à envoyer par le `notifier` module	

Tâche	Description	Compétences requises
	pour le mode audit et le mode d'application. • Nom du paramètre SSM de l'utilisateur SMTP (**`SMTPUserParamName`**) et nom du paramètre SSM du mot de passe SMTP (`SMTPPasswordParamName`) : informations sur l'utilisateur et le mot de passe pour le protocole SMTP (Simple Mail Transfer Protocol).	

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle pour les rôles assumés.	1. Dans la CloudFormation console AWS, lancez le `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` modèle pour chaque compte pour lequel vous souhaitez faire pivoter les clés. Si vous avez plusieurs comptes, vous pouvez déployer le CloudFormation modèle principal de votre compte de gestion sous forme de pile et déployer le `ASA-iam-key-auto-rotation-iam-assumed-roles.yaml` modèle avec des ensembles de CloudFormation piles sur tous les comptes requis. Pour plus d'informations, consultez la section Travailler avec AWS CloudFormation StackSets dans la CloudFormation documentation. 2. Spécifiez les valeurs des paramètres suivants : • Nom de rôle IAM supposé (**`IAMRoleName`**) : nom du rôle IAM qui sera assumé par la fonction Lambda. `access_key_auto_ro`	Architecte du cloud

Tâche	Description	Compétences requises
	`tation` Vous pouvez conserver la valeur par défaut. • Nom du rôle d'exécution IAM (`Execution RoleName`) : rôle IAM qui assumera le rôle de sous-compte pour exécuter la fonction Lambda. • ID de compte AWS principal (`PrimaryAccountID`) : ID de compte AWS sur lequel le modèle principal sera déployé. • Groupe d'exemption IAM (`IAMExemptionGroup`) : nom du groupe IAM utilisé pour faciliter les comptes IAM que vous souhaitez exclure de la rotation automatique des clés.	

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle d'inventaire des comptes.	1. Lancez le `ASA-iam-key-auto-rotation-list-accounts-role.yaml` modèle dans le compte de gestion/central 2. Spécifiez les valeurs des paramètres suivants : • Nom de rôle IAM supposé (**`IAMRoleName`**) : nom du rôle IAM que la fonction Lambda adopteraaccess_key_auto_rotation . • Nom du rôle d'exécution IAM pour le compte Lambda `AccountExecutionRoleName` () : nom du rôle IAM que la fonction Lambda `notifier` assumera. • Nom du rôle d'exécution IAM pour la rotation Lambda `RotationExecutionRoleName` () : nom du rôle IAM que la fonction Lambda `access_key_auto_rotation` assumera. • ID de compte AWS principal (`PrimaryAccountID`) : ID de compte AWS sur lequel	Architecte du cloud

Tâche	Description	Compétences requises
	le modèle principal sera déployé.	
Lancez le CloudFormation modèle pour les points de terminaison VPC.	Cette tâche est facultative. 1. Lancez le `ASA-iam-key-auto-rotation-vpc-endpoints.yaml` modèle dans le compte de déploiement. 2. Spécifiez les valeurs des paramètres suivants : • ID VPC (**`pVpcId`**), ID de sous-réseau () et plage d'**`pSubnetId`** adresses CIDR pour VPC (**`pVPCCidr`**) : fournissez des informations sur le VPC, le CIDR et le sous-réseau. • Définissez le paramètre pour chaque point de terminaison VPC sur True. Si vous avez déjà des points de terminaison, vous pouvez choisir False.	Architecte du cloud

Ressources connexes

- Bonnes pratiques de sécurité dans l'IAM (documentation IAM)
- Organisations AWS et rôles liés aux services (documentation AWS Organizations)
- Sélection d'un modèle de pile (CloudFormation documentation)

- Utilisation d'AWS CloudFormation StackSets (CloudFormation documentation)

Validez et déployez automatiquement les politiques et les rôles IAM dans un compte AWS à l'aide d' CodePipelineIAM Access Analyzer et de macros AWS CloudFormation

Créée par Helton Ribeiro (AWS) et Guilherme Simoes (AWS)

Récapitulatif

Remarque : AWS n' CodeCommit est plus disponible pour les nouveaux clients. Les clients actuels d'AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus.

Ce modèle décrit les étapes et fournit le code permettant de créer un pipeline de déploiement permettant à vos équipes de développement de créer des politiques et des rôles AWS Identity and Access Management (IAM) dans vos comptes Amazon Web Services (AWS). Cette approche permet à votre organisation de réduire les frais généraux de vos équipes opérationnelles et d'accélérer le processus de déploiement. Il aide également vos développeurs à créer des rôles et des politiques IAM compatibles avec vos contrôles de gouvernance et de sécurité existants.

L'approche de ce modèle utilise AWS Identity and Access Management Access Analyzer pour valider les politiques IAM que vous souhaitez associer aux rôles IAM et utilise AWS CloudFormation pour déployer les rôles IAM. Toutefois, au lieu de modifier directement le fichier CloudFormation modèle AWS, votre équipe de développement crée des politiques et des rôles IAM au format JSON. Une CloudFormation macro AWS transforme ces fichiers de politique au format JSON en types de ressources AWS CloudFormation IAM avant de commencer le déploiement.

Le pipeline de déploiement (`RolesPipeline`) comporte des étapes de source, de validation et de déploiement. Au cours de la phase source, votre équipe de développement transmet les fichiers JSON contenant la définition des rôles et politiques IAM vers un référentiel AWS CodeCommit . AWS exécute CodeBuild ensuite un script pour valider ces fichiers et les copie dans un compartiment Amazon Simple Storage Service (Amazon S3). Vos équipes de développement n'ayant pas un accès direct au fichier CloudFormation modèle AWS stocké dans un compartiment S3 distinct, elles doivent suivre le processus de création et de validation du fichier JSON.

Enfin, pendant la phase de déploiement, AWS CodeDeploy utilise une CloudFormation pile AWS pour mettre à jour ou supprimer les politiques et les rôles IAM d'un compte.

> **Important**
>
> Le flux de travail de ce modèle est une preuve de concept (POC) et nous vous recommandons de ne l'utiliser que dans un environnement de test. Si vous souhaitez utiliser l'approche de ce modèle dans un environnement de production, consultez les meilleures pratiques de sécurité dans IAM dans la documentation IAM et apportez les modifications nécessaires à vos rôles IAM et à vos services AWS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un compartiment S3 nouveau ou existant pour le `RolesPipeline` pipeline. Assurez-vous que les informations d'accès que vous utilisez sont autorisées à télécharger des objets dans ce compartiment.
- Interface de ligne de commande AWS (AWS CLI), installée et configurée. Pour plus d'informations à ce sujet, consultez la section Installation, mise à jour et désinstallation de l'interface de ligne de commande AWS dans la documentation de l'interface de ligne de commande AWS.
- CLI AWS Serverless Application Model (AWS SAM), installée et configurée. Pour plus d'informations à ce sujet, consultez la section Installation de l'interface de ligne de commande AWS SAM dans la documentation AWS SAM.
- Python 3, installé sur votre machine locale. Pour plus d'informations à ce sujet, consultez la documentation Python.
- Un client Git, installé et configuré.
- Le GitHub `IAM roles pipeline` référentiel, cloné sur votre machine locale.
- Politiques et rôles IAM existants au format JSON. Pour plus d'informations à ce sujet, consultez le ReadMefichier dans le `IAM roles pipeline` référentiel Github.
- Votre équipe de développeurs ne doit pas être autorisée à modifier les CodeDeploy ressources AWS CodePipeline et AWS de cette solution. CodeBuild

Limites

- Le flux de travail de ce modèle est une preuve de concept (POC) et nous vous recommandons de ne l'utiliser que dans un environnement de test. Si vous souhaitez utiliser l'approche de ce modèle dans un environnement de production, consultez les meilleures pratiques de sécurité dans IAM dans la documentation IAM et apportez les modifications nécessaires à vos rôles IAM et à vos services AWS.

Architecture

Le schéma suivant explique comment valider et déployer automatiquement les rôles et les politiques IAM sur un compte à l'aide CodePipeline de l'analyseur d'accès IAM et des macros AWS. CloudFormation

Le schéma suivant illustre le flux de travail suivant :

1. Un développeur écrit des fichiers JSON contenant les définitions des politiques et des rôles IAM. Le développeur envoie le code vers un CodeCommit référentiel CodePipeline , puis lance le `RolesPipeline` pipeline.
2. CodeBuild valide les fichiers JSON à l'aide d'IAM Access Analyzer. En cas de détection de problèmes de sécurité ou d'erreur, le processus de déploiement est arrêté.
3. S'il n'y a aucun résultat lié à la sécurité ou à une erreur, les fichiers JSON sont envoyés au `RolesBucket` compartiment S3.
4. Une CloudFormation macro AWS implémentée en tant que fonction AWS Lambda lit ensuite les fichiers JSON depuis le `RolesBucket` compartiment et les transforme en types de ressources AWS CloudFormation IAM.
5. Une CloudFormation pile AWS prédéfinie installe, met à jour ou supprime les politiques et les rôles IAM du compte.

Automatisation et mise à l'échelle

CloudFormation Les modèles AWS qui déploient automatiquement ce modèle sont fournis dans le référentiel du pipeline de rôles GitHub IAM.

Outils

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- IAM Access Analyzer vous aide à identifier les ressources de votre organisation et les comptes, tels que les compartiments S3 ou les rôles IAM, qui sont partagés avec une entité externe. Cela vous permet d'identifier les accès involontaires à vos ressources et à vos données.
- AWS Serverless Application Model (AWS SAM) est un framework open source qui vous aide à créer des applications sans serveur dans le cloud AWS.

Code

Le code source et les modèles de ce modèle sont disponibles dans le référentiel de pipelines de rôles GitHub IAM.

Épopées

Cloner le référentiel

Tâche	Description	Compétences requises
Clonez le référentiel d'échantillons.	Clonez le référentiel de pipelines de rôles GitHub IAM sur votre machine locale.	Développeur d'applications, AWS général

Déployer le RolesPipeline pipeline

Tâche	Description	Compétences requises
Déployez le pipeline.	1. Accédez au répertoire qui contient le référentiel cloné.	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	2. **Important** Exécutez la `make deploy bucket=<bucket_name>` commande. : vous devez `<bucket_name>` remplacer par le nom du compartiment S3 existant. 3. Exécutez la `aws codepipeline get-pipeline –name RolesPipeline` commande pour vérifier si votre déploiement est réussi.	

Tâche	Description	Compétences requises
Clonez le référentiel du pipeline.	1. La CloudFormation pile `RolesPipeline` AWS crée le `roles-pipeline-repo` CodeCommit référentiel. 2. Connectez-vous à l'AWS Management Console, ouvrez la CodeCommit console AWS, puis copiez l'URL du CodeCommit référentiel pour le cloner sur votre machine locale. Pour plus d'informations à ce sujet, consultez Connect to an AWS CodeCommit repository dans la CodeCommit documentation AWS.	Développeur d'applications, AWS général

Testez le RolesPipeline pipeline

Tâche	Description	Compétences requises
Testez le RolesPipeline pipeline avec des politiques et des rôles IAM valides.	1. Créez des fichiers JSON pour vos politiques et rôles IAM. Vous pouvez utiliser les exemples contenus dans le `role-example` répertoire depuis le GitHub `IAM roles pipeline` référentiel.	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	2. **Important** Définissez vos politiques et rôles IAM avec les configurations requises. : Assurez-vous de suivre le format décrit dans le `ReadMe` fichier issu du GitHub `IAM roles pipeline` référentiel. 3. Transférez les modifications dans le `roles-pipeline-repo` CodeCommit référentiel. 4. Vérifiez la mise en œuvre du `RolesPipeline` pipeline. 5. Assurez-vous que les politiques et les rôles IAM sont correctement déployés dans le compte. 6. Validez s'il existe une limite d'autorisations associée aux politiques ou aux rôles IAM. Pour plus d'informations à ce sujet, consultez la section Limites d'autorisations pour les entités IAM dans la documentation IAM.	

Tâche	Description	Compétences requises
Testez le RolesPipeline pipeline avec des politiques et des rôles IAM non valides.	1. Modifiez le `roles-pipeline-repo` CodeCommit référentiel et incluez des rôles ou des politiques IAM non valides. Par exemple, vous pouvez utiliser une action qui n'existe pas ou une version de politique IAM non valide. 2. Vérifiez la mise en œuvre du pipeline. IAM Access Analyzer arrête le pipeline pendant la phase de validation s'il détecte des politiques ou des rôles IAM non valides.	Développeur d'applications, AWS général

Nettoyage de vos ressources

Tâche	Description	Compétences requises
Préparez-vous au nettoyage.	Videz les compartiments S3, puis exécutez la `destroy` commande.	Développeur d'applications, AWS général
Supprimez la RolesStack pile.	1. Le `RolesPipeline` pipeline crée une CloudFormation pile `RolesStack` AWS qui déploie les politique s et les rôles IAM. Vous devez supprimer cette	Développeur d'applications, AWS général

Tâche	Description	Compétences requises
	pile avant de supprimer le `RolesPipeline` pipeline. 2. Connectez-vous à l'AWS Management Console, ouvrez la CloudForm ation console AWS, puis choisissez la `RolesStac k` pile et choisissez Delete.	
Supprimez la RolesPipeline pile.	Pour supprimer la CloudForm ation pile `RolesPipeline` AWS, suivez les instructions du ReadMefichier dans le `IAM roles pipeline` référentiel Github.	Développeur d'applications, AWS général

Ressources connexes

- Analyseur d'accès IAM - Validation des politiques (blog d'actualités AWS)
- Utilisation de CloudFormation macros AWS pour effectuer un traitement personnalisé sur des modèles (CloudFormation documentation AWS)
- Création de fonctions Lambda avec Python (documentation AWS Lambda)

Intégration bidirectionnelle au logiciel AWS Security Hub Jira

Créée par Joaquin Rinaudo (AWS)

Récapitulatif

Cette solution prend en charge une intégration bidirectionnelle entre AWS Security Hub et Jira. Grâce à cette solution, vous pouvez créer et mettre à jour automatiquement et manuellement des tickets Jira à partir des résultats du Security Hub. Les équipes de sécurité peuvent utiliser cette intégration pour informer les équipes de développement des problèmes de sécurité graves nécessitant une action.

La solution vous permet de :

- Sélectionnez les contrôles Security Hub qui créent ou mettent à jour automatiquement les tickets dans Jira.
- Dans la console Security Hub, utilisez les actions personnalisées de Security Hub pour augmenter manuellement les tickets dans Jira.
- Attribuez automatiquement des tickets dans Jira en fonction des Compte AWS balises définies dans AWS Organizations. Si cette balise n'est pas définie, un destinataire par défaut est utilisé.
- Supprimez automatiquement les résultats du Security Hub marqués comme faussement positifs ou présentant un risque accepté dans Jira.
- Fermez automatiquement un ticket Jira lorsque le résultat correspondant est archivé dans Security Hub.
- Rouvrez les tickets Jira lorsque les résultats de Security Hub se reproduisent.

Flux de travail Jira

La solution utilise un flux de travail Jira personnalisé qui permet aux développeurs de gérer et de documenter les risques. Au fur et à mesure que le problème progresse dans le flux de travail, l'intégration bidirectionnelle garantit que le statut du ticket Jira et la découverte du Security Hub sont synchronisés entre les flux de travail des deux services. Ce flux de travail est un dérivé de SecDevOps Risk Workflow de Dinis Cruz, sous licence Apache version 2.0. Nous vous recommandons d'ajouter une condition de flux de travail Jira afin que seuls les membres de votre équipe de sécurité puissent modifier le statut du ticket.

Pour un exemple de ticket Jira généré automatiquement par cette solution, consultez la section Informations supplémentaires de ce modèle.

Conditions préalables et limitations

Prérequis

- Si vous souhaitez déployer cette solution dans un AWS environnement multi-comptes :
  - Votre environnement multi-comptes est actif et géré par AWS Organizations.
  - Security Hub est activé sur votre Comptes AWS.
  - Dans AWS Organizations, vous avez désigné un compte administrateur Security Hub.
  - Vous disposez d'un rôle multi-comptes AWS Identity and Access Management (IAM) autorisé à accéder `AWSOrganizationsReadOnlyAccess` au compte de AWS Organizations gestion.
  - (Facultatif) Vous avez Comptes AWS `SecurityContactID` tagué votre Cette balise est utilisée pour attribuer des tickets Jira aux contacts de sécurité définis.
- Si vous souhaitez déployer cette solution en une seule fois Compte AWS :
  - Vous avez un actif Compte AWS.
  - Security Hub est activé sur votre Compte AWS.
- Une instance de centre de données Jira

> **Important**
>
> Cette solution prend en charge l'utilisation de Jira Cloud. Cependant, Jira Cloud ne prend pas en charge l'importation de flux de travail XML. Vous devez donc recréer manuellement le flux de travail dans Jira. Vous pouvez trouver les transitions et le statut dans le GitHub référentiel.

- Autorisations d'administrateur dans Jira
- L'un des jetons Jira suivants :
  - Pour Jira Enterprise, un jeton d'accès personnel (PAT). Pour plus d'informations, consultez la section Utilisation de jetons d'accès personnels (assistance Atlassian).
  - Pour Jira Cloud, un jeton d'API Jira. Pour plus d'informations, consultez Gérer les jetons d'API (support Atlassian).

Architecture

Cette section illustre l'architecture de la solution dans différents scénarios, par exemple lorsque le développeur et l'ingénieur en sécurité décident d'accepter le risque ou de résoudre le problème.

Scénario 1 : le développeur résout le problème

1. Security Hub génère une constatation par rapport à un contrôle de sécurité spécifié, tel que ceux de la norme AWS Foundational Security Best Practices.
2. Un CloudWatch événement Amazon associé à la recherche et à l'`CreateJIRAaction` déclenche une AWS Lambda fonction.
3. La fonction Lambda utilise son fichier de configuration et le `GeneratorId` champ du résultat pour déterminer si elle doit augmenter le résultat.
4. La fonction Lambda détermine que le résultat doit être augmenté, elle obtient le tag du compte depuis AWS Organizations le `SecurityContactID` compte de gestion. AWS Cet identifiant est associé au développeur et est utilisé comme identifiant de destinataire pour le ticket Jira.
5. La fonction Lambda utilise les informations d'identification enregistrées AWS Secrets Manager pour créer un ticket dans Jira. Jira avertit le développeur.
6. Le développeur répond à la constatation de sécurité sous-jacente et, dans Jira, change le statut du ticket en`TEST FIX`.
7. Security Hub met à jour le résultat au fur `ARCHIVED` et à mesure qu'un nouvel événement est généré. Cet événement entraîne la fermeture automatique du ticket Jira par la fonction Lambda.

Scénario 2 : le développeur décide d'accepter le risque

1. Security Hub génère une constatation par rapport à un contrôle de sécurité spécifié, tel que ceux de la norme AWS Foundational Security Best Practices.
2. Un CloudWatch événement associé à la découverte et à l'`CreateJIRAaction` déclenche une fonction Lambda.
3. La fonction Lambda utilise son fichier de configuration et le `GeneratorId` champ du résultat pour déterminer si elle doit augmenter le résultat.
4. La fonction Lambda détermine que le résultat doit être augmenté, elle obtient le tag du compte depuis AWS Organizations le `SecurityContactID` compte de gestion. AWS Cet identifiant est associé au développeur et est utilisé comme identifiant de destinataire pour le ticket Jira.

5. La fonction Lambda utilise les informations d'identification stockées dans Secrets Manager pour créer un ticket dans Jira. Jira avertit le développeur.
6. Le développeur décide d'accepter le risque et, dans Jira, change le statut du ticket en`AWAITING RISK ACCEPTANCE`.
7. L'ingénieur en sécurité examine la demande et trouve que la justification commerciale est appropriée. L'ingénieur de sécurité change le statut du ticket Jira en`ACCEPTED RISK`. Cela ferme le ticket Jira.
8. Un événement CloudWatch quotidien lance la fonction d'actualisation Lambda, qui identifie les tickets Jira fermés et met à jour les résultats correspondants du Security Hub en conséquence. `SUPPRESSED`

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- Amazon CloudWatch Events vous aide à surveiller les événements du système pour vos AWS ressources en utilisant des règles pour faire correspondre les événements et les acheminer vers des fonctions ou des flux.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.

Référentiel de code

Le code de ce modèle est disponible sur GitHub, dans le référentiel aws-securityhub-jira-software-integration. Il inclut l'exemple de code et le flux de travail Jira pour cette solution.

Épopées

Configuration de Jira

Tâche	Description	Compétences requises
Importez le flux de travail.	En tant qu'administrateur de Jira, importez le `issue-workflow.xml` fichier dans votre instance de Jira Data Center. Si vous utilisez Jira Cloud, vous devez créer le flux de travail en fonction des `assets/jira-cloud-status.png` fichiers `assets/jira-cloud-transitions.png` et. Les fichiers se trouvent dans le référentiel aws-securityhub-jira-software-integration dans GitHub. Pour obtenir des instructions, consultez Utiliser le XML pour créer un flux de travail (documentation Jira).	Administrateur Jira
Activez et attribuez le flux de travail.	Les flux de travail sont inactifs tant que vous ne les affectez pas à un schéma de flux de travail. Vous attribuez ensuite le schéma de flux de travail à un projet.	Administrateur Jira

Tâche	Description	Compétences requises
	1. Pour votre projet, assurez-vous d'avoir identifié un schéma de type de problème pour le projet. Vous pouvez créer un nouveau type de problème ou en sélectionner un existant, tel queBug. 2. Assignez le flux de travail importé à un schéma de flux de travail conformément aux instructions de la section Activer un flux de travail (documentation Jira). 3. Assignez le schéma de flux de travail à un projet conformément aux instructions de la section Associer un schéma de flux de travail à un projet (documentation Jira).	

Configurer les paramètres de la solution

Tâche	Description	Compétences requises
Configurez les paramètres de la solution.	1. Dans le dossier conf, ouvrez`params_prod.shfile` . 2. Fournissez des valeurs pour les paramètres suivants :	Administrateur système AWS

Tâche	Description	Compétences requises
	• `ORG_ACCOUNT_ID` — L'identifiant de compte de votre compte AWS Organizations de gestion. La solution lit les balises de compte et attribue des tickets aux contacts de sécurité spécifiqu es définis dans ces Compte AWS balises. • `ORG_ROLE`— Le nom du rôle IAM utilisé pour accéder au compte de AWS Organizations gestion. Ce rôle doit disposer d'`OrganizationsReadOnlyAccess` autorisations. • `EXTERNAL_ID` — Paramètre facultatif si vous utilisez un ID externe pour assumer le rôle IAM défini dans`ORG_ROLE`. Pour plus d'informations, consultez Comment utiliser un identifiant externe (documentation IAM). • `JIRA_DEFAULT_ASSIGNEE` — Il s'agit du responsable par défaut de Jira pour tous les	

Tâche	Description	Compétences requises
	problèmes de sécurité. Ce responsable par défaut est utilisé dans le cas où le compte n'est pas correctement étiqueté ou si le rôle ne peut pas être assumé. • `JIRA_INSTANCE` — L'adresse HTTPS de votre point de terminaison Jira au format suivant : `team-<team-id>.atlassian.net/` • `JIRA_PROJECT_KEY` — Le nom de la clé de projet Jira utilisée pour créer des tickets, par exemple `SEC` ou`TEST`. Ce projet doit déjà exister dans Jira. • `ISSUE_TYPE` — Le nom du schéma de type de problème attribué au projet dans Jira, tel que `Bug` ou`Security Issue`. • `REGIONS`— Liste des Région AWS codes dans lesquels vous souhaitez déployer cette solution, par exemple`eu-west-1`.	

Tâche	Description	Compétences requises
	3. Enregistrez et fermez le fichier de paramètres de solution.	
Identifiez les résultats que vous souhaitez automatiser.	1. Ouvrez la console Security Hub. 2. Dans le volet de navigation du Security Hub, sélectionnez Findings. 3. Choisissez le titre de la recherche. 4. Choisissez l'ID de recherche. Cela affiche le code JSON complet pour le résultat. 5. Dans le JSON, copiez la chaîne dans le `GeneratorId` champ. Cette valeur est au format ASFF (AWS Security Finding Format). Par exemple, `aws-foundational-security-best-practices/v/1.0.0/S3.1` correspond aux résultats du contrôle de sécurité S3.1, le paramètre S3 Block Public Access doit être activé. 6. Répétez ces étapes jusqu'à ce que vous ayez copié toutes les `GeneratorID` valeurs des résultats que vous souhaitez automatiser.	

Tâche	Description	Compétences requises
Ajoutez les résultats au fichier de configuration.	1. Dans src/code, ouvrez le `config.jsonconfig` fichier. 2. Collez les `Generator ID` valeurs que vous avez récupérées dans l'article précédent dans le `default` paramètre et utilisez des virgules pour séparer chaque identifiant. 3. Enregistrez et fermez le fichier de configuration . L'exemple de code suivant montre l'automatisation des `aws-foundational-security-best-practices/v/1.0.0/S3.1` résultats `aws-foundational-security-best-practices/v/1.0.0/SNS.1` et. `{ "Controls" : { "eu-west-1": [ "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22" ], "default": [ aws-foundational-security-best-practices/v/1.0.0/SNS.1,`	Administrateur système AWS

Tâche	Description	Compétences requises

	<pre>aws-foundational-security-best-practices/v/1.0.0/S3.1
	     ]
	    }
	 }</pre>
	Note
	Vous pouvez choisir d'automatiser différents résultats pour chacun d'entre eux Région AWS. Une bonne pratique pour éviter la duplication des résultats consiste à sélectionner une seule région pour automatiser la création de contrôles liés à l'IAM.	

Déployez l'intégration

Tâche	Description	Compétences requises
Déployez l'intégration.	Dans un terminal de ligne de commande, entrez la commande suivante : <pre>./deploy.sh prod</pre>	Administrateur système AWS

Tâche	Description	Compétences requises
Téléchargez les informations d'identification Jira dans Secrets Manager.	1. Ouvrez la console Secrets Manager. 2. Sous Secrets, choisissez Store a new secret (Stocker un nouveau secret). 3. Pour Secret type (Type de secret), choisissez Other type of secret (Autre type de secret). 4. Si vous utilisez Jira Enterprise, pour les paires clé/valeur, procédez comme suit : • Dans la première ligne, entrez `auth` dans la zone clé, puis entrez `token_auth` dans la zone valeur. • Ajoutez une deuxième ligne, entrez `token` dans la zone clé, puis entrez votre jeton d'accès personnel dans la zone valeur. Si vous utilisez Jira Cloud, pour les paires clé/valeur, procédez comme suit : • Dans la première ligne, entrez `auth` dans la zone clé, puis entrez `basic_auth` dans la zone valeur.	Administrateur système AWS

Tâche	Description	Compétences requises
	• Ajoutez une deuxième ligne, entrez `token` dans la zone clé, puis entrez votre jeton d'API dans la zone valeur. • Ajoutez une troisième ligne, entrez `email` dans la zone clé, puis entrez votre adresse e-mail dans la zone de valeur. 5. Choisissez Suivant. 6. Dans Nom du secret`Jira-Token` , entrez, puis au bas de la page, choisissez Next. 7. Sur la page Secret rotation (Rotation du secret), gardez Disable automatic rotation (Désactiver la rotation automatique), puis au bas de la page, choisissez Next (Suivant). 8. Sur la page Review (Vérification), passez en revue vos paramètres, puis choisissez Store (Stocker).	

Tâche	Description	Compétences requises
Créez l'action personnalisée Security Hub.	1. Pour chacun Région AWS, dans le AWS Command Line Interface (AWS CLI), utilisez la create-action-targetcommande pour créer une action personnalisée Security Hub nomméeCreateJiraIssue . `aws securityhub create-action-target --name "CreateJiraIssue" \ --description "Create ticket in JIRA" \ --id "CreateJiraIssue" --region $<aws-region>` 2. Ouvrez la console Security Hub. 3. Dans le volet de navigation du Security Hub, sélectionnez Findings. 4. Dans la liste des résultats , sélectionnez les résultats que vous souhaitez escalader. 5. Dans le menu Actions, choisissezCreateJiraIssue .	Administrateur système AWS

Ressources connexes

- AWS Connecteur de gestion des services pour Jira Service Management
- AWS Norme sur les meilleures pratiques de sécurité fondamentales

Informations supplémentaires

Exemple de ticket Jira

Lorsqu'une découverte spécifique du Security Hub se produit, cette solution crée automatiquement un ticket Jira. Le billet contient les informations suivantes :

- Titre — Le titre identifie le problème de sécurité dans le format suivant :

```
AWS Security Issue :: <AWS account ID> :: <Security Hub finding title>
```

- Description — La section de description du ticket décrit le contrôle de sécurité associé à la découverte, inclut un lien vers la découverte dans la console Security Hub et fournit une brève description de la manière de gérer le problème de sécurité dans le flux de travail Jira.

Voici un exemple de ticket Jira généré automatiquement.

Titre	AWS Problème de sécurité : 012345678912 : : Lambda.1 Les politiques relatives aux fonctions Lambda devraient interdire l'accès public.
Description	Quel est le problème ? Nous avons détecté une faille de sécurité dans le Compte AWS 012345678912 dont vous êtes responsable. Ce contrôle vérifie si la politique AWS Lambda fonctionnelle attachée à la ressource Lambda interdit l'accès public. Si la politique de la fonction Lambda autorise l'accès public, le contrôle échoue. <Link to Security Hub finding>

Que dois-je faire avec le billet ?

- Accédez au compte et vérifiez la configura tion. Confirmez avoir travaillé sur le ticket en le déplaçant vers « Alloué pour correction ». Une fois résolu, déplacé vers le correctif de test afin que la sécurité valide le problème soit résolu.
- Si vous pensez que le risque doit être accepté, déplacez-le vers « En attente d'acceptation du risque ». Cela nécessitera un examen par un ingénieur en sécurité.
- Si vous pensez qu'il s'agit d'un faux positif, remplacez-le par « Marquer comme faux positif ». Cela sera examiné par un ingénieur en sécurité et rouvrir/fermé en conséquence.

Créez un pipeline pour les images de conteneurs renforcées à l'aide d' EC2 Image Builder et de Terraform

Créée par Mike Saintcross (AWS) et Andrew Ranes (AWS)

Récapitulatif

Ce modèle crée un pipeline EC2 Image Builder qui produit une image de conteneur de base Amazon Linux 2 renforcée. Terraform est utilisé comme outil d'infrastructure en tant que code (IaC) pour configurer et approvisionner l'infrastructure utilisée pour créer des images de conteneurs renforcées. La recette vous aide à déployer une image de conteneur Amazon Linux 2 basée sur Docker qui a été renforcée conformément à Red Hat Enterprise Linux (RHEL) 7 STIG version 3, version 7 – Medium. (Voir STIG-Build-Linux-Medium la version 2022.2.1 dans la section des composants Linux STIG de la documentation EC2 Image Builder.) C'est ce qu'on appelle une image de contenant doré.

La version inclut deux EventBridge règles Amazon. Une règle lance le pipeline d'images du conteneur lorsque le résultat d'Amazon Inspector est élevé ou critique, de sorte que les images non sécurisées sont remplacées. Cette règle exige que le scan amélioré Amazon Inspector et Amazon Elastic Container Registry (Amazon ECR) soit activé. L'autre règle envoie des notifications à une file d'attente Amazon Simple Queue Service (Amazon SQS) après un transfert d'image réussi vers le référentiel Amazon ECR, afin de vous aider à utiliser les dernières images de conteneur.

> **Note**
>
> Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.

Conditions préalables et limitations

Prérequis

- Un compte AWS dans lequel vous pouvez déployer l'infrastructure.
- Interface de ligne de commande AWS (AWS CLI) installée pour définir vos informations d'identification AWS pour le déploiement local.
- Terraform a été téléchargé et configuré en suivant les instructions de la documentation Terraform.
- Git (si vous effectuez le provisionnement depuis une machine locale).

- Rôle au sein du compte AWS que vous pouvez utiliser pour créer des ressources AWS.
- Toutes les variables définies dans le fichier .tfvars. Vous pouvez également définir toutes les variables lorsque vous appliquez la configuration Terraform.

Limites

- Cette solution crée une infrastructure Amazon Virtual Private Cloud (Amazon VPC) qui inclut une passerelle NAT et une passerelle Internet pour la connectivité Internet depuis son sous-réseau privé. Vous ne pouvez pas utiliser les points de terminaison VPC, car le processus d'amorçage d'AWS Task Orchestrator and Executor () AWSTOE installe la version 2 de l'interface de ligne de commande AWS depuis Internet.

Versions du produit

- Amazon Linux 2
- AWS CLI version 1.1 ou ultérieure

Architecture

Pile technologique cible

Ce modèle crée 43 ressources, dont :

- Deux compartiments Amazon Simple Storage Service (Amazon S3) : un pour les fichiers des composants du pipeline et un pour l'accès au serveur et aux journaux de flux Amazon VPC
- Un référentiel Amazon ECR
- Un cloud privé virtuel (VPC) qui contient un sous-réseau public, un sous-réseau privé, des tables de routage, une passerelle NAT et une passerelle Internet
- Un pipeline, une recette et des composants d' EC2 Image Builder
- Une image de conteneur
- Une clé AWS Key Management Service (AWS KMS) pour le chiffrement des images
- Une file d'attente SQS
- Trois rôles : un pour exécuter le pipeline EC2 Image Builder, un profil d'instance pour EC2 Image Builder et un pour les EventBridge règles
- Deux EventBridge règles

Structure du module Terraform

Pour le code source, consultez le GitHub référentiel Terraform EC2 Image Builder Container Hardening Pipeline.

```
### components.tf
### config.tf
### dist-config.tf
### files
#   ###assumption-policy.json
### hardening-pipeline.tfvars
### image.tf
### infr-config.tf
### infra-network-config.tf
### kms-key.tf
### main.tf
### outputs.tf
### pipeline.tf
### recipes.tf
### roles.tf
### sec-groups.tf
### trigger-build.tf
### variables.tf
```

Détails du module

- `components.tf`contient une ressource de téléchargement Amazon S3 pour télécharger le contenu du `/files` répertoire. Vous pouvez également y ajouter des fichiers YAML de composants personnalisés de manière modulaire.
- `/files`contient les `.yml` fichiers qui définissent les composants utilisés dans`components.tf`.
- `image.tf`contient les définitions du système d'exploitation de l'image de base. C'est ici que vous pouvez modifier les définitions d'un autre pipeline d'images de base.
- `infr-config.tf`et `dist-config.tf` contiennent les ressources nécessaires à l'infrastructure AWS minimale nécessaire pour créer et distribuer l'image.
- `infra-network-config.tf`contient l'infrastructure VPC minimale dans laquelle déployer l'image du conteneur.
- `hardening-pipeline.tfvars`contient les variables Terraform à utiliser au moment de l'application.
- `pipeline.tf`crée et gère un pipeline EC2 Image Builder dans Terraform.

- `recipes.tf`est l'endroit où vous pouvez spécifier différents mélanges de composants pour créer des recettes de conteneurs.
- `roles.tf`contient les définitions de la politique AWS Identity and Access Management (IAM) pour le profil d'instance Amazon Elastic Compute Cloud (Amazon EC2) et le rôle de déploiement du pipeline.
- `trigger-build.tf`contient les EventBridge règles et les ressources de file d'attente SQS.

Architecture cible

Le diagramme illustre le flux de travail suivant :

1. EC2 Image Builder crée une image de conteneur en utilisant la recette définie, qui installe les mises à jour du système d'exploitation et applique le RHEL Medium STIG à l'image de base Amazon Linux 2.
2. L'image renforcée est publiée dans un registre Amazon ECR privé, et une EventBridge règle envoie un message à une file d'attente SQS lorsque l'image a été publiée avec succès.
3. Si Amazon Inspector est configuré pour une analyse améliorée, il analyse le registre Amazon ECR.
4. Si Amazon Inspector génère un résultat de gravité critique ou élevé pour l'image, une EventBridge règle déclenche la réexécution du pipeline EC2 Image Builder et la publication d'une image récemment durcie.

Automatisation et mise à l'échelle

- Ce modèle décrit comment provisionner l'infrastructure et créer le pipeline sur votre ordinateur. Cependant, il est destiné à être utilisé à grande échelle. Au lieu de déployer les modules Terraform localement, vous pouvez les utiliser dans un environnement multi-comptes, tel qu'un environnement AWS Control Tower with Account Factory pour Terraform. Dans ce cas, vous devez utiliser un compartiment S3 d'état principal pour gérer les fichiers d'état Terraform au lieu de gérer l'état de configuration localement.
- Pour une utilisation à grande échelle, déployez la solution sur un compte central, tel qu'un compte Shared Services ou Common Services, à partir d'un modèle de compte Control Tower ou landing zone, et autorisez les comptes clients à accéder au référentiel Amazon ECR et à la clé AWS KMS. Pour plus d'informations sur la configuration, consultez l'article Re:Post Comment autoriser un compte secondaire à envoyer ou à extraire des images dans mon référentiel d'images Amazon

ECR ? Par exemple, dans un distributeur automatique de comptes ou Account Factory for Terraform, ajoutez des autorisations à chaque ligne de base de compte ou à chaque ligne de base de personnalisation du compte pour donner accès à ce référentiel Amazon ECR et à cette clé de chiffrement.

- Une fois le pipeline d'images de conteneur déployé, vous pouvez le modifier à l'aide des fonctionnalités EC2 d'Image Builder, telles que les composants, qui vous aident à intégrer davantage de composants dans la version Docker.
- La clé AWS KMS utilisée pour chiffrer l'image du conteneur doit être partagée entre les comptes dans lesquels l'image est destinée à être utilisée.
- Vous pouvez ajouter la prise en charge d'autres images en dupliquant l'intégralité du module Terraform et en modifiant les attributs suivants : `recipes.tf`
  - Passez `parent_image = "amazonlinux:latest"` à un autre type d'image.
  - Modifiez `repository_name` pour pointer vers un référentiel Amazon ECR existant. Cela crée un autre pipeline qui déploie un type d'image parent différent dans votre référentiel Amazon ECR existant.

Outils

Outils

- Terraform (provisionnement iAC)
- Git (en cas de provisionnement local)
- CLI AWS version 1 ou version 2 (en cas de provisionnement local)

Code

Le code de ce modèle se trouve dans le GitHub référentiel Terraform EC2 Image Builder Container Hardening Pipeline. Pour utiliser l'exemple de code, suivez les instructions de la section suivante.

Épopées

Fournir l'infrastructure

Tâche	Description	Compétences requises

Configurez les informations d'identification locales.	Configurez vos informations d'identification temporaires AWS.
	
	1. Vérifiez si l'AWS CLI est installée :
	
	``
	$ aws --version
	aws-cli/1.16.249
	 Python/3.6.8...
	``
	
	• La version de l'AWS CLI doit être 1.1 ou ultérieure.
	• Si la commande est introuvable, installez l'AWS CLI.
	2. Exécutez `aws configure` et fournissez les valeurs suivantes :
	
	``
	$ aws configure
	AWS Access Key ID
	 [*************xxxx
	]: <Your AWS access
	 key ID>
	AWS Secret Access Key
	 [**************xxx
	x]: <Your AWS secret
	 access key>
	Default region name:
	 [us-east-1]: <Your
	 desired Region for
	 deployment>
	``
		AWS DevOps

Tâche	Description	Compétences requises
	`Default output format [None]: <Your desired output format>`	

Pour cloner le référentiel.	1. Clonez le référentiel fourni avec ce modèle. Vous pouvez utiliser le protocole HTTPS ou le protocole Secure Shell (SSH).
	
	HTTPS :
	
	`git clone https://github.com/aws-samples/terraform-ec2-image-builder-container-hardening-pipeline`
	
	SSH :
	
	`git clone git@github.com:aws-samples/terraform-ec2-image-builder-container-hardening-pipeline.git`
	2. Accédez à votre répertoire local qui contient cette solution :
	
	`cd terraform-ec2-image-builder-container-hardening-pipeline`
		AWS DevOps

Tâche	Description	Compétences requises

Mettez à jour les variables.	Mettez à jour les variables du `hardening-pipeline.tfvars` fichier en fonction de votre environnement et de la configuration souhaitée. Vous devez fournir le vôtre`account_id`. Cependant, vous devez également modifier le reste des variables en fonction du déploiement souhaité. Toutes les variables sont obligatoires.
	
	`account_id = "<DEPLOYMENT-ACCOUNT-ID>"`
	`aws_region = "us-east-1"`
	`vpc_name = "example-hardening-pipeline-vpc"`
	`kms_key_alias = "image-builder-container-key"`
	`ec2_iam_role_name = "example-hardening-instance-role"`
	`hardening_pipeline_role_name = "example-hardening-pipeline-role"`
	`aws_s3_ami_resources_bucket = "example-hardening-ami-resources-bucket-0123"`
	`image_name = "example-hardening-al2-container-image"`
		AWS DevOps

Tâche	Description	Compétences requises

	`ecr_name = "example-hardening-container-repo"`
	`recipe_version = "1.0.0"`
	`ebs_root_vol_size = 10`
	
	Voici une description de chaque variable :
	
	• `account_id` – Le numéro de compte AWS dans lequel vous souhaitez déployer la solution.
	• `aws_region` – La région AWS dans laquelle vous souhaitez déployer la solution.
	• `vpc_name`– Le nom de votre infrastructure VPC.
	• `kms_key_alias` – Le nom de clé AWS KMS à utiliser par la configuration de l'infrastructure EC2 Image Builder.
	• `ec2_iam_role_name` – Nom du rôle qui sera utilisé comme profil d' EC2 instance.
	• `hardening_pipeline_role_name` – Nom du rôle qui sera utilisé pour déployer le pipeline de renforcement.	

Tâche	Description	Compétences requises
	• `aws_s3_ami_resources_bucket` – Nom d'un compartiment S3 qui hébergera tous les fichiers nécessaires à la création du pipeline et des images du conteneur. • `image_name` – Le nom de l'image du conteneur. Cette valeur doit être comprise entre 3 et 50 caractères et ne doit contenir que des caractères alphanumériques et des tirets. • `ecr_name`– Le nom du registre Amazon ECR dans lequel les images du conteneur seront stockées. • `recipe_version` – La version de la recette imagée. La valeur par défaut est 1.0.0. • `ebs_root_vol_size` – Taille (en gigaoctets) du volume racine Amazon Elastic Block Store (Amazon EBS). La valeur par défaut est de 10 gigaoctets.	

Tâche	Description	Compétences requises
Initialisez Terraform.	Après avoir mis à jour les valeurs de vos variables, vous pouvez initialiser le répertoire de configuration Terraform. L'initialisation d'un répertoire de configuration télécharge et installe le fournisseur AWS, qui est défini dans la configuration. `terraform init` Vous devriez voir un message indiquant que Terraform a été correctement initialisé et identifiant la version du fournisseur qui a été installée.	AWS DevOps
Déployez l'infrastructure et créez une image de conteneur.	Utilisez la commande suivante pour initialiser, valider et appliquer les modules Terraform à l'environnement en utilisant les variables définies dans votre fichier : `.tfvars` `terraform init && terraform validate && terraform apply -var-file *.tfvars -auto-approve`	AWS DevOps

Tâche	Description	Compétences requises
Personnalisez le conteneur.	Vous pouvez créer une nouvelle version d'une recette de conteneur une fois qu' EC2 Image Builder a déployé le pipeline et la recette initiale. Vous pouvez ajouter n'importe lequel des 31 composant s disponibles dans EC2 Image Builder pour personnal iser la construction du conteneur. Pour plus d'informa tions, consultez la section Composants de la section Créer une nouvelle version d'une recette de conteneur dans la documentation EC2 d'Image Builder.	Administrateur AWS

Valider les ressources

Tâche	Description	Compétences requises
Validez le provisionnement de l'infrastructure AWS.	Une fois que vous avez terminé avec succès votre première `apply` commande Terraform, si vous effectuez le provisionnement localemen t, vous devriez voir cet extrait dans le terminal de votre machine locale :	AWS DevOps

Tâche	Description	Compétences requises
	`Apply complete! Resources: 43 added, 0 changed, 0 destroyed.`	
Validez les ressources individuelles de l'infrastructure AWS.	Pour valider les ressources individuelles qui ont été déployées, si vous approvisionnez localement, vous pouvez exécuter la commande suivante : `terraform state list` Cette commande renvoie une liste de 43 ressources.	AWS DevOps

Supprimer des ressources

Tâche	Description	Compétences requises
Supprimez l'image de l'infrastructure et du conteneur.	Lorsque vous avez fini de travailler avec votre configuration Terraform, vous pouvez exécuter la commande suivante pour supprimer des ressources : `terraform init && terraform validate && terraform destroy -var-file *.tfvars -auto-approve`	AWS DevOps

Résolution des problèmes

Problème	Solution
Erreur lors de la validation des informations d'identification du fournisseur	Lorsque vous exécutez la `destroy` commande Terraform `apply` ou depuis votre machine locale, vous pouvez rencontrer une erreur similaire à la suivante : `Error: configuring Terraform AWS Provider: error validating provider credentials: error calling sts:GetCallerIdentity: operation error STS: GetCallerIdentity, https response error StatusCode: 403, RequestID: 123456a9-fbc1-40ed-b8d8-513d0133ba7f, api error InvalidClientTokenId: The security token included in the request is invalid.` Cette erreur est due à l'expiration du jeton de sécurité pour les informations d'identification utilisées dans la configuration de votre machine locale. Pour résoudre l'erreur, consultez la section Définir et afficher les paramètres de configuration dans la documentation de l'AWS CLI.

Ressources connexes

- Pipeline de renforcement des conteneurs Terraform EC2 Image Builder (référentiel) GitHub
- EC2 Documentation d'Image Builder
- AWS Control Tower Account Factory pour Terraform (article de blog AWS)
- État du compartiment S3 du backend (documentation Terraform)
- Installation ou mise à jour de la dernière version de l'AWS CLI (documentation de l'AWS CLI)

- Télécharger Terraform

Centralisez la gestion des clés d'accès IAM dans AWS Organizations à l'aide de Terraform

Créée par Aarti Rajput (AWS), Chintamani Aphale (AWS), T.V.R.L.Phani Kumar Dadi (AWS), Pradip kumar Pandey (AWS), Mayuri Shinde (AWS) et Pratap Kumar Nanda (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus

L'application des règles de sécurité pour les clés et les mots de passe est une tâche essentielle pour chaque organisation. L'une des règles importantes consiste à alterner les clés AWS Identity and Access Management (IAM) à intervalles réguliers pour renforcer la sécurité. Les clés d'accès AWS sont généralement créées et configurées localement chaque fois que les équipes souhaitent accéder à AWS depuis l'interface de ligne de commande AWS (AWS CLI) ou depuis des applications extérieures à AWS. Pour garantir une sécurité renforcée au sein de l'entreprise, les anciennes clés de sécurité doivent être modifiées ou supprimées une fois que les exigences ont été satisfaites ou à intervalles réguliers. Le processus de gestion de la rotation des clés entre plusieurs comptes d'une organisation est long et fastidieux. Ce modèle vous permet d'automatiser le processus de rotation en utilisant Account Factory for Terraform (AFT) et les services AWS.

Le modèle offre les avantages suivants :

- Gère votre clé d'accès IDs et vos clés d'accès secrètes sur tous les comptes de votre organisation à partir d'un emplacement central.
- Fait automatiquement pivoter les variables `AWS_ACCESS_KEY_ID` d'`AWS_SECRET_ACCESS_KEY`environnement et.
- Applique le renouvellement si les informations d'identification de l'utilisateur sont compromises.

Le modèle utilise Terraform pour déployer les fonctions AWS Lambda, les règles EventBridge Amazon et les rôles IAM. Une EventBridge règle s'exécute à intervalles réguliers et appelle une fonction Lambda qui répertorie toutes les clés d'accès utilisateur en fonction de leur date de création. Des fonctions Lambda supplémentaires créent un nouvel identifiant de clé d'accès et une nouvelle clé d'accès secrète, si la clé précédente est antérieure à la période de rotation que vous avez définie (par exemple, 45 jours), et en informent un administrateur de sécurité à l'aide d'Amazon

Simple Notification Service (Amazon SNS) et d'Amazon Simple Email Service (Amazon SES). Les secrets sont créés dans AWS Secrets Manager pour cet utilisateur, l'ancienne clé d'accès secrète est stockée dans Secrets Manager et les autorisations d'accès à l'ancienne clé sont configurées. Pour garantir que l'ancienne clé d'accès ne soit plus utilisée, elle est désactivée après une période d'inactivité (par exemple, 60 jours, soit 15 jours après la rotation des clés dans notre exemple). Après une période tampon inactive (par exemple, 90 jours ou 45 jours après la rotation des clés dans notre exemple), les anciennes clés d'accès sont supprimées d'AWS Secrets Manager. Pour une architecture et un flux de travail détaillés, consultez la section Architecture.

Conditions préalables et limitations

- Une zone de landing zone pour votre organisation créée à l'aide d'AWS Control Tower (version 3.1 ou ultérieure)
- Account Factory for Terraform (AFT) configuré avec trois comptes :
  - Le compte de gestion de l'organisation gère l'ensemble de l'organisation à partir d'un emplacement central.
  - Le compte de gestion AFT héberge le pipeline Terraform et déploie l'infrastructure dans le compte de déploiement.
  - Le compte de déploiement déploie cette solution complète et gère les clés IAM à partir d'un emplacement central.
- Terraform version 0.15.0 ou ultérieure pour le provisionnement de l'infrastructure dans le compte de déploiement.
- Adresse e-mail configurée dans Amazon Simple Email Service (Amazon SES).
- (Recommandé) Pour améliorer la sécurité, déployez cette solution dans un sous-réseau privé (compte de déploiement) au sein d'un cloud privé virtuel (VPC). Vous pouvez fournir les détails du VPC et du sous-réseau lorsque vous personnalisez les variables (voir Personnaliser les paramètres du pipeline de code dans la section Epics).

Architecture

Référentiels AFT

Ce modèle utilise Account Factory for Terraform (AFT) pour créer toutes les ressources AWS requises et le pipeline de code pour déployer les ressources dans un compte de déploiement. Le pipeline de code s'exécute dans deux référentiels :

- La personnalisation globale contient le code Terraform qui s'appliquera à tous les comptes enregistrés auprès d'AFT.
- Les personnalisations de compte contiennent du code Terraform qui s'exécutera dans le compte de déploiement.

Détails de la ressource

Les CodePipeline tâches AWS créent les ressources suivantes dans le compte de déploiement :

- EventBridge Règle AWS et règle configurée
- Fonction Lambda `account-inventory`
- Fonction Lambda `IAM-access-key-rotation`
- Fonction Lambda `Notification`
- Compartiment Amazon Simple Storage Service (Amazon S3) contenant un modèle d'e-mail
- Politique IAM requise

Architecture

Le diagramme illustre les éléments suivants :

1. Une EventBridge règle appelle la fonction `account-inventory` Lambda toutes les 24 heures.
2. La fonction `account-inventory` Lambda interroge AWS Organizations pour obtenir la liste de tous les comptes IDs, noms de comptes et e-mails relatifs aux comptes AWS.
3. La fonction `account-inventory` Lambda lance une fonction `IAM-access-key-auto-rotation` Lambda pour chaque compte AWS et lui transmet les métadonnées pour un traitement supplémentaire.
4. La fonction `IAM-access-key-auto-rotation` Lambda utilise un rôle IAM supposé pour accéder au compte AWS. Le script Lambda exécute un audit de tous les utilisateurs et de leurs clés d'accès IAM dans le compte.
5. Le seuil de rotation des clés IAM (période de rotation) est configuré en tant que variable d'environnement lorsque la fonction `IAM-access-key-auto-rotation` Lambda est déployée. Si la période de rotation est modifiée, la fonction `IAM-access-key-auto-rotation` Lambda est redéployée avec une variable d'environnement mise à jour. Vous pouvez configurer des paramètres pour définir la période de rotation, la période d'inactivité pour les anciennes clés

et le tampon inactif après lequel les anciennes clés seront supprimées (voir Personnaliser les paramètres du pipeline de code dans la section Epics).

6. La fonction `IAM-access-key-auto-rotation` Lambda valide l'âge de la clé d'accès en fonction de sa configuration. Si l'âge de la clé d'accès IAM n'a pas dépassé la période de rotation que vous avez définie, la fonction Lambda n'entreprend aucune autre action.
7. Si l'âge de la clé d'accès IAM dépasse la période de rotation que vous avez définie, la fonction `IAM-access-key-auto-rotation` Lambda crée une nouvelle clé et fait pivoter la clé existante.
8. La fonction Lambda enregistre l'ancienne clé dans Secrets Manager et limite les autorisations aux utilisateurs dont les clés d'accès ne sont pas conformes aux normes de sécurité. La fonction Lambda crée également une politique basée sur les ressources qui permet uniquement au principal IAM spécifié d'accéder au secret et de le récupérer.
9. La fonction `IAM-access-key-rotation` Lambda appelle la fonction Lambda`Notification`.
10. La fonction `Notification` Lambda interroge le compartiment S3 à la recherche d'un modèle d'e-mail et génère dynamiquement des e-mails avec les métadonnées d'activité pertinentes.
11. La fonction `Notification` Lambda appelle Amazon SES pour qu'il prenne d'autres mesures.
12. Amazon SES envoie un e-mail contenant les informations pertinentes à l'adresse e-mail du titulaire du compte.

Outils

Services AWS

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser. Ce modèle nécessite des rôles et des autorisations IAM.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Secrets Manager vous aide à remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation.
- Amazon Simple Email Service (Amazon SES) vous permet d'envoyer et de recevoir des e-mails en utilisant vos propres adresses e-mail et domaines.

Autres outils

- Terraform est un outil d'infrastructure en tant que code (IaC) HashiCorp qui vous aide à créer et à gérer des ressources sur site et dans le cloud.

Référentiel de code

Les instructions et le code de ce modèle sont disponibles dans le référentiel de rotation des clés d'accès GitHub IAM. Vous pouvez déployer le code dans le compte de déploiement central d'AWS Control Tower pour gérer la rotation des clés depuis un emplacement central.

Bonnes pratiques

- Pour IAM, consultez les meilleures pratiques de sécurité dans la documentation IAM.
- Pour la rotation des clés, consultez les instructions relatives à la mise à jour des clés d'accès dans la documentation IAM.

Épopées

Configuration des fichiers sources

Tâche	Description	Compétences requises
Pour cloner le référentiel.	1. Clonez le GitHub référentiel de rotation des clés d'accès IAM : `$ git clone https://github.com/aws-samples/centralized-iam-key-management-aws-organizations-terraform.git` 2. Vérifiez que votre copie locale du référentiel contient trois dossiers :	DevOps ingénieur

Tâche	Description	Compétences requises

	`$ cd Iam-Access-keys-Rotation`
	`$ ls`
	`org-account-customization`
	`global-account-customization`
	`account-customization`	

Configurer les comptes

Tâche	Description	Compétences requises

Configurez le compte d'amorçage.	Dans le cadre du processus de démarrage AFT, vous devriez avoir un dossier appelé `aft-bootstrap` sur votre machine locale.
	1. Copiez manuellement tous les fichiers Terraform de votre GitHub org-account-customizationdossier local vers votre `aft-bootstrap` dossier.
	2. Exécutez les commandes Terraform pour configurer le rôle global entre comptes dans le compte de gestion AWS Control Tower :
	`$ cd aft-bootstrap`
	`$ terraform init`
		DevOps ingénieur

Tâche	Description	Compétences requises
	`$ terraform apply –auto-approve`	

Configurez les personnalisations globales.	Dans le cadre de la configuration du dossier AFT, vous devriez avoir un dossier appelé `aft-global-customizations` sur votre machine locale.
	1. Copiez manuellement tous les fichiers Terraform de votre GitHub global-account-customizationdossier local vers votre `aft-global-customizations/terraform` dossier.
	2. Envoyez le code à AWS CodeCommit :
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps ingénieur

Tâche	Description	Compétences requises

Configurez les personnalisations du compte.	Dans le cadre de la configuration du dossier AFT, vous devez être appelé dossier `aft-account-customizations` sur votre machine locale.
	1. Créez un dossier avec votre numéro de compte vendeur.
	2. Copiez manuellement tous les fichiers Terraform de votre dossier de GitHub personnalisation de compte local vers votre dossier. `aft-account-customizations/<vended account>/terraform`
	3. Envoyez le code à AWS CodeCommit :
	`$ git add *`
	`$ git commit -m "message"`
	`$ git push`
		DevOps ingénieur

Personnaliser les paramètres du pipeline de code

Tâche	Description	Compétences requises
Personnalisez les paramètres du pipeline de code autres que Terraform pour tous les comptes.	Créez un fichier appelé `input.auto.tfvars` dans le `aft-global-customizations/terraform/` dossier et fournissez les	DevOps ingénieur

Tâche	Description	Compétences requises
	données d'entrée requises. Consultez le fichier du GitHub référentiel pour les valeurs par défaut.	

Tâche	Description	Compétences requises
Personnalisez les paramètres du pipeline de code pour le compte de déploiement.	Créez un fichier appelé `input.auto.tfvars` dans le `aft-account-customizations/<AccountName>/terraform/` dossier et envoyez le code à AWS CodeCommit. Le transfert de code vers AWS lance CodeCommit automatiquement le pipeline de code. Spécifiez les valeurs des paramètres en fonction des exigences de votre organisation, notamment les suivantes (voir le fichier dans le référentiel Github pour les valeurs par défaut) : • `s3_bucket_name` — Un nom de compartiment unique pour le modèle d'e-mail. • `s3_bucket_prefix` — Un nom de dossier dans le compartiment S3. • `admin_email_address` — L'adresse e-mail de l'administrateur qui doit recevoir la notification. • `org_list_account` — Le numéro de compte du compte de gestion.	DevOps ingénieur

Tâche	Description	Compétences requises
	• `rotation_period` — Le nombre de jours après lesquels une clé doit passer d'active à inactive. • `inactive_period` — Le nombre de jours après lesquels les touches pivotées doivent être désactivées. Cette valeur doit être supérieure à la valeur de`rotation_period` . • `inactive_buffer` — Le délai de grâce entre la rotation et la désactivation d'une clé. • `recovery_grace_period` — Le délai de grâce entre la désactivation et la suppression d'une clé. • `dry_run_flag` — Réglez sur true si vous souhaitez envoyer une notification à l'administrateur à des fins de test, sans rotation des touches. • `store_secrets_in_central_account` — Définissez ce paramètre sur true si vous souhaitez enregistrer le secret dans le compte de déploiement. Si la variable est définie sur false (valeur par défaut), le	

Tâche	Description	Compétences requises
	secret sera stocké dans le compte du membre. • `credential_replication_region` — La région AWS dans laquelle vous souhaitez déployer la fonction Lambda et les compartiments S3 pour le modèle d'e-mail. • `run_lambda_in_vpc` — Définissez sur true pour exécuter la fonction Lambda dans le VPC. • `vpc_id`— L'ID VPC du compte de déploiement, si vous souhaitez exécuter la fonction Lambda dans le VPC. • `vpc_cidr`— La plage CIDR pour le compte de déploiement. • `subnet_id` — Le sous-réseau du compte IDs de déploiement. • `create_smtp_endpoint` — Réglez sur true si vous souhaitez activer le point de terminaison de messagerie.	

Valider la rotation des clés

Tâche	Description	Compétences requises
Validez la solution.	1. À partir de l'AWS Management Console, connectez-vous au compte de déploiement. 2. Ouvrez la console IAM et vérifiez si les informations d'identification de l'utilisateur (clé d'accès IDs et clés secrètes) sont modifiées comme indiqué. 3. Après avoir fait pivoter une clé IAM, confirmez les points suivants : • L'ancienne valeur est stockée dans AWS Secrets Manager. • Le nom du secret est au format`Account_<account ID>_User_<username>_AccessKey` . • L'utilisateur que vous avez spécifié dans le `admin_email_address` paramètre reçoit une notification par e-mail concernant la rotation des touches.	DevOps ingénieur

Élargir la solution

Tâche	Description	Compétences requises
Personnalisez la date de notification par e-mail.	Si vous souhaitez envoyer des notifications par e-mail un jour précis avant de désactiver la clé d'accès, vous pouvez mettre à jour la fonction `IAM-access-key-auto-rotation` Lambda avec les modifications suivantes : 1. Définissez une variable appelée`notify-period` . 2. Ajoutez une `if` condition `main.py` avant de désactiver la clé : `If (keyage>rotation-period-notify-period){ send_to_notifier(context, aws_account_id, account_name, resource_owner, resource_actions[resource_owner], dryrun, config.emailTemplateAudit) }`	DevOps ingénieur

Résolution des problèmes

Problème	Solution
La tâche `account-inventory` Lambda échoue lors de la mise `AccessDenied` en liste des comptes.	Si vous rencontrez ce problème, vous devez valider les autorisations : 1. Connectez-vous au compte que vous venez de vendre, ouvrez la CloudWatch console Amazon, puis consultez le groupe `/aws/lambda/account-inventory-lambda` de CloudWatch journaux. 2. Dans les derniers CloudWatch journaux, identifiez le numéro de compte à l'origine du problème de refus d'accès. 3. Connectez-vous au compte de gestion AWS Control Tower et confirmez que le rôle `allow-list-account` a été créé. 4. Si le rôle n'existe pas, réexécutez le code Terraform à l'aide de la commande. `terraform apply` 5. Choisissez l'onglet Compte de confiance et vérifiez que le même compte est approuvé.

Ressources connexes

- Pratiques recommandées par Terraform (documentation Terraform)
- Bonnes pratiques de sécurité dans l'IAM (documentation IAM)
- Meilleures pratiques pour la rotation des clés (documentation IAM)

Consultez une CloudFront distribution Amazon pour la journalisation des accès, les versions HTTPS et TLS

Créée par SaiJeevan Devireddy (AWS) et Bijesh Bal (AWS)

Récapitulatif

Ce modèle vérifie une CloudFront distribution Amazon pour s'assurer qu'elle utilise le protocole HTTPS, qu'elle utilise le protocole TLS (Transport Layer Security) version 1.2 ou ultérieure et que la journalisation des accès est activée. CloudFront est un service fourni par Amazon Web Services (AWS) qui accélère la distribution de votre contenu Web statique et dynamique, tel que les fichiers .html, .css, .js et les fichiers image, à vos utilisateurs. CloudFront diffuse votre contenu par le biais d'un réseau mondial de centres de données appelés emplacements périphériques. Lorsqu'un utilisateur demande le contenu que vous diffusez CloudFront, la demande est acheminée vers l'emplacement périphérique offrant le moins de latence (délai), afin que le contenu soit diffusé avec les meilleures performances possibles.

Ce modèle fournit une fonction AWS Lambda qui est lancée lorsqu'Amazon CloudWatch Events détecte l'appel CloudFront d'API CreateDistributionCreateDistributionWithTags, ou. UpdateDistribution La logique personnalisée de la fonction Lambda évalue toutes les CloudFront distributions créées ou mises à jour dans le compte AWS. Il envoie une notification de violation à l'aide d'Amazon Simple Notification Service (Amazon SNS) s'il détecte les violations suivantes :

- Contrôles globaux :
  - Le certificat personnalisé n'utilise pas la version 1.2 du protocole TLS
  - La journalisation est désactivée pour la distribution
- Contrôles d'origine :
  - Origin n'est pas configuré avec TLS version 1.2
  - La communication avec l'origine est autorisée sur un protocole autre que HTTPS
- Contrôles de comportement :
  - Comportement par défaut, la communication est autorisée sur un protocole autre que HTTPS
  - La communication basée sur un comportement personnalisé est autorisée sur un protocole autre que HTTPS

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une adresse e-mail à laquelle vous souhaitez recevoir les notifications de violation

Limites

- Ce contrôle de sécurité ne vérifie pas les distributions Cloudfront existantes, sauf si une mise à jour a été apportée à la distribution.
- CloudFront est considéré comme un service mondial et n'est pas lié à une région AWS spécifique. Toutefois, la journalisation des API Amazon CloudWatch Logs et AWS Cloudtrail pour les services internationaux a lieu dans la région de l'est des États-Unis (Virginie du Nord) (`us-east-1`). Par conséquent, ce contrôle de sécurité pour CloudFront doit être déployé et maintenu dans`us-east-1`. Ce déploiement unique surveille toutes les distributions pour CloudFront. Ne déployez le contrôle de sécurité dans aucune autre région AWS. (Le déploiement dans d'autres régions empêchera le lancement des CloudWatch événements et de la fonction Lambda, et aucune notification SNS ne sera envoyée.)
- Cette solution a fait l'objet de tests approfondis avec des distributions de contenu CloudFront Web. Il ne couvre pas les distributions de streaming au moyen du protocole de messagerie en temps réel (RTMP).

Architecture

Pile technologique cible

- fonction Lambda
- Rubrique SNS
- EventBridge Règle Amazon

Architecture cible

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer le modèle ci-joint sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- AWS CloudFormation CloudFormation est un service qui vous aide à modéliser et à configurer les ressources AWS en utilisant l'infrastructure sous forme de code.
- Amazon EventBridge — EventBridge fournit un flux de données en temps réel à partir de vos propres applications, applications SaaS (logiciel en tant que service) et services AWS, en acheminant ces données vers des cibles telles que les fonctions Lambda.
- AWS Lambda — Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon SNS coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Le code ci-joint inclut :

- Un fichier .zip contenant le code Lambda (index.py)
- Un CloudFormation modèle (fichier .yml) que vous exécutez pour déployer le code Lambda

Épopées

Téléchargez le contrôle de sécurité

Tâche	Description	Compétences requises
Créez le compartiment S3 pour le code Lambda.	Sur la console Amazon S3, créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Votre compartiment S3 doit se trouver dans la région où vous prévoyez de déployer le code Lambda.	Architecte du cloud
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le code Lambda (fichier cloudfront_ssl_log _lambda.zip) fourni dans la section Pièces jointes dans le compartiment S3 que vous avez créé à l'étape précédent e.	Architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Sur la CloudFormation console AWS, dans la même région AWS que le compartiment S3, déployez le CloudFormation modèle	Architecte du cloud

Tâche	Description	Compétences requises
	(cloudfront-ssl-logging.yml) fourni dans la section Pièces jointes.	
Spécifiez le nom du compartiment S3.	Pour le paramètre S3 Bucket, spécifiez le nom du bucket S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud
Spécifiez le nom de clé Amazon S3 pour le fichier Lambda.	Pour le paramètre S3 Key, spécifiez l'emplacement Amazon S3 du fichier .zip de code Lambda dans votre compartiment S3. N'incluez pas de barres obliques en tête (par exemple, vous pouvez saisir lambda.zip ou controls/lambda.zip).	Architecte du cloud
Indiquez une adresse e-mail de notification.	Pour le paramètre E-mail de notification, indiquez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications de violation.	Architecte du cloud

Tâche	Description	Compétences requises
Définissez le niveau de journalisation.	Pour le paramètre Lambda Logging level, définissez le niveau de journalisation de votre fonction Lambda. Choisissez l'une des valeurs suivantes : • INFO pour obtenir des messages d'information détaillés sur la progression de l'application. • ERREUR pour obtenir des informations sur les événements d'erreur susceptibles de permettre à l'application de continuer à s'exécuter. • AVERTISSEMENT pour obtenir des informations sur des situations potentiel lement dangereuses.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le CloudFormation modèle a été déployé avec succès, une nouvelle rubrique SNS est créée et un message d'abonnement est envoyé à l'adresse e-mail que vous avez fournie. Vous devez confirmer cet abonnement par e-mail	Architecte du cloud

Tâche	Description	Compétences requises
	pour recevoir des notifications de violation.	

Ressources connexes

- CloudFormation Informations AWS
- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation)
- CloudFront journalisation (CloudFront documentation)
- Informations sur Amazon S3
- Informations sur AWS Lambda

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Vérifiez les entrées du réseau à hôte unique dans les règles d'entrée du groupe de sécurité pour et IPv4 IPv6

Créée par SaiJeevan Devireddy (AWS), Ganesh Kumar (AWS) et John Reynolds (AWS)

Récapitulatif

Ce modèle fournit un contrôle de sécurité qui vous avertit lorsque les ressources Amazon Web Services (AWS) ne répondent pas à vos spécifications. Il fournit une fonction AWS Lambda qui recherche les entrées du réseau à hôte unique dans les champs d'adresse source du protocole Internet version 4 (IPv4) et du groupe IPv6 de sécurité. La fonction Lambda est lancée lorsqu'Amazon CloudWatch Events détecte l'appel d'AuthorizeSecurityGroupIngressAPI Amazon Elastic Compute Cloud EC2 (Amazon). La logique personnalisée de la fonction Lambda évalue le masque de sous-réseau du bloc CIDR de la règle d'entrée du groupe de sécurité. S'il est déterminé que le masque de sous-réseau est autre que /32 (IPv4) ou /128 (IPv6), la fonction Lambda envoie une notification de violation à l'aide d'Amazon Simple Notification Service (Amazon Simple Notification Service) (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une adresse e-mail à laquelle vous souhaitez recevoir les notifications de violation

Limites

- Cette solution de surveillance de la sécurité est régionale et doit être déployée dans chaque région AWS que vous souhaitez surveiller.

Architecture

Pile technologique cible

- fonction Lambda
- Rubrique SNS

- EventBridge Règle Amazon

Architecture cible

Automatisation et évolutivité

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- AWS CloudFormation est un service qui vous aide à modéliser et à configurer les ressources AWS en utilisant l'infrastructure sous forme de code.
- Amazon EventBridge fournit un flux de données en temps réel provenant de vos propres applications, d'applications SaaS (Software as a Service) et de services AWS, et achemine ces données vers des cibles telles que les fonctions Lambda.
- AWS Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Le code ci-joint inclut :

- Un fichier .zip contenant le code de contrôle de sécurité Lambda () `index.py`
- Un CloudFormation modèle (`security-control.yml`fichier) que vous exécutez pour déployer le code Lambda

Épopées

Téléchargez le contrôle de sécurité

Tâche	Description	Compétences requises
Créez le compartiment S3 pour le code Lambda.	Sur la console Amazon S3, créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Votre compartiment S3 doit se trouver dans la région AWS où vous souhaitez déployer le contrôle d'entrée du groupe de sécurité.	Architecte du cloud
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le code Lambda (`security-control-lambda.zip` fichier) fourni dans la section Pièces jointes dans le compartiment S3 que vous avez créé à l'étape précédente.	Architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Modifiez la version de Python.	Téléchargez le CloudFormation modèle (`security-control.yml`) fourni dans la section Pièces jointes.	Architecte du cloud

Tâche	Description	Compétences requises
	Ouvrez le fichier et modifiez la version de Python pour qu'elle reflète la dernière version prise en charge par Lambda (actuellement Python 3.9). Par exemple, vous pouvez rechercher `python` dans le code et modifier la valeur `Runtime` de `python3.6` à`python3.9` . Pour obtenir les dernières informations sur la prise en charge des versions d'exécution de Python, consultez la documentation AWS Lambda.	
Déployez le CloudFormation modèle AWS.	Sur la CloudFormation console AWS, dans la même région AWS que le compartiment S3, déployez le CloudFormation modèle (`security-control.yml`).	Architecte du cloud
Spécifiez le nom du compartiment S3.	Pour le paramètre S3 Bucket, spécifiez le nom du bucket S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud

Tâche	Description	Compétences requises
Spécifiez le nom de clé Amazon S3 pour le fichier Lambda.	Pour le paramètre S3 Key, spécifiez l'emplacement Amazon S3 du fichier .zip de code Lambda dans votre compartiment S3. N'incluez pas de barres obliques (par exemple, vous pouvez saisir `lambda.zip` ou `controls/lambda.zip`).	Architecte du cloud
Indiquez une adresse e-mail de notification.	Pour le paramètre E-mail de notification, indiquez l'adresse e-mail à laquelle vous souhaitez recevoir les notifications de violation.	Architecte du cloud

Tâche	Description	Compétences requises
Définissez le niveau de journalisation.	Pour le paramètre Lambda Logging level, définissez le niveau de journalisation de votre fonction Lambda. Choisissez l'une des valeurs suivantes : • INFO pour obtenir des messages d'information détaillés sur la progression de l'application. • ERREUR pour obtenir des informations sur les événements d'erreur susceptibles de permettre à l'application de continuer à s'exécuter. • AVERTISSEMENT pour obtenir des informations sur des situations potentiel lement dangereuses.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le CloudFormation modèle a été déployé avec succès, une nouvelle rubrique SNS est créée et un message d'abonnement est envoyé à l'adresse e-mail que vous avez fournie. Vous devez confirmer cet abonnement par e-mail	Architecte du cloud

Tâche	Description	Compétences requises
	pour recevoir des notifications de violation.	

Ressources connexes

- CloudFormation Informations AWS
- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Groupes de sécurité pour votre VPC (documentation Amazon VPC)
- Informations sur Amazon S3
- Informations sur AWS Lambda

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Choisissez un flux d'authentification Amazon Cognito pour les applications d'entreprise

Créée par Michael Daehnert (AWS) et Fabian Jahnke (AWS)

Récapitulatif

Amazon Cognito assure l'authentification, l'autorisation et la gestion des utilisateurs pour les applications Web et mobiles. Il offre des fonctionnalités avantageuses pour l'authentification des identités fédérées. Pour le rendre opérationnel, les architectes techniques doivent décider de la manière dont ils souhaitent utiliser ces fonctionnalités.

Amazon Cognito prend en charge plusieurs flux pour les demandes d'authentification. Ces flux définissent la manière dont vos utilisateurs peuvent vérifier leur identité. Le choix du flux d'authentification à utiliser dépend des exigences spécifiques de votre application et peut s'avérer complexe. Ce modèle vous aide à choisir le flux d'authentification le mieux adapté à votre application d'entreprise. Il suppose que vous avez déjà une connaissance de base d'Amazon Cognito, d'OpenID Connect (OIDC) et de la fédération, et il vous explique en détail les différents flux d'authentification fédérés.

Cette solution est destinée aux décideurs techniques. Il vous aide à comprendre les différents flux d'authentification et à les adapter aux exigences de votre application. Les responsables techniques doivent recueillir les informations nécessaires pour démarrer les intégrations avec Amazon Cognito. Étant donné que les entreprises se concentrent principalement sur la fédération SAML, ce modèle inclut des descriptions des groupes d'utilisateurs Amazon Cognito dotés de la fédération SAML.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Rôles et autorisations AWS Identity and Access Management (IAM) avec accès complet à Amazon Cognito
- (Facultatif) Accès à votre fournisseur d'identité (IdP), tel que Microsoft Entra ID, Active Directory Federation Service (AD FS) ou Okta
- Un haut niveau d'expertise pour votre application
- Connaissances de base d'Amazon Cognito, d'OpenID Connect (OIDC) et de la fédération

Limites

- Ce modèle se concentre sur les groupes d'utilisateurs et les fournisseurs d'identité Amazon Cognito. Pour plus d'informations sur les groupes d'identités Amazon Cognito, consultez la section Informations supplémentaires.

Architecture

Utilisez le tableau suivant pour vous aider à choisir un flux d'authentification. Plus d'informations sur chaque flux sont fournies dans cette section.

Avez-vous besoin d'une machine-to-machine authentification ?	Votre application est-elle une application Web dont le frontend est affiché sur le serveur ?	Votre application est-elle une application monopage (SPA) ou une application frontale mobile ?	Votre application nécessite-t-elle des jetons d'actualisation pour une fonctionnalité « Maintenez-moi connecté » ?	Le frontend propose-t-il un mécanisme de redirection basé sur le navigateur ?	Flux Amazon Cognito recommandé
Oui	Non	Non	Non	Non	Flux d'informations d'identification du client
Non	Oui	Non	Oui	Oui	Flux de code d'autorisation
Non	Non	Oui	Oui	Oui	Flux de code d'autorisation avec clé de preuve pour

					l'échange de code (PKCE)
Non	Non	Non	Non	Non	Flux de mots de passe du propriétaire des ressources

* Le flux de mots de passe du propriétaire de la ressource ne doit être utilisé qu'en cas d'absolue nécessité. Pour plus d'informations, consultez la section relative au flux de mots de passe du propriétaire de la ressource dans ce modèle.

Flux d'informations d'identification du client

Le flux d'informations d'identification du client est le plus court des flux Amazon Cognito. Il doit être utilisé si les systèmes ou les services communiquent entre eux sans aucune interaction de l'utilisateur. Le système demandeur utilise l'ID client et le secret du client pour récupérer un jeton d'accès. Étant donné que les deux systèmes fonctionnent sans interaction avec l'utilisateur, aucune étape de consentement supplémentaire n'est requise.

Le diagramme illustre les éléments suivants :

1. L'application 1 envoie une demande d'authentification avec l'ID client et le secret du client au point de terminaison Amazon Cognito, et elle récupère un jeton d'accès.
2. L'application 1 utilise ce jeton d'accès pour chaque appel suivant à l'application 2.
3. L'application 2 valide le jeton d'accès avec Amazon Cognito.

Ce flux doit être utilisé :

- Pour les communications entre applications sans interaction avec l'utilisateur

Ce flux ne doit pas être utilisé :

- Pour toute communication dans laquelle des interactions avec les utilisateurs sont possibles

Flux de code d'autorisation

Le flux de code d'autorisation est destiné à l'authentification Web classique. Dans ce flux, le backend gère tous les échanges et le stockage des jetons. Le client basé sur un navigateur ne voit pas les jetons réels. Cette solution est utilisée pour les applications écrites dans des frameworks tels que .NET Core, Jakarta Faces ou Jakarta Server Pages (JSP).

Le flux de code d'autorisation est un flux basé sur la redirection. Le client doit être en mesure d'interagir avec le navigateur Web ou un client similaire. Le client est redirigé vers un serveur d'authentification et s'authentifie auprès de ce serveur. Si le client s'authentifie correctement, il est redirigé vers le serveur.

Le diagramme illustre les éléments suivants :

1. Le client envoie une demande au serveur Web.
2. Le serveur Web redirige le client vers Amazon Cognito à l'aide d'un code d'état HTTP 302. Le client suit automatiquement cette redirection vers le login IdP configuré.
3. L'IdP vérifie s'il existe une session de navigateur existante du côté de l'IdP. S'il n'en existe aucun, l'utilisateur est invité à s'authentifier en fournissant son nom d'utilisateur et son mot de passe. L'IdP envoie un jeton SAML à Amazon Cognito.
4. Amazon Cognito fonctionne avec un jeton Web JSON (JWT), en particulier un jeton de code. Le serveur Web calls /oauth2/token qui échange le jeton de code contre un jeton d'accès. Le serveur Web envoie l'ID client et le secret du client à Amazon Cognito pour validation.
5. Le jeton d'accès est utilisé pour chaque appel ultérieur à d'autres applications.
6. D'autres applications valident le jeton d'accès avec Amazon Cognito.

Ce flux doit être utilisé :

- Si l'utilisateur est en mesure d'interagir avec le navigateur Web ou le client. Le code de l'application est exécuté et affiché sur le serveur pour s'assurer qu'aucun secret n'est exposé au navigateur.

Ce flux ne doit pas être utilisé :

- Pour les applications d'une seule page (SPAs) ou les applications mobiles, car elles sont affichées sur le client et ne doivent pas utiliser les secrets du client.

Flux de code d'autorisation avec PKCE

Le flux de code d'autorisation avec clé de preuve pour l'échange de code (PKCE) doit être utilisé pour les applications d'une seule page et les applications mobiles. Il est le successeur du flux implicite et est plus sécurisé car il utilise le protocole PKCE. PKCE est une extension de l'octroi de code d'autorisation OAuth 2.0 pour les clients publics. Le PKCE protège contre le rachat de codes d'autorisation interceptés.

Le diagramme illustre les éléments suivants :

1. L'application crée un vérificateur de code et un défi de code. Il s'agit de valeurs uniques bien définies qui sont envoyées à Amazon Cognito pour référence future.
2. L'application appelle le the /oauth2/authorization point de terminaison d'Amazon Cognito. Il redirige automatiquement l'utilisateur vers le login IdP configuré.
3. L'IdP vérifie la présence d'une session existante. S'il n'en existe aucun, l'utilisateur est invité à s'authentifier en fournissant son nom d'utilisateur et son mot de passe. L'IdP envoie un jeton SAML à Amazon Cognito.
4. Une fois qu'Amazon Cognito a renvoyé avec succès un jeton de code, le serveur Web doit calls / oauth2/token échanger le jeton de code contre un jeton d'accès.
5. Le jeton d'accès est utilisé pour chaque appel ultérieur à d'autres applications.
6. Les autres applications valident le jeton d'accès avec Amazon Cognito.

Ce flux doit être utilisé :

- Pour SPAs nos applications mobiles

Ce flux ne doit pas être utilisé :

- Si le backend de l'application gère l'authentification

Flux de mots de passe du propriétaire des ressources

Le flux de mots de passe du propriétaire de la ressource est destiné aux applications ne disposant pas de fonctionnalités de redirection. Il est construit en créant un formulaire de connexion dans votre propre application. La connexion est vérifiée sur Amazon Cognito via un appel de CLI ou de

SDK au lieu de s'appuyer sur des flux de redirection. La fédération n'est pas possible dans ce flux d'authentification car la fédération nécessite des redirections basées sur le navigateur.

Le diagramme illustre les éléments suivants :

1. L'utilisateur saisit ses informations d'identification sur un formulaire de connexion fourni par l'application.
2. L'interface de ligne de commande AWS (AWS CLI) appelle Amazon admin-initiated-authCognito.

> **Note**
>
> Vous pouvez également utiliser AWS SDKs au lieu de l'AWS CLI.

3. Amazon Cognito renvoie un jeton d'accès.
4. Le jeton d'accès est utilisé pour chaque appel ultérieur à d'autres applications.
5. Les autres applications valident le jeton d'accès avec Amazon Cognito.

Ce flux doit être utilisé :

- Lors de la migration de clients existants qui utilisent une logique d'authentification directe (telle que l'authentification d'accès de base ou l'authentification d'accès OAuth par condensé) en convertissant les informations d'identification stockées en jeton d'accès

Ce flux ne doit pas être utilisé :

- Si vous souhaitez utiliser des identités fédérées
- Si votre application prend en charge les redirections

Outils

Services AWS

- Amazon Cognito fournit des fonctionnalités d'authentification, d'autorisation et de gestion des utilisateurs pour les applications Web et mobiles.

Autres outils

- Le débogueur de jetons Web JSON (JWT) est un outil de validation JWT basé sur le Web.

Épopées

Évaluez votre candidature

Tâche	Description	Compétences requises
Définissez les exigences en matière d'authentification.	Évaluez votre application en fonction de vos exigences d'authentification spécifiques.	Développeur d'applications, architecte d'applications
Alignez les exigences avec les flux d'authentification.	Dans la section Architecture, utilisez le tableau de décision et les explications de chaque flux pour choisir votre flux d'authentification Amazon Cognito.	Développeur d'applications, AWS général, architecte d'applications

Configuration du groupe d'utilisateurs Amazon Cognito

Tâche	Description	Compétences requises
Créez un groupe d'utilisateurs.	1. Connectez-vous à la console de gestion AWS, puis ouvrez la console Amazon Cognito. 2. Créez un nouveau groupe d'utilisateurs de Cognito. Pour obtenir des instructions, consultez la section Groupes d'utilisateurs Amazon Cognito. 3. Mettez à jour les paramètres et les attributs du groupe d'utilisateurs selon les	AWS général

Tâche	Description	Compétences requises
	besoins. Par exemple, définissez une politique de mot de passe pour le groupe d'utilisateurs. Ne créez pas encore de clients d'applications.	
(Facultatif) Configurez un fournisseur d'identité.	1. Créez un fournisseur d'identité SAML dans le groupe d'utilisateurs Amazon Cognito. Pour obtenir des instructions, consultez la section Ajout et gestion de fournisseurs d'identité SAML dans un groupe d'utilisateurs. 2. Configurez votre fournisseur d'identité SAML tiers pour qu'il fonctionne avec la fédération pour les groupes d'utilisateurs Amazon Cognito. Pour plus d'informations, consultez la section Configuration de votre fournisseur d'identité SAML tiers. Si vous utilisez AD FS, consultez Création d'une fédération AD FS pour votre application Web à l'aide des groupes d'utilisateurs Amazon Cognito (article de blog AWS).	AWS général, administrateur de la fédération

Tâche	Description	Compétences requises
Créez un client d'application.	1. Créez un client d'application pour le groupe d'utilisateurs. Pour obtenir des instructions, consultez la section Création d'un client d'application. Remarques : • Modifiez les paramètres selon vos besoins, tels que l'expiration des jetons. • Si votre flux d'authentification ne nécessite pas de secret client, décochez la case Générer un secret client. 2. Choisissez les paramètres du client de l'application pour modifier son intégration en une connexion à un groupe d'utilisateurs (nom d'utilisateur et mot de passe) ou une connexion fédérée via un IdP basé sur SAML. 3. Activez votre IdP en définissant URLs et en définissant des OAuth flux ou des portées selon vos besoins.	AWS général

Intégrer l'application à Amazon Cognito

Tâche	Description	Compétences requises
Détails de l'intégration d'Exchange Amazon Cognito.	En fonction de votre flux d'authentification, partagez les informations Amazon Cognito avec l'application, telles que l'identifiant du groupe d'utilisa teurs et l'identifiant du client de l'application.	Développeur d'applications, AWS général
Implémentez l'authentification Amazon Cognito.	Cela dépend du flux d'authent ification que vous avez choisi, de votre langage de programmation et des frameworks que vous utilisez. Pour certains liens permettan t de démarrer, consultez la section Ressources connexes.	Développeur d’applications

Ressources connexes

Documentation AWS

- Flux d'authentification du groupe d'utilisateurs
- Vérification d'un jeton Web JSON
- Accédez aux services AWS depuis une application ASP.NET Core à l'aide des pools d'identités Amazon Cognito
- Cadres et SDKs :
  - Authentification Amazon Amplify
  - Exemples de fournisseurs d'identité Amazon Cognito (documentation du kit SDK AWS pour Java 2.x)
  - Authentification des utilisateurs avec Amazon Cognito (documentation du kit SDK AWS pour .NET)

Articles de blog AWS

- Authorization @Edge à l'aide de cookies : protégez votre CloudFront contenu Amazon contre le téléchargement par des utilisateurs non authentifiés
- Création d'une fédération AD FS pour votre application Web à l'aide des groupes d'utilisateurs Amazon Cognito

Partenaires de mise en œuvre

- Partenaires AWS pour les solutions d'authentification

Informations supplémentaires

FAQ

Pourquoi le flux implicite est-il obsolète ?

Depuis la sortie du framework OAuth 2.1, le flux implicite est marqué comme obsolète pour des raisons de sécurité. Comme alternative, veuillez utiliser le flux de code d'autorisation avec PKCE décrit dans la section Architecture.

Et si Amazon Cognito ne propose pas certaines fonctionnalités dont j'ai besoin ?

Les partenaires AWS proposent différentes intégrations pour les solutions d'authentification et d'autorisation. Pour plus d'informations, consultez la section Partenaires AWS pour les solutions d'authentification.

Qu'en est-il des flux du pool d'identités Amazon Cognito ?

Les groupes d'utilisateurs et les identités fédérées Amazon Cognito sont destinés à l'authentification. Les groupes d'identités Amazon Cognito sont utilisés pour autoriser l'accès aux ressources AWS en demandant des informations d'identification AWS temporaires. L'échange de jetons d'identification et de jetons d'accès pour les pools d'identités n'est pas abordé dans ce modèle. Pour plus d'informations, consultez Quelle est la différence entre les groupes d'utilisateurs et les groupes d'identités Amazon Cognito et Scénarios Amazon Cognito courants.

Étapes suivantes

Ce modèle fournit une vue d'ensemble des flux d'authentification Amazon Cognito. L'étape suivante consiste à choisir l'implémentation détaillée du langage de programmation de l'application. Plusieurs

langages SDKs et frameworks que vous pouvez utiliser avec Amazon Cognito. Pour des références utiles, consultez la section Ressources connexes.

Créez des règles AWS Config personnalisées à l'aide AWS CloudFormation Guard de politiques

Créée par Andrew Lok (AWS), Kailash Havildar (AWS), Nicole Brown (AWS) et Tanya Howell (AWS)

Récapitulatif

AWS Configles règles vous aident à évaluer vos AWS ressources et l'état de leur configuration cible. Il existe deux types de AWS Config règles : les règles gérées et les règles personnalisées. Vous pouvez créer des règles personnalisées avec AWS Lambda des fonctions ou avec AWS CloudFormation Guard(GitHub), une policy-as-code langue.

Les règles créées avec Guard fournissent un contrôle plus granulaire que les règles gérées, et elles sont généralement plus faciles à configurer que les règles Lambda entièrement personnalisées. Cette approche permet aux ingénieurs et aux architectes de créer des règles sans avoir besoin de connaître Python, NodeJS ou Java, qui sont nécessaires pour déployer des règles personnalisées via Lambda.

Ce modèle fournit des modèles pratiques, des exemples de code et des approches de déploiement pour vous aider à adopter des règles personnalisées avec Guard. En utilisant ce modèle, un administrateur peut AWS Config créer des règles de conformité personnalisées dotées d'attributs d'éléments de configuration. Par exemple, les développeurs peuvent utiliser les politiques Guard sur les éléments de AWS Config configuration afin de surveiller en permanence l'état des AWS ressources déployées AWS et non déployées, de détecter les violations des règles et de lancer automatiquement des mesures correctives.

Objectifs

Après avoir lu ce modèle, vous devriez être capable de :

- Découvrez comment le code de politique de Guard interagit avec le AWS Config service.
- Déployez le scénario 1, qui est une règle AWS Config personnalisée qui utilise la syntaxe Guard pour valider la conformité des volumes chiffrés. Cette règle vérifie que le lecteur est en cours d'utilisation et que le type de lecteur est gp3.
- Déployez le scénario 2, qui est une règle AWS Config personnalisée qui utilise la syntaxe Guard pour valider la GuardDuty conformité d'Amazon. Cette règle vérifie que la protection Amazon Simple Storage Service (Amazon S3) et la protection Amazon Elastic Kubernetes Service (Amazon EKS) sont activées sur les GuardDuty enregistreurs.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- AWS Config, configurez dans votre Compte AWS

Limites

- Les règles personnalisées de Guard ne peuvent interroger que des paires clé-valeur dans un enregistrement JSON d'élément de configuration cible

Architecture

Vous appliquez la syntaxe Guard à une AWS Config règle en tant que politique personnalisée. AWS Config capture le JSON hiérarchique de chacune des ressources spécifiées. Le JSON de l'élément de AWS Config configuration contient des paires clé-valeur. Ces attributs sont utilisés dans la syntaxe Guard en tant que variables assignées à leur valeur correspondante.

Voici une explication de la syntaxe Guard. Les variables de l'élément de configuration JSON sont utilisées et précédées d'un `%` caractère.

```
# declare variable
let <variable name> = <'value'>

# create rule and assign condition and policy
    rule <rule name> when
        <CI json key> == <"CI json value"> {
            <top level CI json key>.<next level CI json key> == %<variable name>
        }
```

Scénario 1 : volumes Amazon EBS

Le scénario 1 déploie une règle AWS Config personnalisée qui utilise la syntaxe Guard pour valider la conformité des volumes chiffrés. Cette règle vérifie que le lecteur est en cours d'utilisation et que le type de lecteur est gp3.

Voici un exemple d'élément de AWS Config configuration pour le scénario 1. Cet élément de configuration comporte trois paires clé-valeur qui sont utilisées comme variables dans la politique

Guard : `volumestatusvolumeencryptionstatus`, et. `volumetype` La `resourceType` clé est également utilisée comme filtre dans la politique Guard.


```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-01-15T19:04:45.402Z",
  "configurationItemStatus": "ResourceDiscovered",
  "configurationStateId": "4444444444444",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:ec2:us-west-2:111111111111:volume/vol-222222222222",
  "resourceType": "AWS::EC2::Volume",
  "resourceId": "vol-222222222222",
  "awsRegion": "us-west-2",
  "availabilityZone": "us-west-2b",
  "resourceCreationTime": "2023-01-15T19:03:22.247Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [
    {
      "resourceType": "AWS::EC2::Instance",
      "resourceId": "i-33333333333333333",
      "relationshipName": "Is attached to Instance"
    }
  ],
  "configuration": {
    "attachments": [
      {
        "attachTime": "2023-01-15T19:03:22.000Z",
        "device": "/dev/xvda",
        "instanceId": "i-33333333333333333",
        "state": "attached",
        "volumeId": "vol-222222222222",
        "deleteOnTermination": true,
        "associatedResource": null,
        "instanceOwningService": null
      }
    ],
    "availabilityZone": "us-west-2b",
    "createTime": "2023-01-15T19:03:22.247Z",
    "encrypted": false,
    "kmsKeyId": null,
    "outpostArn": null,
```

```
    "size": 8,
    "snapshotId": "snap-55555555555555555",
    "state": "in-use",
    "volumeId": "vol-222222222222",
    "iops": 100,
    "tags": [],
    "volumeType": "gp2",
    "fastRestored": null,
    "multiAttachEnabled": false,
    "throughput": null,
    "sseType": null
  },
  "supplementaryConfiguration": {}
}
```

Voici un exemple d'utilisation de la syntaxe Guard pour définir les variables et les règles du scénario 1. Dans l'exemple suivant :

- Les trois premières lignes définissent les variables à l'aide de la `let` commande. Ils reçoivent un nom et une valeur dérivés des attributs de l'élément de configuration.
- Le bloc de `compliancecheck` règles ajoute une dépendance conditionnelle « when » qui recherche une paire `resourceType` clé-valeur correspondante. `AWS::EC2::Volume` Si une correspondance est trouvée, la règle passe en revue le reste des attributs JSON et recherche des correspondances dans les trois conditions suivantes : `stateencrypted`, et`volumeType`.

```
let volumestatus = 'available'
let volumetype = 'gp3'
let volumeencryptionstatus = true

    rule compliancecheck when
        resourceType == "AWS::EC2::Volume" {
            configuration.state == %volumestatus
            configuration.encrypted == %volumeencryptionstatus
            configuration.volumeType == %volumetype
        }
```

Pour connaître la politique personnalisée complète de Guard qui implémente cette règle personnalisée, consultez awsconfig-guard-cft.yaml ou awsconfig-guard-tf-ec2vol.json dans le référentiel de code. GitHub Pour le code HashiCorp Terraform qui déploie cette politique personnalisée dans Guard, voir awsconfig-guard-tf-example.json dans le référentiel de code.

Scénario 2 : GuardDuty conformité

Le scénario 2 déploie une règle AWS Config personnalisée qui utilise la syntaxe Guard pour valider la GuardDuty conformité d'Amazon. Cette règle vérifie que Amazon S3 Protection et Amazon EKS Protection sont activées sur les GuardDuty enregistreurs. Il vérifie également que les GuardDuty résultats sont publiés toutes les 15 minutes. Ce scénario pourrait être déployé dans l'ensemble Comptes AWS et Régions AWS au sein d'une organisation (in AWS Organizations).

Voici un exemple d'élément de AWS Config configuration pour le scénario 2. Cet élément de configuration comporte trois paires clé-valeur qui sont utilisées comme variables dans la politique Guard : `FindingPublishingFrequency`S3Logs, et. `Kubernetes` La `resourceType` clé est également utilisée comme filtre dans la politique.

```
{
  "version": "1.3",
  "accountId": "111111111111",
  "configurationItemCaptureTime": "2023-11-27T13:34:28.888Z",
  "configurationItemStatus": "OK",
  "configurationStateId": "7777777777777",
  "configurationItemMD5Hash": "",
  "arn": "arn:aws:guardduty:us-
west-2:111111111111:detector/66666666666666666666666666666666",
  "resourceType": "AWS::GuardDuty::Detector",
  "resourceId": "66666666666666666666666666666666",
  "resourceName": "66666666666666666666666666666666",
  "awsRegion": "us-west-2",
  "availabilityZone": "Regional",
  "resourceCreationTime": "2020-02-17T02:48:04.511Z",
  "tags": {},
  "relatedEvents": [],
  "relationships": [],
  "configuration": {
    "Enable": true,
    "FindingPublishingFrequency": "FIFTEEN_MINUTES",
    "DataSources": {
      "S3Logs": {
        "Enable": true
      },
      "Kubernetes": {
        "AuditLogs": {
          "Enable": true
        }
```

```
      }
    },

    "Id": "66666666666666666666666666666666",
    "Tags": []
  },
  "supplementaryConfiguration": {
    "CreatedAt": "2020-02-17T02:48:04.511Z"
  }
}
```

Voici un exemple d'utilisation de la syntaxe Guard pour définir les variables et les règles du scénario 2. Dans l'exemple suivant :

- Les trois premières lignes définissent les variables à l'aide de la `let` commande. Ils reçoivent un nom et une valeur dérivés des attributs de l'élément de configuration.
- Le bloc de `compliancecheck` règles ajoute une dépendance conditionnelle « when » qui recherche une paire `resourceType` clé-valeur correspondante. `AWS::GuardDuty::Detector` Si une correspondance est trouvée, la règle passe en revue le reste des attributs JSON et recherche des correspondances dans les trois conditions suivantes : `S3Logs.EnableKubernetes.AuditLogs.Enable`, et`FindingPublishingFrequency`.

```
let s3protection = true
let kubernetesprotection = true
let publishfrequency = 'FIFTEEN_MINUTES'

    rule compliancecheck when
        resourceType == "AWS::GuardDuty::Detector" {
            configuration.DataSources.S3Logs.Enable == %s3protection
            configuration.DataSources.Kubernetes.AuditLogs.Enable ==
 %kubernetesprotection
            configuration.FindingPublishingFrequency == %publishfrequency
        }
```

Pour la politique personnalisée complète de Guard qui implémente cette règle personnalisée, voir awsconfig-guard-cft-gd.yaml dans le référentiel de GitHub code. Pour le code HashiCorp Terraform qui déploie cette politique personnalisée dans Guard, voir awsconfig-guard-tf-gd.json dans le référentiel de code.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier la façon dont les ressources sont liées les unes aux autres et comment leurs configurations ont évolué au fil du temps.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.

Référentiel de code

Le code de ce modèle est disponible dans le AWS CloudFormation Guard référentiel GitHub AWS Config with. Ce référentiel de code contient des exemples pour les deux scénarios décrits dans ce modèle.

Épopées

Création de règles AWS Config personnalisées

Tâche	Description	Compétences requises
(Facultatif) Sélectionnez des paires clé-valeur pour la règle.	Procédez comme suit si vous définissez une politique Guard personnalisée. Si vous utilisez l'un des exemples de politique s pour le scénario 1 ou 2, ignorez ces étapes. 1. Connectez-vous à la AWS Config console AWS	Administrateur AWS, ingénieur en sécurité

Tâche	Description	Compétences requises
	Management Console et ouvrez-la. 2. Dans le volet de navigation de gauche, sélectionnez Ressources. 3. Dans l'inventaire des ressources, choisissez le type de ressource pour lequel vous souhaitez créer une règle AWS Config personnalisée. 4. Sélectionnez Afficher les détails. 5. Choisissez Afficher l'élément de configuration (JSON). Cette section s'étend pour afficher l'élément de configuration au format JSON. 6. Identifiez les paires clé-valeur pour lesquelles vous souhaitez créer une règle AWS Config personnalisée.	
Créez la règle personnalisée.	À l'aide des paires clé-valeur que vous avez identifiées précédemment ou à l'aide de l'un des exemples de politiques Guard fournis, suivez les instructions de la section Création de règles de politique AWS Config personnalisées pour créer une règle personnalisée.	Administrateur AWS, ingénieur en sécurité

Tâche	Description	Compétences requises
Validez la règle personnalisée.	Procédez de l'une des manières suivantes pour valider la règle Guard personnalisée : • Entrez la commande suivante dans le AWS Command Line Interface (AWS CLI). `cfn-guard validate -r guard-s3.guard -d s3bucket-prod-pass.json` • Suivez les instructions du mode Detective dans Evaluating Your Resources with AWS Config Rules pour déployer la règle dans AWS Config. Vérifiez que la syntaxe Guard correspond correctement aux ressources correspondantes du compte ou du fichier cible.	Administrateur AWS, ingénieur en sécurité

Résolution des problèmes

Problème	Solution
Testez la politique Guard en dehors de AWS Config	Les tests unitaires peuvent être effectués sur votre appareil local ou dans un environnement de développement intégré (IDE), tel qu'un AWS Cloud9 IDE. Pour effectuer un test unitaire, procédez comme suit :

Problème	Solution

	1. Installez la AWS CloudFormation Guard CLI et ses dépendances.
	2. Enregistrez un exemple de CI au format JSON sur votre poste de travail sous la forme d'un fichier .json.
	3. Enregistrez la GuardDuty politique sur votre poste de travail sous forme de fichier .guard.
	4. Dans la CLI Guard, entrez la commande suivante pour valider l'exemple de fichier JSON à l'aide de la politique Guard.
	`cfn-guard validate \`
	`-r guard-s3.guard \`
	`-d s3bucket-prod-pass.json`

Déboguer une règle AWS Config personnalisée	Dans votre politique Guard, remplacez la `EnableDebugLogDelivery` valeur par`true`. La valeur par défaut est `false`. Les messages du journal sont stockés sur Amazon CloudWatch.

Ressources connexes

AWS documentation

- Création de règles de politique AWS Config personnalisées (AWS Config documentation)
- AWS CloudFormation Guard Règles de rédaction (documentation Guard)

AWS articles de blog et ateliers

- Présentation de la AWS CloudFormation Guard version 2.0 (article de AWS blog)

Autres ressources

- AWS CloudFormation Guard (GitHub)
- AWS CloudFormation Guard Documentation CLI (GitHub)

Créez un rapport consolidé des découvertes de sécurité de Prowler à partir de plusieurs Comptes AWS

Créée par Mike Virgilio (AWS), Andrea Di Fabio (AWS) et Jay Durga (AWS)

Récapitulatif

Prowler (GitHub) est un outil de ligne de commande open source qui peut vous aider à évaluer, auditer et surveiller vos comptes Amazon Web Services (AWS) afin de garantir leur conformité aux meilleures pratiques en matière de sécurité. Dans ce modèle, vous déployez Prowler de manière centralisée Compte AWS au sein de votre organisation, géré par AWS Organizations, puis vous utilisez Prowler pour effectuer une évaluation de sécurité de tous les comptes de l'organisation.

Bien qu'il existe de nombreuses méthodes pour déployer et utiliser Prowler à des fins d'évaluation, cette solution a été conçue pour un déploiement rapide, une analyse complète de tous les comptes de l'organisation ou des comptes cibles définis, et des rapports accessibles sur les résultats de sécurité. Dans cette solution, lorsque Prowler termine l'évaluation de la sécurité de tous les comptes de l'organisation, il consolide les résultats. Il filtre également tous les messages d'erreur attendus, tels que les erreurs liées aux restrictions qui empêchent Prowler de scanner les compartiments Amazon Simple Storage Service (Amazon S3) dans les comptes approvisionnés par le biais de ce service. AWS Control Tower Les résultats filtrés et consolidés sont présentés dans un modèle Microsoft Excel inclus dans ce modèle. Vous pouvez utiliser ce rapport pour identifier les améliorations potentielles des contrôles de sécurité au sein de votre organisation.

Cette solution a été conçue avec les éléments suivants à l'esprit :

- Les AWS CloudFormation modèles réduisent l'effort requis pour déployer les AWS ressources selon ce modèle.
- Vous pouvez ajuster les paramètres des CloudFormation modèles et du script prowler_scan.sh au moment du déploiement afin de personnaliser les modèles en fonction de votre environnement.
- Les vitesses d'évaluation et de génération de rapports de Prowler sont optimisées grâce au traitement parallèle des résultats agrégés Comptes AWS, à des rapports consolidés avec des mesures correctives recommandées et à des visualisations générées automatiquement.
- L'utilisateur n'a pas besoin de surveiller la progression de l'analyse. Lorsque l'évaluation est terminée, l'utilisateur est averti via une rubrique Amazon Simple Notification Service (Amazon SNS) afin qu'il puisse récupérer le rapport.

- Le modèle de rapport vous permet de lire et d'évaluer uniquement les résultats pertinents pour l'ensemble de votre organisation.

Conditions préalables et limitations

Prérequis

- Et Compte AWS pour héberger des services et outils de sécurité, gérés en tant que compte membre d'une organisation dans AWS Organizations. Dans ce modèle, ce compte est appelé compte de sécurité.
- Dans le compte de sécurité, vous devez disposer d'un sous-réseau privé avec accès Internet sortant. Pour obtenir des instructions, consultez la section VPC avec serveurs dans des sous-réseaux privés et NAT dans la documentation Amazon Virtual Private Cloud (Amazon VPC). Vous pouvez établir un accès à Internet à l'aide d'une passerelle NAT configurée dans un sous-réseau public.
- Accès au compte AWS Organizations de gestion ou à un compte doté d'autorisations d'administrateur déléguées pour CloudFormation. Pour obtenir des instructions, voir Enregistrer un administrateur délégué dans la CloudFormation documentation.
- Activez un accès fiable entre AWS Organizations et CloudFormation. Pour obtenir des instructions, consultez la section Activer l'accès sécurisé avec AWS Organizations dans la CloudFormation documentation.

Limites

- La cible Comptes AWS doit être gérée en tant qu'organisation dans AWS Organizations. Si vous ne l'utilisez pas AWS Organizations, vous pouvez mettre à jour le CloudFormation modèle IAM-ProwlerExecRole .yaml et le script prowler_scan.sh pour votre environnement. Au lieu de cela, vous fournissez une liste Compte AWS IDs des régions dans lesquelles vous souhaitez exécuter le script.
- Le CloudFormation modèle est conçu pour déployer l'instance Amazon Elastic Compute Cloud (Amazon EC2) dans un sous-réseau privé doté d'un accès Internet sortant. L' AWS Systems Manager agent (agent SSM) a besoin d'un accès sortant pour atteindre le point de terminaison du AWS Systems Manager service, et vous avez besoin d'un accès sortant pour cloner le référentiel de code et installer les dépendances. Si vous souhaitez utiliser un sous-réseau public, vous devez modifier le modèle prowler-resources.yaml pour associer une adresse IP élastique à l'instance. EC2

Versions du produit

- Prowler version 4.0 ou ultérieure

Architecture

Le schéma montre le processus suivant :

1. À l'aide du Gestionnaire de session, une fonctionnalité de AWS Systems Manager, l'utilisateur s'authentifie auprès de l' EC2 instance et exécute le script prowler_scan.sh. Ce script shell exécute les étapes 2 à 8.
2. L' EC2 instance assume le rôle `ProwlerEC2Role` IAM, qui accorde des autorisations pour accéder au compartiment S3 et pour assumer les rôles `ProwlerExecRole` IAM dans les autres comptes de l'organisation.
3. L' EC2 instance assume le rôle `ProwlerExecRole` IAM dans le compte de gestion de l'organisation et génère une liste des comptes de l'organisation.
4. L' EC2 instance assume le rôle `ProwlerExecRole` IAM dans les comptes membres de l'organisation (appelés comptes de charge de travail dans le schéma d'architecture) et effectue une évaluation de la sécurité de chaque compte. Les résultats sont stockés sous forme de fichiers CSV et HTML sur l' EC2 instance.

   > **Note**
   >
   > Les fichiers HTML sont le résultat de l'évaluation Prowler. En raison de la nature du HTML, ils ne sont pas concaténés, traités ou utilisés directement dans ce modèle. Toutefois, ils peuvent être utiles pour l'examen des rapports de compte individuels.

5. L' EC2 instance traite tous les fichiers CSV pour supprimer les erreurs connues et attendues et consolide les résultats restants dans un seul fichier CSV.
6. L' EC2 instance regroupe les résultats des comptes individuels et les résultats agrégés dans un fichier zip.
7. L' EC2 instance télécharge le fichier zip dans le compartiment S3.
8. Une EventBridge règle détecte le téléchargement du fichier et utilise une rubrique Amazon SNS pour envoyer un e-mail à l'utilisateur l'informant que l'évaluation est terminée.

9. L'utilisateur télécharge le fichier zip depuis le compartiment S3. L'utilisateur importe les résultats dans le modèle Excel et les examine.

Outils

Services AWS

- Amazon Elastic Compute Cloud (Amazon EC2) fournit une capacité de calcul évolutive dans le AWS Cloud. Vous pouvez lancer autant de serveurs virtuels que vous le souhaitez et les augmenter ou les diminuer rapidement.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, AWS Lambda des fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle. Ce modèle utilise Session Manager, une fonctionnalité de Systems Manager.

Autres outils

- Prowler est un outil de ligne de commande open source qui vous permet d'évaluer, d'auditer et de surveiller la conformité de vos comptes aux meilleures pratiques de AWS sécurité et aux autres cadres et normes de sécurité.

Référentiel de code

Le code de ce modèle est disponible dans l'évaluation de la sécurité GitHub multi-comptes via le référentiel Prowler. Le référentiel de code contient les fichiers suivants :

- prowler_scan.sh — Ce script bash est utilisé pour démarrer une évaluation de sécurité multiple par Prowler, Comptes AWS en parallèle. Comme défini dans le fichier Prowler-Resources.yaml CloudFormationtemplate, ce script est automatiquement déployé dans le dossier de l'instance. `usr/local/prowler` EC2
- Prowler-Resources.yaml — Vous utilisez ce CloudFormation modèle pour créer une pile dans le compte de sécurité de l'organisation. Ce modèle déploie toutes les ressources requises pour ce compte afin de prendre en charge la solution. Cette pile doit être déployée avant le modèle IAM-ProwlerExecRole .yaml. Nous vous déconseillons de déployer ces ressources dans un compte hébergeant des charges de travail de production critiques.

> **Note**
>
> Si cette pile est supprimée et redéployée, vous devez reconstruire l'ensemble de `ProwlerExecRole` piles afin de rétablir les dépendances entre comptes entre les rôles IAM.

- IAM- ProwlerExecRole .yaml — Vous utilisez ce CloudFormation modèle pour créer un stack set qui déploie le rôle `ProwlerExecRole` IAM dans tous les comptes de l'organisation, y compris le compte de gestion.
- prowler-report-template.xlsm — Vous utilisez ce modèle Excel pour traiter les résultats du Prowler. Les tableaux croisés dynamiques du rapport fournissent des fonctionnalités de recherche, des graphiques et des résultats consolidés.

Épopées

Préparation au déploiement

Tâche	Description	Compétences requises
Clonez le référentiel de code.	1. Dans une interface de ligne de commande, remplacez votre répertoire de travail par l'emplacement où	AWS DevOps

Tâche	Description	Compétences requises
	vous souhaitez stocker les fichiers d'exemple. 2. Entrez la commande suivante : `git clone https://github.com/aws-samples/multi-account-security-assessment-via-prowler.git`	
Passez en revue les modèles.	1. Dans le référentiel cloné, ouvrez les fichiers Prowler-Resources.yaml et IAM- .yaml. ProwlerExecRole 2. Passez en revue les ressources créées par ces modèles et ajustez-les en fonction des besoins de votre environnement. Pour plus d'informations, consultez la section Utilisation des modèles dans la CloudFormation documentation. 3. Enregistrez et fermez les fichiers Prowler-Resources.yaml et IAM- .yaml. ProwlerExecRole	AWS DevOps

Créez les CloudFormation piles

Tâche	Description	Compétences requises
Fournir des ressources dans le compte de sécurité.	À l'aide du modèle prowler-resources.yaml, vous créez une CloudFormation pile qui déploie toutes les ressources requises dans le compte de sécurité. Pour obtenir des instructions, consultez la section Création d'une pile dans la CloudFormation documentation. Tenez compte des points suivants lors du déploiement de ce modèle : 1. Sur la page Spécifier le modèle, sélectionnez Le modèle est prêt, puis téléchargez le fichier prowler-resources.yaml. 2. Sur la page Spécifier les détails de la pile, dans le champ Nom de la pile, entrez`Prowler-Resources` . 3. Dans la section Paramètres, entrez les informations suivantes : • `VPCId`— Sélectionnez un VPC dans le compte. • `SubnetId`— Sélectionnez un sous-réseau privé ayant accès à Internet.	AWS DevOps

Tâche	Description	Compétences requises

	Remarque : Si vous sélectionnez un sous-réseau public, aucune adresse IP publique ne sera attribuée à l' EC2 instance car le CloudFormation modèle, par défaut, ne fournit ni n'attache d'adresse IP élastique.
	• `InstanceType` — Sélectionnez une taille d'instance en fonction du nombre d'évaluations parallèles :
	  • Pour 10, choisisse `zr6i.large` .
	  • Pour 12, choisisse `zr6i.xlarge` .
	  • Pour 14 à 18 ans, choisissez. `r6i.2xlarge`
	• `InstanceImageId` — Conservez la valeur par défaut pour Amazon Linux.
	• `KeyPairName` — Si vous utilisez SSH pour l'accès, spécifiez le nom d'une paire de clés existante.
	• `PermittedSSHInboun d` — Si vous utilisez SSH	

Tâche	Description	Compétences requises
	pour l'accès, spécifiez un bloc CIDR autorisé. Si vous n'utilisez pas SSH, conservez la valeur par défaut de`127.0.0.1` . • `BucketName` — La valeur par défaut est`prowler-output-<accountID>-<region>` . Vous pouvez le modifier selon vos besoins. Si vous spécifiez une valeur personnalisée, l'ID du compte et la région sont automatiquement ajoutés à la valeur spécifiée. • `EmailAddress` — Spécifiez une adresse e-mail pour une notification Amazon SNS lorsque Prowler termine l'évaluation et télécharge le fichier .zip dans le compartiment S3. Remarque : La configuration de l'abonnement SNS doit être confirmée avant que Prowler ne termine l'évaluation, faute de quoi aucune notification ne sera envoyée.	

Tâche	Description	Compétences requises
	• `IAMProwler rEC2Role` — Conservez la valeur par défaut, sauf si vos conventions de dénomination exigent un nom différent pour ce rôle IAM. • `IAMProwlerExecRole` — Conservez la valeur par défaut à moins qu'un autre nom ne soit utilisé lors du déploiement du fichier IAM- ProwlerEx ecRole .yaml. • `Parallelism` — Spécifiez le nombre d'évaluations parallèle s à effectuer. Assurez-vous que la valeur du `InstanceType` paramètre prend en charge ce nombre d'évaluations parallèles. • `FindingOutput` — Si vous souhaitez exclure les résultats de réussite, sélectionnez`Fail0nly`. Cela réduit considéra blement la taille de sortie et se concentre sur les vérifications qui pourraien t devoir être résolues. Si vous souhaitez inclure les résultats de réussite,	

Tâche	Description	Compétences requises
	sélectionnez`FailAndPass` . 4. Sur la page de révision, sélectionnez Les ressources suivantes nécessitent des fonctionnalités : [AWS::IAM::Role], puis choisissez Create Stack. 5. Une fois la pile créée avec succès, dans la CloudFormation console, dans l'onglet Outputs, copiez le `ProwlerEC2Role` Amazon Resource Name (ARN). Vous utiliserez cet ARN ultérieurement lors du déploiement du fichier IAM-ProwlerExecRole .yaml.	

Tâche	Description	Compétences requises
Attribuez le rôle IAM dans les comptes des membres.	Dans le compte AWS Organizations de gestion ou dans un compte doté d'autorisations d'administrateur déléguées pour CloudFormation, utilisez le modèle IAM-ProwlerExecRole .yaml pour créer un CloudFormation stack set. Le stack set déploie le rôle `ProwlerExecRole` IAM dans tous les comptes membres de l'organisation. Pour obtenir des instructions, consultez la section Créer un ensemble de piles avec des autorisations gérées par les services dans la CloudFormation documentation. Tenez compte des points suivants lors du déploiement de ce modèle : 1. Sous Préparer le modèle, sélectionnez Le modèle est prêt, puis téléchargez le fichier IAM- ProwlerExecRole .yaml. 2. Sur la page Spécifier StackSet les détails, nommez l'ensemble de piles`IAM-ProwlerExecRole` .	AWS DevOps

Tâche	Description	Compétences requises
	3. Dans la section Paramètres, entrez les informations suivantes : • `AuthorizedARN` — Entrez l'`ProwlerEC2Role` ARN que vous avez copié lors de la création de la `Prowler-Resources` pile. • `ProwlerExecRoleName` — Conservez la valeur par défaut, `ProwlerExecRole` sauf si un autre nom a été utilisé lors du déploiement du fichier Prowler-Resources.yaml. 4. Sous Autorisations, choisissez Autorisations gérées par le service. 5. Sur la page Définir les options de déploiement, sous Cibles de déploiement, choisissez Déployer vers l'organisation et acceptez toutes les valeurs par défaut. Remarque : Si vous souhaitez que les piles soient déployées simultanément sur tous les comptes membres, définissez le nombre maximal de comptes simultanés et la	

Tâche	Description	Compétences requises
	tolérance d'échec sur une valeur élevée, telle que`100`. 6. Sous Régions de déploiement, choisissez l' Région AWS endroit où l' EC2 instance de Prowler est déployée. Les ressources IAM étant mondiales et non régionales, le rôle IAM est déployé dans toutes les régions actives. 7. Sur la page de révision, sélectionnez Je reconnais que des ressources IAM AWS CloudFormation peuvent être créées avec des noms personnalisés, puis choisissez Créer StackSet. 8. Surveillez l'onglet Stack instances (pour le statut des comptes individuels) et l'onglet Opérations (pour le statut général) afin de déterminer quand le déploiement est terminé.	

Tâche	Description	Compétences requises
Attribuez le rôle IAM dans le compte de gestion.	À l'aide du modèle IAM-ProwlerExecRole .yaml, vous créez une CloudFormation pile qui déploie le rôle `ProwlerExecRole` IAM dans le compte de gestion de l'organisation. Le stack set que vous avez créé précédemment ne déploie pas le rôle IAM dans le compte de gestion. Pour obtenir des instructions, consultez la section Création d'une pile dans la CloudFormation documentation. Tenez compte des points suivants lors du déploiement de ce modèle : 1. Sur la page Spécifier le modèle, sélectionnez Le modèle est prêt, puis téléchargez le fichier IAM-ProwlerExecRole .yaml. 2. Sur la page Spécifier les détails de la pile, dans le champ Nom de la pile, entrez`IAM-ProwlerExecRole` . 3. Dans la section Paramètres, entrez les informations suivantes : • `AuthorizedARN` — Entrez l'`ProwlerEC2Role` ARN que vous	AWS DevOps

Tâche	Description	Compétences requises
	avez copié lors de la création de la `Prowler-Resources` pile. • `ProwlerExecRoleName` — Conservez la valeur par défaut, `ProwlerExecRole` sauf si un autre nom a été utilisé lors du déploiement du fichier Prowler-Resources.yaml. 4. Sur la page de révision, sélectionnez Les ressources suivantes nécessitent des fonctionnalités : [AWS::IAM::Role], puis choisissez Create Stack.	

Réaliser l'évaluation de sécurité du Prowler

Tâche	Description	Compétences requises
Lancez le scan.	1. Connectez-vous au compte de sécurité de l'organisation. 2. À l'aide du gestionnaire de session, connectez-vous à l' EC2 instance de Prowler que vous avez précédemment provisionnée. Pour obtenir des instructions, voir Se connecter à votre instance Linux à l'aide du gestionnaire de session. Si vous ne parvenez pas à	Administrateur AWS

Tâche	Description	Compétences requises
	vous connecter, consultez la section Dépannage de ce modèle. 3. Accédez au fichier prowler_scan.sh **`usr/local/prowler`** , puis ouvrez-le. 4. Passez en revue et modifiez les paramètres et variables ajustables de ce script en fonction des besoins de votre environnement. Pour plus d'informations sur les options de personnalisation, consultez les commentaires au début du script. Par exemple, au lieu d'obtenir une liste de tous les comptes membres de l'organisation à partir du compte de gestion, vous pouvez modifier le script pour spécifier le Compte AWS IDs ou Régions AWS que vous souhaitez scanner, ou vous pouvez faire référence à un fichier externe contenant ces paramètres. 5. Enregistrez et fermez le fichier prowler_scan.sh.	

Tâche	Description	Compétences requises

	6. Entrez les commandes suivantes : Cela exécute le script prowler_scan.sh.
	
	`sudo -i`
	`screen`
	`cd /usr/local/prowler`
	`./prowler_scan.sh`
	
	Remarques :
	• La commande screen permet au script de continuer à s'exécuter en cas d'expiration de la connexion ou de perte de l'accès à la console.
	• Une fois le scan lancé, vous pouvez forcer le détachement de l'écran en appuyant sur Ctrl+A D. L'écran se détache et vous pouvez fermer la connexion à l'instance et autoriser l'évaluation à se poursuivre.
	• Pour reprendre une session détachée, connectez-vous à l'instance, entrez `sudo -i` puis entrez`screen -r`.
	• Pour suivre la progressi on des évaluations des comptes individuels, vous pouvez accéder au	

Tâche	Description	Compétences requises
	`usr/local/prowler` répertoire et saisir la commande`tail -f output/stdout-<account-id>` . 7. Attendez que Prowler ait terminé les scans de tous les comptes. Le script évalue plusieurs comptes en même temps. Lorsque l'évaluation est terminée dans tous les comptes, vous recevez une notification si vous avez indiqué une adresse e-mail lors du déploiement du fichier Prowler-Resources.yaml.	

Tâche	Description	Compétences requises
Récupérez les découvertes du Prowler.	1. Téléchargez le `prowler-output-<assessDate>.zip` fichier depuis le `prowler-output-<accountID>-<region>` bucket. Pour obtenir des instructions, consultez la section Téléchargement d'un objet dans la documentation Amazon S3. 2. Supprimez tous les objets du compartiment, y compris le fichier que vous avez téléchargé. Il s'agit d'une bonne pratique pour optimiser les coûts et pour vous assurer que vous pouvez supprimer la `Prowler-Resources` CloudFormation pile à tout moment. Pour obtenir des instructions, consultez Supprimer des objets dans la documentation Amazon S3.	AWS général
Arrêtez l' EC2 instance.	Pour empêcher la facturation lorsque l'instance est inactive, arrêtez l' EC2 instance qui exécute Prowler. Pour obtenir des instructions, consultez la section Arrêter et démarrer vos instances dans la EC2 documentation Amazon.	AWS DevOps

Créez un rapport sur les résultats

Tâche	Description	Compétences requises
Importez les résultats.	1. Dans Excel, ouvrez le fichier prowler-report-template.xlsx, puis sélectionnez la feuille de calcul Prowler CSV. 2. Supprimez tous les exemples de données, y compris la ligne d'en-tête. Si vous êtes invité à supprimer la requête associée aux données supprimées, choisissez Non. La suppression de la requête peut affecter la fonctionnalité des tableaux croisés dynamiques dans le modèle Excel. 3. Extrayez le contenu du fichier zip que vous téléchargez depuis le compartiment S3. 4. Dans Excel, ouvrez le fichier prowler-fullorgresults-accessdeniedfiltered.txt. Nous vous recommandons d'utiliser ce fichier car les erreurs non exploitables les plus courantes ont déjà été supprimées, telles que les `Access Denied` erreurs liées aux tentatives d'analyse des AWS Control	AWS général

Tâche	Description	Compétences requises
	Tower ressources. Si vous souhaitez obtenir les résultats non filtrés, ouvrez plutôt le fichier prowler-f ullorgresults.txt. 5. Sélectionnez la colonne A. 6. Si vous utilisez Windows, entrez Ctrl+C, ou si vous utilisez macOS, entrez Cmd +C. Toutes les données sont alors copiées dans le presse-papiers. 7. Dans le modèle de rapport Excel, sur la feuille de calcul Prowler CSV, sélectionnez la cellule A1. 8. Si vous utilisez Windows, entrez Ctrl+V, ou si vous utilisez macOS, entrez Cmd+V. Cela permet de coller les résultats dans le rapport. 9. Vérifiez que toutes les cellules contenant les données collées sont sélectionnées. Dans le cas contraire, sélectionnez la colonne A. 10. Dans l'onglet Données, sélectionnez Texte en colonnes. 11. Dans l'assistant, procédez comme suit :	

Tâche	Description	Compétences requises
	• Pour l'étape 1, choisissez Délimité. • Pour l'étape 2, pour Délimiteurs, choisissez Point-virgule. Dans le volet d'aperçu des données, vérifiez que les données sont séparées en colonnes. • Pour l'étape 3, choisissez Terminer. 12. Vérifiez que les données de texte sont délimitées sur plusieurs colonnes. 13. Enregistrez le rapport Excel sous un nouveau nom. 14. Recherchez et supprimez toute `Access Denied` erreur dans les résultats . Pour obtenir des instructions sur la façon de les supprimer par programmation, consultez la section Suppression par programmation des erreurs dans la section Informations supplémentaires.	

Tâche	Description	Compétences requises
Finalisez le rapport.	1. Choisissez la feuille de travail Conclusions, puis sélectionnez la cellule A17. Cette cellule est l'en-tête du tableau croisé dynamique. 2. Dans le ruban, sous PivotTable Outils, choisissez Analyser, puis sous Actualiser, choisissez Actualiser tout. Cela met à jour les tableaux croisés dynamiques avec le nouvel ensemble de données. 3. Par défaut, Excel n'affiche pas correctement Compte AWS les nombres. Pour corriger le formatage des nombres, procédez comme suit : • Dans la feuille de travail Résultats, ouvrez le menu contextuel (clic droit) de la colonne A, puis choisissez Formater les cellules. • Choisissez Nombre, puis entrez `0` au décimal. • Choisissez OK. Remarque : Si un Compte AWS nombre commence par un ou plusieurs zéros, Excel supprime automatiquement	AWS général

Tâche	Description	Compétences requises
	les zéros. Si le numéro de compte comporte moins de 12 chiffres dans le rapport, les chiffres manquants sont des zéros au début du numéro. 4. (Facultatif) Vous pouvez réduire les champs pour faciliter la lecture des résultats. Procédez comme suit : • Dans la feuille de travail Constatations, si vous déplacez le curseur sur la ligne située entre les lignes 18 et 19 (l'espace entre l'en-tête critique et le premier résultat) , l'icône du curseur se transforme en une petite flèche pointant vers le bas. • Cliquez pour sélection ner tous les champs de recherche. • Ouvrez le menu contextuel (clic droit), recherchez Développer/ Réduire, puis choisissez Réduire. 5. Pour plus de détails sur l'évaluation, consultez les feuilles de travail sur	

Tâche	Description	Compétences requises
	les résultats, la gravité et l'échec réussi.	

(Facultatif) Mettez à jour Prowler ou les ressources du référentiel de code

Tâche	Description	Compétences requises

Mettez à jour Prowler.	Si vous souhaitez mettre à jour Prowler vers la dernière version, procédez comme suit :
	1. Connectez-vous à l' EC2 instance de Prowler à l'aide du gestionnaire de session. Pour obtenir des instructions, voir Se connecter à votre instance Linux à l'aide du gestionnaire de session.
	2. Entrez la commande suivante.
	`sudo -i`
	`pip3 install --upgrade prowler`
		AWS général

Mettez à jour le script prowler_scan.sh.	Si vous souhaitez mettre à jour le script prowler_scan.sh vers la dernière version du dépôt, procédez comme suit : 1. Connectez-vous à l' EC2 instance de Prowler à l'aide du gestionnaire de session. Pour obtenir des instructi	AWS général

Tâche	Description	Compétences requises

	ons, voir Se connecter à votre instance Linux à l'aide du gestionnaire de session.
	2. Entrez la commande suivante.
	`sudo -i`
	3. Accédez au répertoire des scripts Prowler.
	`cd /usr/local/prowler`
	4. Entrez la commande suivante pour stocker le script local afin de pouvoir fusionner les modifications personnalisées dans la version la plus récente.
	`git stash`
	5. Entrez la commande suivante pour obtenir la dernière version du script.
	`git pull`
	6. Entrez la commande suivante pour fusionner le script personnalisé avec la dernière version du script.
	`git stash pop`	

Tâche	Description	Compétences requises
	Note Vous pouvez recevoir des avertissements concernant des fichiers générés localement qui ne figurent pas dans le GitHub dépôt, tels que la recherche de rapports. Vous pouvez les ignorer tant que le fichier prowler_scan.sh indique que les modifications stockées localement sont réintégrées.	

(Facultatif) Nettoyer

Tâche	Description	Compétences requises
Supprimez toutes les ressources déployées.	Vous pouvez laisser les ressources déployées dans les comptes. Si vous arrêtez l' EC2 instance lorsqu'elle n'est pas utilisée et que vous laissez le compartiment S3 vide, cela réduit les coûts de maintenance des ressources pour les futures analyses.	AWS DevOps

Tâche	Description	Compétences requises
	Si vous souhaitez déprovisionner toutes les ressources, procédez comme suit : 1. Supprimez la `IAM-ProwlerExecRole` pile provisionnée dans le compte de gestion. Pour obtenir des instructions, consultez la section Suppression d'une pile dans la CloudFormation documentation. 2. Supprimez le `IAM-ProwlerExecRole` stack set provisionné dans le compte de gestion de l'organisation ou dans le compte d'administrateur délégué. Pour obtenir des instructions, voir Supprimer un ensemble de piles dans la CloudFormation documentation. 3. Supprimez tous les objets du compartiment `prowler-output` S3. Pour obtenir des instructions, consultez Supprimer des objets dans la documentation Amazon S3. 4. Supprimez la `Prowler-Resources` pile provision	

Tâche	Description	Compétences requises
	née dans le compte de sécurité. Pour obtenir des instructions, consultez la section Suppression d'une pile dans la CloudFormation documentation.	

Résolution des problèmes

Problème	Solution
Impossible de se connecter à l' EC2 instance à l'aide du gestionnaire de session.	L'agent SSM doit être capable de communiquer avec le point de terminaison Systems Manager. Procédez comme suit : 1. Vérifiez que le sous-réseau sur lequel l' EC2 instance est déployée dispose d'un accès Internet. 2. Redémarrez l' EC2 instance.
Lorsque vous déployez le stack set, la CloudFormation console vous invite à`Enable trusted access with AWS Organizations to use service-managed permissions .`	Cela indique que l'accès sécurisé n'a pas été activé entre AWS Organizations et CloudFormation. Un accès sécurisé est requis pour déployer le stack set géré par les services. Cliquez sur le bouton pour activer l'accès sécurisé. Pour plus d'informations, consultez la section Activer l'accès sécurisé dans la CloudFormation documentation.

Ressources connexes

AWS documentation

- Mise en œuvre de contrôles de sécurité sur AWS (AWS directives prescriptives)

Autres ressources

- Prowler () GitHub

Informations supplémentaires

Suppression des erreurs par programmation

Si les résultats contiennent des `Access Denied` erreurs, vous devez les supprimer des résultats. Ces erreurs sont généralement dues à une influence externe sur les autorisations qui empêchent Prowler d'évaluer une ressource particulière. Par exemple, certaines vérifications échouent lors de l'examen des compartiments S3 provisionnés via. AWS Control Tower Vous pouvez extraire ces résultats par programmation et enregistrer les résultats filtrés dans un nouveau fichier.

Les commandes suivantes suppriment les lignes contenant une seule chaîne de texte (un modèle), puis affichent les résultats dans un nouveau fichier.

- Pour Linux ou macOS (Grep)

```
grep -v -i "Access Denied getting bucket" myoutput.csv > myoutput_modified.csv
```

- Pour Windows (PowerShell)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket' -NotMatch >
 myoutput_modified.csv
```

Les commandes suivantes suppriment les lignes correspondant à plusieurs chaînes de texte, puis affichent les résultats dans un nouveau fichier.

- Pour Linux ou macOS (utilise un canal échappé entre les chaînes)

```
grep -v -i 'Access Denied getting bucket\|Access Denied Trying to Get' myoutput.csv >
 myoutput_modified.csv
```

- Pour Windows (utilise une virgule entre les chaînes)

```
Select-String -Path myoutput.csv -Pattern 'Access Denied getting bucket', 'Access
 Denied Trying to Get' -NotMatch > myoutput_modified.csv
```

Exemples de rapports

L'image suivante est un exemple de la feuille de travail Conclusions du rapport sur les résultats consolidés de Prowler.

L'image suivante est un exemple de la feuille de travail Pass Fail figurant dans le rapport des résultats consolidés de Prowler. (Par défaut, les résultats de réussite sont exclus de la sortie.)

L'image suivante est un exemple de la feuille de travail sur la gravité figurant dans le rapport des résultats consolidés de Prowler.

Supprimez les volumes Amazon EBS inutilisés en utilisant AWS Config et AWS Systems Manager

Créée par Sankar Sangubotla (AWS)

Récapitulatif

Le cycle de vie d'un volume Amazon Elastic Block Store (Amazon EBS) est généralement indépendant du cycle de vie de l'instance Amazon Elastic Compute Cloud (EC2Amazon) à laquelle il est rattaché. À moins que vous ne sélectionniez l'option Supprimer en cas de résiliation au moment du lancement, la résiliation de l' EC2 instance Amazon détache le volume Amazon EBS mais ne le supprime pas. En particulier dans les environnements de développement et de test où il est courant de lancer et de mettre fin à EC2 des instances Amazon, cela peut entraîner l'inutilisation d'un grand nombre de volumes Amazon EBS. Les volumes Amazon EBS vous facturent des frais Compte AWS, qu'ils soient utilisés ou non. La suppression de ces volumes peut vous aider à optimiser les coûts pour votre Comptes AWS. En outre, la suppression des volumes Amazon EBS inutilisés est une bonne pratique de sécurité pour empêcher l'accès aux données inutilisées et potentiellement sensibles de ces volumes.

AWS Config peut vous aider à corriger manuellement ou automatiquement les ressources non conformes. Ce modèle décrit comment configurer une AWS Config règle et une action de correction automatique qui suppriment les volumes Amazon EBS inutilisés du compte. L'action de correction est un runbook prédéfini pour Automation, une fonctionnalité de. AWS Systems Manager Vous pouvez configurer le runbook pour créer un instantané du volume avant de le supprimer.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Identity and Access Management Autorisations (IAM) pour exécuter le `AWSConfigRemediation-DeleteUnusedEBSVolume` runbook for Automation, une fonctionnalité de Systems Manager. Pour plus d'informations, consultez la section Autorisations IAM requises dans AWSConfigRemediation-DeleteUnusedEBSVolume.
- Un ou plusieurs volumes Amazon EBS inutilisés.

Limites

- Les volumes Amazon EBS non utilisés doivent être en bon `available` état.

Architecture

Architecture cible

1. La AWS Config règle évalue les volumes Amazon EBS.
2. La règle renvoie une liste de ressources conformes et non conformes. Les volumes Amazon EBS en `available` état, qui sont des volumes non utilisés, sont considérés comme non conformes.
3. AWS Config démarre automatiquement le runbook Automation.
4. S'il est configuré, Systems Manager crée des instantanés des volumes inutilisés avant de les supprimer.
5. Systems Manager supprime les volumes Amazon EBS inutilisés.

Automatisation et mise à l'échelle

Vous pouvez appliquer cette solution à tous les comptes de votre organisation. Pour plus d'informations, consultez la section Gestion des règles pour tous les comptes de votre organisation dans la AWS Config documentation.

Outils

- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.
- AWS Systems Manager L'automatisation simplifie les tâches courantes de maintenance, de déploiement et de correction pour de nombreuses personnes Services AWS.

Épopées

Configuration de la AWS Config règle

Tâche	Description	Compétences requises
Créez un rôle pour le runbook Automation.	Créez un rôle appelé`AssumeRole` . Systems Manager Automation utilise ce rôle pour exécuter le runbook. Pour obtenir des instructions, consultez la section Configuration d'un accès à un rôle de service (assumer un rôle) pour les automatisations dans la documentation de Systems Manager.	Administrateur système AWS
Allumez l' AWS Config enregistreur.	Suivez les instructions de la section Configuration AWS Config avec la console de la AWS Config documentation pour vous assurer qu' AWS Config elle fonctionne et qu'elle est configurée pour enregistrer les volumes Amazon EBS.	Administrateur système AWS
Exécutez la règle.	1. Suivez les instructions de la section Évaluation de vos ressources dans la AWS Config documentation pour exécuter la `ec2-volume-inuse-check` règle. Attendez que l'évaluation soit terminée.	Administrateur système AWS

Tâche	Description	Compétences requises
	2. Sur la page Règles, sélectionnez la `ec2-volume-inuse-check` règle, puis pour Ressources concernées, choisissez Non conforme. 3. Vérifiez qu'il existe un ou plusieurs volumes Amazon EBS inutilisés dans les résultats de l'évaluation.	

Configurer la correction automatique des volumes Amazon EBS inutilisés

Tâche	Description	Compétences requises
Ajoutez l'action de correction automatique.	1. Sur la page Règles, sélectionnez la `ec2-volume-inuse-check` règle. 2. Suivez les instructions de la section Configuration de la correction automatique dans la AWS Config documentation. Remarques : 3. Dans la section Détails de l'action de correction, sélectionnez`AWSConfigRemediation-DeleteUnusedEBSVolume` . • Sélectionnez le paramètre Resource ID, puis dans la liste, choisissez VolumeId.	Administrateur système AWS

Tâche	Description	Compétences requises
	Lors de l'exécution, ce paramètre est remplacé par l'ID du volume Amazon EBS non conforme. • Dans la section Paramètres, indiquez les valeurs des paramètres suivants : • `CreateSnapshot` — (Facultatif) Si ce paramètre est défini sur`true`, l'automat isation crée un instantané du volume Amazon EBS avant sa suppression. • `Automatio nAssumeRole` — Entrez le nom de ressource Amazon (ARN) du rôle de `AssumeRole` service que vous avez créé précédemment.	

Tâche	Description	Compétences requises
Testez la correction automatique de la AWS Config règle.	1. Dans la AWS Config console, sur la page Règles, sélectionnez la `ec2-volume-inuse-check` règle. 2. Dans le menu Actions, choisissez Réévaluer. 3. Permettez à la règle d'évaluer les ressources non conformes, puis confirmez que les volumes Amazon EBS inutilisés sont supprimés.	Administrateur système AWS

Résolution des problèmes

Problème	Solution
AWS Config ne reflète pas exactement l'état de la ressource.	Parfois, AWS Config ne met pas à jour l'état des ressources. Éteignez puis rallumez l'enregistreur sur la page des AWS Config paramètres. L'enregistreur enregistre l'état des ressources. Pour les ressources nouvellement créées ou supprimées, l'enregistreur peut mettre un certain temps à refléter l'état actuel. Pour plus d'informations sur les états des volumes Amazon EBS, consultez la section États des volumes dans la documentation Amazon EBS.

Ressources connexes

- AWSConfigRemediation-DeleteUnusedEBSVolume runbook
- règle ec2- volume-inuse-check
- Corriger les AWS ressources non conformes à l'aide de règles AWS Config

Déployez et gérez AWS Control Tower les contrôles en utilisant AWS CDK et CloudFormation

Créée par Iker Reina Fuente (AWS) et Ivan Girardi (AWS)

Récapitulatif

Ce modèle décrit comment utiliser, AWS Cloud Development Kit (AWS CDK) implémenter AWS CloudFormation et administrer des AWS Control Tower contrôles préventifs, détectifs et proactifs sous forme d'infrastructure sous forme de code (IaC). Un contrôle (également appelé garde-corps) est une règle de haut niveau qui fournit une gouvernance continue de votre environnement global AWS Control Tower . Par exemple, vous pouvez utiliser des contrôles pour exiger la journalisation de votre compte, Comptes AWS puis configurer des notifications automatiques si des événements spécifiques liés à la sécurité se produisent.

AWS Control Tower vous aide à mettre en œuvre des contrôles préventifs, détectifs et proactifs qui régissent vos AWS ressources et surveillent la conformité sur plusieurs sites Comptes AWS. Chaque contrôle applique une seule règle. Dans ce modèle, vous utilisez un modèle IaC fourni pour spécifier les contrôles que vous souhaitez déployer dans votre environnement.

AWS Control Tower les contrôles s'appliquent à l'ensemble d'une unité organisationnelle (UO), et le contrôle affecte chaque unité Compte AWS au sein de l'UO. Par conséquent, lorsque les utilisateurs effectuent une action sur n'importe quel compte de votre zone de landing zone, cette action est soumise aux contrôles qui régissent l'unité d'organisation.

La mise en œuvre de AWS Control Tower contrôles permet d'établir une base de sécurité solide pour votre zone AWS d'atterrissage. En utilisant ce modèle pour déployer les commandes sous forme d'iAC via CloudFormation et AWS CDK, vous pouvez standardiser les commandes dans votre zone d'atterrissage et les déployer et les gérer plus efficacement. Cette solution utilise cdk_nag pour scanner l'application pendant le AWS CDK déploiement. Cet outil vérifie que l'application est conforme aux AWS meilleures pratiques.

Pour déployer AWS Control Tower des contrôles sous forme d'iAc, vous pouvez également utiliser HashiCorp Terraform au lieu de. AWS CDK Pour plus d'informations, voir Déployer et gérer les AWS Control Tower contrôles à l'aide de Terraform.

Public visé

Ce modèle est recommandé aux utilisateurs expérimentés avec AWS Control Tower, CloudFormation AWS CDK, et AWS Organizations.

Conditions préalables et limitations

Prérequis

- Comptes AWS Gestion active en tant qu'organisation AWS Organizations et zone d' AWS Control Tower atterrissage. Pour obtenir des instructions, consultez la section Mise en route dans la AWS Control Tower documentation.
- AWS Command Line Interface (AWS CLI), installé et configuré.
- Gestionnaire de packages de nœuds (npm), installé et configuré pour le AWS CDK.
- Prérequis pour. AWS CDK
- Autorisations permettant d'assumer un rôle AWS Identity and Access Management (IAM) existant dans un compte de déploiement.
- Autorisations permettant d'assumer un rôle IAM dans le compte de gestion de l'organisation qui peut être utilisé pour démarrer. AWS CDK Le rôle doit disposer des autorisations nécessaires pour modifier et déployer CloudFormation des ressources. Pour plus d'informations, consultez Bootstrapping dans la AWS CDK documentation.
- Autorisations permettant de créer des rôles et des politiques IAM dans le compte de gestion de l'organisation. Pour plus d'informations, consultez la section Autorisations requises pour accéder aux ressources IAM dans la documentation IAM.

Limites

- Ce modèle fournit des instructions pour déployer cette solution entre Comptes AWS un compte de déploiement et le compte de gestion de l'organisation. À des fins de test, vous pouvez déployer cette solution directement dans le compte de gestion, mais les instructions relatives à cette configuration ne sont pas explicitement fournies.
- Pour les AWS Control Tower contrôles, ce modèle nécessite l'utilisation d'identifiants globaux au format suivant :

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  Les versions précédentes de ce modèle utilisaient des identifiants régionaux qui ne sont plus pris en charge. Nous vous recommandons de passer des identifiants régionaux aux identifiants

globaux. Les identifiants globaux vous aident à gérer les contrôles et à augmenter le nombre de contrôles que vous pouvez utiliser.

> **Note**
>
> Dans la plupart des cas, la valeur de `<PARTITION>` est`aws`.

Versions du produit

- AWS Control Tower version 3.2 ou ultérieure
- Python version 3.9 ou ultérieure
- npm version 8.9.0 ou ultérieure

Architecture

Cette section fournit une présentation générale de cette solution et de l'architecture établie par l'exemple de code. Le schéma suivant montre les contrôles déployés sur les différents comptes de l'unité d'organisation.

AWS Control Tower les contrôles sont classés en fonction de leur comportement et de leurs instructions.

Il existe trois principaux types de comportements de contrôle :

1. Les contrôles préventifs sont conçus pour empêcher les actions de se produire. Elles sont mises en œuvre avec des politiques de contrôle des services (SCPs) ou des politiques de contrôle des ressources (RCPs) dans AWS Organizations. Le statut d'un contrôle préventif est soit appliqué, soit non activé. Les contrôles préventifs sont pris en charge dans tous les cas Régions AWS.
2. Les contrôles Detective sont conçus pour détecter des événements spécifiques lorsqu'ils se produisent et pour enregistrer l'action AWS CloudTrail. Elles sont mises en œuvre avec AWS Config des règles. Le statut d'un contrôle de détection est soit clair, soit en violation, soit non activé. Les contrôles Detective ne s'appliquent que dans ceux Régions AWS pris en charge par AWS Control Tower.
3. Les contrôles proactifs analysent les ressources qui seraient mises à disposition par votre entreprise AWS CloudFormation et vérifient si elles sont conformes aux politiques et aux

objectifs de votre entreprise. Les ressources non conformes ne seront pas provisionnées. Ils sont implémentés avec des AWS CloudFormation crochets. Le statut d'un contrôle proactif est PASS, FAIL ou SKIP.

Les directives de contrôle font référence à la pratique recommandée pour appliquer chaque contrôle à votre OUs. AWS Control Tower fournit trois catégories de conseils : obligatoires, fortement recommandés et facultatifs. Le guidage d'un contrôle est indépendant de son comportement. Pour plus d'informations, consultez la section Contrôle du comportement et instructions.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code. Le AWS CDK kit d'outils est le principal outil d'interaction avec votre AWS CDK application.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.
- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps.
- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

Autres outils

- cdk_nag est un outil open source qui utilise une combinaison de packs de règles pour vérifier que les AWS CDK applications respectent les meilleures pratiques.
- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.
- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans les AWS Control Tower contrôles de GitHub déploiement à l'aide AWS CDK du référentiel. Vous utilisez le fichier cdk.json pour interagir avec l' AWS CDK application, et vous utilisez le fichier package.json pour installer les packages npm.

Bonnes pratiques

- Respectez le principe du moindre privilège (documentation IAM). Les exemples de politique IAM et de politique de confiance fournis dans ce modèle incluent les autorisations minimales requises, et les AWS CDK piles créées dans le compte de gestion sont limitées par ces autorisations.
- Suivez les meilleures pratiques pour AWS Control Tower les administrateurs (AWS Control Tower documentation).
- Suivez les meilleures pratiques pour le développement et le déploiement d'une infrastructure cloud avec la AWS CDK (AWS CDK documentation).
- Lors du démarrage du AWS CDK, personnalisez le modèle de bootstrap pour définir les politiques et les comptes fiables qui devraient être capables de lire et d'écrire sur n'importe quelle ressource du compte de gestion. Pour plus d'informations, consultez la section Personnalisation du bootstrap.
- Utilisez des outils d'analyse de code, tels que cfn_nag, pour scanner les modèles générés. CloudFormation L'outil cfn-nag recherche dans les modèles des CloudFormation modèles susceptibles d'indiquer que l'infrastructure n'est pas sécurisée. Vous pouvez également utiliser cdk-nag pour vérifier vos CloudFormation modèles à l'aide du module cloudformation-include.

Épopées

Préparez-vous à activer les commandes

Tâche	Description	Compétences requises
Créez le rôle IAM dans le compte de gestion.	1. Créez une politique IAM dans le compte de gestion avec les autorisations définies dans la politique IAM dans la section Informations supplémentaires. Pour obtenir des instructions, consultez la section Création de	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises

	politiques IAM dans la documentation IAM. Prenez note de l'Amazon Resource Name (ARN) de la politique. Voici un exemple d'ARN.
	
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`
	
	2. Créez un rôle IAM dans le compte de gestion, joignez la politique d'autorisation IAM que vous avez créée à l'étape précédente et associez la politique de confiance personnalisée à la politique de confiance de la section Informations supplémentaires. Pour obtenir des instructions, consultez la section Création d'un rôle à l'aide de politiques de confiance personnalisées dans la documentation IAM. Voici un exemple d'ARN pour le nouveau rôle.
	
	`arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:role/<ROLE-NAME>`	

Tâche	Description	Compétences requises
Bootstrap. AWS CDK	1. Dans le compte de gestion, assumez un rôle autorisé à démarrer. AWS CDK 2. Entrez la commande suivante en remplaçant la commande suivante : • `<MANAGEMENT-ACCOUNT-ID>` est l'identifiant du compte de gestion de l'organisation. • `<AWS-CONTROL-TOWER-REGION>` est l' Région AWS endroit où AWS Control Tower est déployé. Pour une liste complète des codes de région, voir Points de terminaison régionaux dans la section Référence AWS générale. • `<DEPLOYMENT-ACCOUNT-ID>` est l'ID du compte de déploiement. • `<DEPLOYMENT-ROLE-NAME>` est le nom du rôle IAM que vous utilisez dans le compte de déploiement. • `<POLICY-NAME>` est le nom de la politique que vous avez créée dans le compte de gestion.	DevOps ingénieur, AWS général, Python

Tâche	Description	Compétences requises
	`$ npx cdk bootstrap aws://<MANAGEMENT-ACCOUNT-ID>/<AWS-CONTROL-TOWER-REGION> \ --trust arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-NAME> \ --cloudformation-execution-policies arn:aws:iam::<MANAGEMENT-ACCOUNT-ID>:policy/<POLICY-NAME>`	
Pour cloner le référentiel.	Dans un shell bash, entrez la commande suivante. Cela clone les AWS Control Tower contrôles Deploy à l'aide du AWS CDK référentiel de GitHub. `git clone https://github.com/aws-samples/aws-control-tower-controls-cdk.git`	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
Modifiez le fichier AWS CDK de configuration.	1. Dans le référentiel cloné, ouvrez le fichier constants .py. 2. Dans le `ACCOUNT_ID` paramètre, saisissez l'identifiant de votre compte de gestion. 3. Dans le `<AWS-CONTROL-TOWER-REGION>` paramètre, entrez l' Région AWS endroit où AWS Control Tower est déployé. 4. Dans le `ROLE_ARN` paramètre, entrez l'ARN du rôle que vous avez créé dans le compte de gestion. 5. Ouvrez Tous les identifiants globaux dans la AWS Control Tower documentation. 6. Dans la liste au format JSON, recherchez le contrôle que vous souhaitez implémenter, puis copiez son identifiant global (également appelé valeur {CONTROL_CATALOG_OPAQUE_ID}). Par exemple, l'identifiant global du contrôle AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED est.	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	`k4izcjxhukijhajp6k s5mjxk` 7. Dans la `GUARDRAIL S_CONFIGURATION` section, dans le `Enable-Control` paramètre, entrez l'identifiant global que vous avez copié. Entrez l'identifiant entre guillemets et séparez les différents identificateurs par des virgules. 8. Dans la `GUARDRAIL S_CONFIGURATION` section, dans le `OrganizationalUnit Ids` paramètre, entrez l'ID de l'unité organisationnelle dans laquelle vous souhaitez activer le contrôle, par exemple`ou-1111-1 1111111` . Entrez l'identif iant entre guillemets et séparez-le IDs par des virgules. Pour plus d'informations sur la façon de récupérer une unité d'organisation IDs, consultez la section Affichage des détails d'une unité d'organisation. 9. Enregistrez et fermez le fichier constants.py.	

Tâche	Description	Compétences requises
	Pour un exemple de fichier constants.py mis à jour, consultez la section Informations supplémentaires de ce modèle.	

Activer les contrôles dans le compte de gestion

Tâche	Description	Compétences requises
Assumez le rôle IAM dans le compte de déploiement.	Dans le compte de déploiement, assumez le rôle IAM autorisé à déployer les AWS CDK piles du compte de gestion. Pour plus d'informations sur l'attribution d'un rôle IAM dans le AWS CLI, voir Utiliser un rôle IAM dans le AWS CLI.	DevOps ingénieur, AWS général
Activez l'environnement.	Si vous utilisez Linux ou macOS : 1. Entrez la commande suivante pour créer un environnement virtuel. `$ python3 -m venv .venv` 2. Une fois l'environnement virtuel créé, entrez la commande suivante pour l'activer.	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises

	`$ source .venv/bin/activate`
	
	Si vous utilisez Windows :
	
	1. Entrez la commande suivante pour activer un environnement virtuel.
	
	`% .venv\Scripts\activate.bat`	

Installez les dépendances.	Une fois l'environnement virtuel activé, entrez la commande suivante pour exécuter le script install_deps.sh. Ce script installe les dépendances requises. `$ ./scripts/install_deps.sh`	DevOps ingénieur, AWS général, Python

Déployez la pile.	Entrez les commandes suivantes pour synthétiser et déployer la CloudFormation pile.
	
	`$ npx cdk synth`
	`$ npx cdk deploy`
		DevOps ingénieur, AWS général, Python

Ressources connexes

AWS documentation

- À propos des contrôles (AWS Control Tower documentation)
- Bibliothèque de commandes (AWS Control Tower documentation)
- AWS CDK Commandes du kit d'outils (AWS CDK documentation)
- Déployez et gérez les AWS Control Tower contrôles à l'aide de Terraform (directivesAWS prescriptives)

Autres ressources

- Python

Informations supplémentaires

Exemple de fichier constants.py

Voici un exemple de fichier constants.py mis à jour. Cet exemple active le contrôle AWS-GR_DISALLOW_CROSS_REGION_NETWORKING (ID global :) et le contrôle AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED (ID global :**`dvuaav61i5cnfazfelmvn9m6k`**). `50z1ot237wl8u1lv5ufau6qqo` Pour une liste des identifiants globaux IDs, voir Tous les identifiants globaux dans la AWS Control Tower documentation.

```
ACCOUNT_ID = 111122223333
AWS_CONTROL_TOWER_REGION = us-east-2
ROLE_ARN = "arn:aws:iam::111122223333:role/CT-Controls-Role"
GUARDRAILS_CONFIGURATION = [
    {
        "Enable-Control": {
            "dvuaav61i5cnfazfelmvn9m6k": {  # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
                "Parameters": {
                    "ExemptedPrincipalArns": ["arn:aws:iam::111122223333:role/
RoleName"]
                },
                "Tags": [{"key": "Environment", "value": "Production"}]
            },
            ...
        },
        "OrganizationalUnitIds": ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
```

```
        "Enable-Control": {
            "50z1ot237wl8u1lv5ufau6qqo",  # AWS-
GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        },
        "OrganizationalUnitIds": ["ou-2222-22222222"...],
    },
]
```

Politique IAM

L'exemple de politique suivant autorise les actions minimales requises pour activer ou désactiver les AWS Control Tower contrôles lors du déploiement de AWS CDK piles d'un compte de déploiement vers le compte de gestion.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Politique d’approbation

La politique de confiance personnalisée suivante permet à un rôle IAM spécifique dans le compte de déploiement d'assumer le rôle IAM dans le compte de gestion. Remplacez les éléments suivants :

- <DEPLOYMENT-ACCOUNT-ID>est l'ID du compte de déploiement
- <DEPLOYMENT-ROLE-NAME>est le nom du rôle dans le compte de déploiement qui est autorisé à assumer le rôle dans le compte de gestion

```
{
    “Version”: “2012-10-17”,
    “Statement”: [
        {
            “Effect”: “Allow”,
            “Principal”: {
                “AWS”: “arn:aws:iam::<DEPLOYMENT-ACCOUNT-ID>:role/<DEPLOYMENT-ROLE-
NAME>”
            },
            “Action”: “sts:AssumeRole”,
            “Condition”: {}
        }
    ]
}
```

Déployez et gérez les AWS Control Tower contrôles à l'aide de Terraform

Créée par Iker Reina Fuente (AWS) et Ivan Girardi (AWS)

Récapitulatif

Ce modèle décrit comment utiliser les AWS Control Tower contrôles, HashiCorp Terraform et l'infrastructure en tant que code (IaC) pour mettre en œuvre et administrer des contrôles de sécurité préventifs, détectifs et proactifs. Un contrôle (également appelé garde-corps) est une règle de haut niveau qui fournit une gouvernance continue de votre environnement global AWS Control Tower . Par exemple, vous pouvez utiliser des contrôles pour exiger la journalisation de votre compte, Comptes AWS puis configurer des notifications automatiques si des événements spécifiques liés à la sécurité se produisent.

AWS Control Tower vous aide à mettre en œuvre des contrôles préventifs, détectifs et proactifs qui régissent vos AWS ressources et surveillent la conformité sur plusieurs sites Comptes AWS. Chaque contrôle applique une seule règle. Dans ce modèle, vous utilisez un modèle IaC fourni pour spécifier les contrôles que vous souhaitez déployer dans votre environnement.

AWS Control Tower les contrôles s'appliquent à l'ensemble d'une unité organisationnelle (UO), et le contrôle affecte chaque unité Compte AWS au sein de l'UO. Par conséquent, lorsque les utilisateurs effectuent une action sur n'importe quel compte de votre zone de landing zone, l'action est soumise aux contrôles qui régissent l'unité d'organisation.

La mise en œuvre de AWS Control Tower contrôles permet d'établir une base de sécurité solide pour votre zone AWS d'atterrissage. En utilisant ce modèle pour déployer les commandes sous forme d'iAc via Terraform, vous pouvez standardiser les commandes dans votre zone d'atterrissage et les déployer et les gérer plus efficacement.

Pour déployer AWS Control Tower des contrôles sous forme d'iAc, vous pouvez également les utiliser à la AWS Cloud Development Kit (AWS CDK) place de Terraform. Pour plus d'informations, voir Déployer et gérer les AWS Control Tower contrôles à l'aide de AWS CDK et AWS CloudFormation.

Public visé

Ce modèle est recommandé aux utilisateurs expérimentés avec AWS Control Tower Terraform et. AWS Organizations

Conditions préalables et limitations

Prérequis

- Comptes AWS Gestion active en tant qu'organisation AWS Organizations et en tant que zone de AWS Control Tower landing zone. Pour obtenir des instructions, consultez la section Mise en route dans la AWS Control Tower documentation.
- AWS Command Line Interface (AWS CLI), installé et configuré.
- Rôle AWS Identity and Access Management (IAM) dans le compte de gestion autorisé à déployer ce modèle. Pour plus d'informations sur les autorisations requises et un exemple de politique, consultez la section Autorisations de moindre privilège pour le rôle IAM dans la section Informations supplémentaires de ce modèle.
- Autorisations permettant d'assumer le rôle IAM dans le compte de gestion.
- Terraform CLI, installée (documentation Terraform).
- AWS Fournisseur Terraform, configuré (documentation Terraform).
- Backend Terraform, configuré (documentation Terraform).

Limites

- Pour les AWS Control Tower contrôles, ce modèle nécessite l'utilisation d'identifiants globaux au format suivant :

```
arn:<PARTITION>:controlcatalog:::control/<CONTROL_CATALOG_OPAQUE_ID>
```

  Les versions précédentes de ce modèle utilisaient des identifiants régionaux qui ne sont plus pris en charge. Nous vous recommandons de passer des identifiants régionaux aux identifiants globaux. Les identifiants globaux vous aident à gérer les contrôles et à augmenter le nombre de contrôles que vous pouvez utiliser.

> **Note**
>
> Dans la plupart des cas, la valeur de `<PARTITION>` est `aws`.

Versions du produit

- AWS Control Tower version 3.2 ou ultérieure
- Terraform version 1.5 ou ultérieure
- Terraform AWS Provider version 4.67 ou ultérieure

Architecture

Cette section fournit une présentation générale de cette solution et de l'architecture établie par l'exemple de code. Le schéma suivant montre les contrôles déployés sur les différents comptes de l'unité d'organisation.

AWS Control Tower les contrôles sont classés en fonction de leur comportement et de leurs instructions.

Il existe trois principaux types de comportements de contrôle :

1. Les contrôles préventifs sont conçus pour empêcher les actions de se produire. Elles sont mises en œuvre avec des politiques de contrôle des services (SCPs) ou des politiques de contrôle des ressources (RCPs) dans AWS Organizations. Le statut d'un contrôle préventif est soit appliqué, soit non activé. Les contrôles préventifs sont pris en charge dans tous les cas Régions AWS.
2. Les contrôles Detective sont conçus pour détecter des événements spécifiques lorsqu'ils se produisent et pour enregistrer l'action AWS CloudTrail. Elles sont mises en œuvre avec AWS Config des règles. Le statut d'un contrôle de détection est soit clair, soit en violation, soit non activé. Les contrôles Detective ne s'appliquent que dans ceux Régions AWS pris en charge par AWS Control Tower.
3. Les contrôles proactifs analysent les ressources qui seraient mises à disposition par votre entreprise AWS CloudFormation et vérifient si elles sont conformes aux politiques et aux objectifs de votre entreprise. Les ressources non conformes ne seront pas provisionnées. Ils sont implémentés avec des AWS CloudFormation crochets. Le statut d'un contrôle proactif est PASS, FAIL ou SKIP.

Les conseils de contrôle sont la pratique recommandée pour savoir comment appliquer chaque contrôle à votre OUs. AWS Control Tower fournit trois catégories de conseils : obligatoires, fortement recommandés et facultatifs. Le guidage d'un contrôle est indépendant de son comportement. Pour plus d'informations, consultez la section Contrôle du comportement et instructions.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier la façon dont les ressources sont liées les unes aux autres et comment leurs configurations ont évolué au fil du temps.
- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.

Autres outils

- HashiCorp Terraform est un outil d'infrastructure en tant que code (IaC) qui vous aide à utiliser le code pour provisionner et gérer l'infrastructure et les ressources du cloud.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Déployer et gérer les AWS Control Tower contrôles à l'aide du référentiel Terraform.

Bonnes pratiques

- Le rôle IAM utilisé pour déployer cette solution doit respecter le principe du moindre privilège (documentation IAM).
- Suivez les meilleures pratiques pour AWS Control Tower les administrateurs (AWS Control Tower documentation).

Épopées

Activer les contrôles dans le compte de gestion

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Dans un shell bash, entrez la commande suivante. Cela clone les AWS Control Tower contrôles de déploiement et de gestion à l'aide du référentiel Terraform à partir de. GitHub `git clone https://github.com/aws-samples/aws-control-tower-controls-terraform.git`	DevOps ingénieur
Modifiez le fichier de configuration du backend Terraform.	1. Dans le dépôt cloné, ouvrez le fichier backend.tf. 2. Modifiez le fichier pour définir la configuration du backend Terraform. La configuration que vous définissez dans ce fichier dépend de votre environnement. Pour plus d'informations, consultez la section Configuration du backend (documentation Terraform). 3. Enregistrez et fermez le fichier backend.tf.	DevOps ingénieur, Terraform
Modifiez le fichier de configuration du fournisseur Terraform.	1. Dans le référentiel cloné, ouvrez le fichier provider.tf.	DevOps ingénieur, Terraform

Tâche	Description	Compétences requises
	2. Modifiez le fichier pour définir la configuration du fournisseur Terraform . Pour plus d'informations, consultez la section Configuration du fournisseur (documentation Terraform). Définissez le Région AWS comme région dans laquelle l' AWS Control Tower API est disponible. 3. Enregistrez et fermez le fichier provider.tf.	

Tâche	Description	Compétences requises
Modifiez le fichier de configuration.	1. Dans le référentiel cloné, ouvrez le fichier variables.tfvars. 2. Ouvrez Tous les identifiants globaux dans la AWS Control Tower documentation. 3. Dans la liste au format JSON, recherchez le contrôle que vous souhaitez implémenter, puis copiez son identifiant global (également appelé valeur {CONTROL_CATALOG_OPAQUE_ID}). Par exemple, l'identifiant global du contrôle AWS-GR_AUDIT_BUCKET_ENCRYPTION_ENABLED est. `k4izcjxhukijhajp6ks5mjxk` 4. Dans la `controls` section, dans le `control_names` paramètre, entrez l'identifiant global que vous avez copié. 5. Dans la `controls` section, dans le `organizational_unit_ids` paramètre, entrez l'ID de l'unité organisationnelle dans laquelle vous souhaitez activer le contrôle, par	DevOps ingénieur, AWS général, Terraform

Tâche	Description	Compétences requises
	exemple`ou-1111-1111111` . Entrez l'identifiant entre guillemets et séparez-le IDs par des virgules. Pour plus d'informations sur la façon de récupérer une unité d'organisation IDs, consultez la section Affichage des détails d'une unité d'organisation. 6. Enregistrez et fermez le fichier variables.tfvars. Pour un exemple de fichier variables.tfvars mis à jour, consultez la section Informations supplémentaires de ce modèle.	
Assumez le rôle IAM dans le compte de gestion.	Dans le compte de gestion, assumez le rôle IAM autorisé à déployer le fichier de configuration Terraform. Pour plus d'informations sur les autorisations requises et un exemple de politique, consultez la section Autorisations de moindre privilège pour le rôle IAM dans la section Informations supplémentaires. Pour plus d'informations sur l'attribution d'un rôle IAM dans le AWS CLI, voir Utiliser un rôle IAM dans le. AWS CLI	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises

Déployez le fichier de configuration.	1. Entrez la commande suivante pour initialiser Terraform.
	`$ terraform init -upgrade`
	2. Entrez la commande suivante pour prévisualiser les modifications par rapport à l'état actuel.
	`$ terraform plan -var-file="variables.tfvars"`
	3. Passez en revue les modifications de configuration dans le plan Terraform et confirmez que vous souhaitez implémenter ces modifications dans l'organisation.
	4. Entrez la commande suivante pour déployer les ressources.
	`$ terraform apply -var-file="variables.tfvars"`
		DevOps ingénieur, AWS général, Terraform

(Facultatif) Désactiver les contrôles dans le compte AWS Control Tower de gestion

Tâche	Description	Compétences requises
Exécutez la commande `destroy`.	Entrez la commande suivante pour supprimer les ressources déployées selon ce modèle. `$ terraform destroy -var-file="variables.tfvars"`	DevOps ingénieur, AWS général, Terraform

Résolution des problèmes

Problème	Solution
`Error: creating ControlTower Control ValidationException: Guardrail <control ID> is already enabled on organizational unit <OU ID>`Erreur	Le contrôle que vous essayez d'activer est déjà activé dans l'unité d'organisation cible. Cette erreur peut se produire si un utilisateur a activé manuellement le contrôle via AWS Management Console, via AWS Control Tower ou via AWS Organizations. Pour déployer le fichier de configuration Terraform, vous pouvez utiliser l'une des options suivantes. Option 1 : mettre à jour le fichier d'état actuel de Terraform Vous pouvez importer la ressource dans le fichier d'état actuel de Terraform. Lorsque vous réexécutez la `apply` commande, Terraform ignore cette ressource. Procédez comme suit pour importer la ressource dans l'état Terraform actuel : 1. Dans le compte AWS Control Tower de gestion, entrez la commande suivante pour

Problème	Solution

	récupérer la liste des Amazon Resource Names (ARNs) pour le OUs, où se `<root-ID>` trouve la racine de l'organisation. Pour plus d'informations sur la récupération de cet identifiant, consultez la section Affichage des détails de la racine.
	
	`aws organizations list-organizational-units-for-parent --parent-id <root-ID>`
	
	2. Pour chaque unité d'organisation renvoyée à l'étape précédente, entrez la commande suivante, où se `<OU-ARN>` trouve l'ARN de l'unité d'organisation.
	
	`aws controltower list-enabled-controls --target-identifier <OU-ARN>`
	
	3. Copiez ARNs et effectuez l'importation Terraform dans le module requis afin qu'il soit inclus dans l'état Terraform. Pour obtenir des instructions, voir Importer (documentation Terraform).
	4. Répétez les étapes décrites dans Déployer la configuration dans la section Epics.
	
	Option 2 : désactiver le contrôle
	
	Si vous travaillez dans un environnement hors production, vous pouvez désactiver le contrôle dans la console. Réactivez-le en répétant les étapes décrites dans Déployer la configuration dans la section Epics. Cette approche n'est pas recommandée pour les environnements de production car le contrôle sera désactivé

Problème	Solution
	pendant un certain temps. Si vous souhaitez utiliser cette option dans un environnement de production, vous pouvez implémenter des contrôles temporaires, tels que l'application temporaire d'un SCP. AWS Organizations

Ressources connexes

AWS documentation

- À propos des contrôles (AWS Control Tower documentation)
- Bibliothèque de commandes (AWS Control Tower documentation)
- Déployez et gérez les AWS Control Tower contrôles à l'aide de AWS CDK et AWS CloudFormation (AWS directives prescriptives)

Autres ressources

- Terraforme
- Documentation de la CLI Terraform

Informations supplémentaires

Exemple de fichier variables.tfvars

Voici un exemple de fichier variables.tfvars mis à jour. Cet exemple active le contrôle AWS-GR_ENCRYPTED_VOLUMES (ID global :) et le contrôle AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED (ID global :`503uicglhjkokaajywfpt6ros`). `50z1ot237wl8u1lv5ufau6qqo` Pour une liste des identifiants globaux IDs, voir Tous les identifiants globaux dans la AWS Control Tower documentation.

L'exemple suivant active également les contrôles dotés de paramètres tels que CT.S3.PV.5 (ID global :**`7mo7a2h2ebsq7118k6uzr96ou`**) et CT.SECRETSMANAGER.PV.1 (ID global :). `dvhe47fxg5o6lryqrq9g6sxg4` Pour une liste des contrôles avec paramètres, voir Contrôles avec paramètres dans la AWS Control Tower documentation.

```
controls = [
    {
        control_names = [
            "503uicglhjkokaajywfpt6ros", # AWS-GR_ENCRYPTED_VOLUMES
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111", "ou-2222-22222222"...],
    },
    {
        control_names = [
            "50z1ot237wl8u1lv5ufau6qqo", # AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED
            ...
        ],
        organizational_unit_ids = ["ou-1111-11111111"...],
    },
]

controls_with_params = [
  {
    control_names = [
      { "7mo7a2h2ebsq71l8k6uzr96ou" = { # CT.S3.PV.5
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
          "ExemptedResourceArns" : [],
        }
      } },
      { "dvhe47fxg5o6lryqrq9g6sxg4" = { # CT.SECRETSMANAGER.PV.1
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-1111-11111111"...]
  },
  {
    control_names = [
      { "dvuaav61i5cnfazfelmvn9m6k" = { # AWS-GR_DISALLOW_CROSS_REGION_NETWORKING
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      { "41ngl8m5c4eb1myoz0t707n7h" = { # AWS-GR_DISALLOW_VPC_INTERNET_ACCESS
```

```
        parameters = {
          "ExemptedPrincipalArns" : ["arn:aws:iam::*:role/RoleName"],
        }
      } },
      ...
    ],
    organizational_unit_ids = ["ou-2222-22222222"...]
  }
]
```

Autorisations avec le moindre privilège pour le rôle IAM

Ce modèle nécessite que vous assumiez un rôle IAM dans le compte de gestion. La meilleure pratique consiste à assumer un rôle avec des autorisations temporaires et à limiter les autorisations conformément au principe du moindre privilège. L'exemple de politique suivant autorise les actions minimales requises pour activer ou désactiver les AWS Control Tower contrôles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "controltower:EnableControl",
                "controltower:DisableControl",
                "controltower:GetControlOperation",
                "controltower:ListEnabledControls",
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeOrganization",
                "organizations:DetachPolicy",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:UpdatePolicy"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Déployez un pipeline qui détecte simultanément les problèmes de sécurité dans plusieurs livrables de code

Créée par Benjamin Morris (AWS), Dina Odum (AWS), Isaiah Schisler (AWS), Sapeksh Madan (AWS) et Tim Hahn (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus.

Le Simple Code Scanning Pipeline (SCSP) permet de créer en deux clics un pipeline d'analyse de code qui exécute en parallèle des outils de sécurité open source conformes aux normes du secteur. Cela permet aux développeurs de vérifier la qualité et la sécurité de leur code sans avoir à installer d'outils ni même à comprendre comment les exécuter. Cela vous permet de réduire les vulnérabilités et les erreurs de configuration dans les livrables du code. Cela réduit également le temps que votre entreprise consacre à l'installation, à la recherche et à la configuration des outils de sécurité.

Avant le SCSP, la numérisation du code à l'aide de cette suite particulière d'outils nécessitait que les développeurs localisent, installent et configurent manuellement les outils d'analyse logicielle. Même installés localement, all-in-one les outils, tels que Automated Security Helper (ASH), nécessitent la configuration d'un conteneur Docker pour fonctionner. Cependant, avec SCSP, une suite d'outils d'analyse de code conformes aux normes du secteur s'exécute automatiquement dans le. AWS Cloud Avec cette solution, vous utilisez Git pour publier les livrables de votre code, puis vous recevez un résultat visuel indiquant at-a-glance quels contrôles de sécurité ont échoué.

Conditions préalables et limitations

- Un actif Compte AWS
- Un ou plusieurs livrables de code que vous souhaitez analyser pour détecter des problèmes de sécurité
- AWS Command Line Interface (AWS CLI), installé et configuré
- Python version 3.0 ou ultérieure et pip version 9.0.3 ou ultérieure, installés
- Git, installé
- Installation git-remote-codecommitsur votre poste de travail local

Architecture

Pile technologique cible

- AWS CodeCommit référentiel
- AWS CodeBuild projet
- AWS CodePipeline pipeline
- Compartiment Amazon Simple Storage Service (Amazon S3)
- AWS CloudFormation modèle

Architecture cible

Le SCSP pour l'analyse de code statique est un DevOps projet conçu pour fournir des informations de sécurité sur le code livrable.

1. Dans le AWS Management Console, connectez-vous à la cible Compte AWS. Vérifiez que vous vous trouvez à l' Région AWS endroit où vous souhaitez déployer le pipeline.
2. Utilisez le CloudFormation modèle du référentiel de code pour déployer la pile SCSP. Cela crée un nouveau CodeCommit référentiel et un nouveau CodeBuild projet.

   > **Note**
   >
   > Comme autre option de déploiement, vous pouvez utiliser un CodeCommit dépôt existant en fournissant le nom de ressource Amazon (ARN) du référentiel en tant que paramètre lors du déploiement de la pile.

3. Clonez le référentiel sur votre poste de travail local, puis ajoutez les fichiers dans leurs dossiers respectifs dans le référentiel cloné.
4. Utilisez Git pour ajouter, valider et transférer les fichiers dans le CodeCommit référentiel.
5. Le transfert vers le CodeCommit référentiel initie une CodeBuild tâche. Le CodeBuild projet utilise les outils de sécurité pour scanner les livrables du code.
6. Passez en revue le résultat du pipeline. Les outils de sécurité qui détectent des problèmes de niveau d'erreur entraîneront l'échec des actions dans le pipeline. Corrigez ces erreurs ou supprimez-les en tant que faux positifs. Consultez les détails de la sortie de l'outil dans les détails de l'action dans CodePipeline ou dans le compartiment S3 du pipeline.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.

Autres outils

Pour obtenir la liste complète des outils utilisés par le SCSP pour scanner les livrables du code, consultez le fichier readme du SCSP dans. GitHub

Référentiel de code

Le code de ce modèle est disponible dans le référentiel SCSP (Simple Code Scanning Pipeline) dans GitHub.

Épopées

Déployez le SCSP

Tâche	Description	Compétences requises
Créez la CloudFormation pile.	1. Connectez-vous à la AWS Management Console. 2. Dans la console, vérifiez que vous vous trouvez dans la région cible dans laquelle vous souhaitez déployer la solution. Pour plus d'informations, voir Choisir une région.	AWS DevOps, administrateur AWS

Tâche	Description	Compétences requises
	3. Cliquez sur le lien suivant. Cela ouvre l'assistant de création rapide de piles dans CloudFormation. https://console.aws.amazon.com/cloudformation/maison ? #/ -Pipeline-Stack.Template.JSON&StackName= stacks/create/review?templateURL=https://proservetools.s3.amazonaws.com/cft/scsp SimpleCodeScanPipeline 4. Dans l'assistant de création rapide d'une pile, passez en revue les paramètres de votre pile et apportez les modifications nécessaires à votre cas d'utilisation. 5. Sélectionnez Je reconnais qu'AWS est CloudFormation susceptible de créer des ressources IAM, puis choisissez Create stack. Cela crée un CodeCommit référentiel, un CodePipeline pipeline, plusieurs définitions de CodeBuild tâches et un compartiment S3. Les exécutions de build et les résultats de numérisation sont	

Tâche	Description	Compétences requises
	copiés dans ce compartiment. Une fois la CloudFormation pile complètement déployée, le SCSP est prêt à être utilisé.	

Utiliser le pipeline

Tâche	Description	Compétences requises
Examinez les résultats de l'analyse.	1. Dans la console Amazon S3, dans Buckets, choisissez le bucket simplecodescanpipeline-deleteresourcespipelinereso. 2. Choisissez le répertoire scan_results, puis le dossier portant le dernier horodatage de numérisation. 3. Passez en revue les fichiers journaux de ce dossier pour vérifier les éventuels problèmes détectés par les outils de sécurité utilisés dans le pipeline. Les outils de sécurité qui détectent des problèmes de niveau d'erreur entraîneront `failed` des actions dans le pipeline. Ces erreurs doivent être corrigées ou supprimées s'il s'agit de faux positifs.	Développeur d'applications, AWS DevOps

Tâche	Description	Compétences requises
	Note Vous pouvez également consulter les détails de la sortie de l'outil (pour les scans réussis ou échoués) dans la CodePipeline console, dans la section Détails de l'action.	

Résolution des problèmes

Problème	Solution
HashiCorp Terraform ou AWS CloudFormation les fichiers ne sont pas numérisés.	Assurez-vous que les fichiers Terraform (.tf) et CloudFormation (.yml, .yaml ou .json) sont placés dans les dossiers appropriés du référentiel cloné. CodeCommit
La `git clone` commande échoue.	Assurez-vous que vous avez installé le référenti el `git-remote-codecommit` et que votre CLI a accès aux AWS informations d'identification autorisées à lire le CodeCommit référentiel.
Une erreur de simultanéité, telle que`Project-level concurrent build limit cannot exceed the account-level concurrent build limit of 1 .`	Réexécutez le pipeline en cliquant sur le bouton Release Change dans la CodePipel ine console. Il s'agit d'un problème connu qui semble être le plus courant les premières fois que le pipeline fonctionne.

Ressources connexes

Donnez votre avis sur le projet SCSP.

Informations supplémentaires

FAQ

Le projet SCSP est-il identique à Automated Security Helper (ASH) ?

Non. Utilisez ASH lorsque vous recherchez un outil CLI qui exécute des outils de numérisation de code à l'aide de conteneurs. Automated Security Helper (ASH) est un outil conçu pour réduire la probabilité d'une violation de sécurité dans un nouveau code, une nouvelle infrastructure ou une nouvelle configuration de ressources IAM. ASH est un utilitaire de ligne de commande qui peut être exécuté localement. L'utilisation locale nécessite l'installation et le fonctionnement d'un environnement de conteneurs sur le système.

Utilisez SCSP lorsque vous souhaitez un pipeline de configuration plus facile qu'ASH. Le SCSP ne nécessite aucune installation locale. Le SCSP est conçu pour exécuter des vérifications individuellement dans un pipeline et afficher les résultats par outil. Le SCSP évite également une grande partie de la surcharge liée à la configuration de Docker, et il est indépendant du système d'exploitation (OS).

Le SCSP est-il réservé aux équipes de sécurité ?

Non, n'importe qui peut déployer le pipeline pour déterminer quelles parties de son code échouent aux contrôles de sécurité. Par exemple, les utilisateurs non liés à la sécurité peuvent utiliser le SCSP pour vérifier leur code avant de le vérifier avec leurs équipes de sécurité.

Puis-je utiliser SCSP si je travaille avec un autre type de dépôt, tel que GitLab GitHub, ou Bitbucket ?

Vous pouvez configurer un dépôt git local pour qu'il pointe vers deux référentiels distants différents. Par exemple, vous pouvez cloner un GitLab référentiel existant, créer une instance SCSP (en spécifiant CloudFormation les dossiers Terraform et AWS Config Rules Development Kit (AWS RDK), si nécessaire), puis l'utiliser `git remote add upstream <SCSPGitLink>` pour pointer également le référentiel local vers le référentiel CodeCommit SCSP. Cela permet d'envoyer les modifications de code au SCSP d'abord, de les valider, puis, après toute mise à jour supplémentaire apportée pour répondre aux résultats, de les transférer vers le GitLab référentiel GitHub, ou Bitbucket. Pour plus d'informations sur les télécommandes multiples, voir Envoyer des validations vers un dépôt Git supplémentaire (article de AWS blog).

> **Note**
>
> Faites attention à la dérive, par exemple en évitant d'apporter des modifications par le biais d'interfaces Web.

Contribuer et ajouter vos propres actions

La configuration du SCSP est gérée en tant que GitHub projet, qui contient le code source de l'application SCSP AWS Cloud Development Kit (AWS CDK) . Pour ajouter des contrôles supplémentaires au pipeline, l' AWS CDK application doit être mise à jour, puis synthétisée ou déployée dans la cible sur Compte AWS laquelle le pipeline sera exécuté. Pour ce faire, commencez par cloner le GitHub projet SCSP, puis recherchez le fichier de définition de pile dans le `lib` dossier.

Si vous souhaitez ajouter une vérification supplémentaire, la `StandardizedCodeBuildProject` classe du AWS CDK code permet d'ajouter des actions très facilement. Entrez le nom, la description `install` et/ou `build` les commandes. AWS CDK crée le CodeBuild projet en utilisant des valeurs par défaut raisonnables. Outre la création du projet de génération, vous devez l'ajouter aux CodePipeline actions de la phase de génération. Lors de la conception d'un nouveau contrôle, l'action doit être `FAIL` effectuée si l'outil d'analyse détecte des problèmes ou ne s'exécute pas. L'action devrait être `PASS` exécutée si l'outil de numérisation ne détecte aucun problème. Pour obtenir un exemple de configuration d'un outil, consultez le code de l'`Bandit`action.

Pour plus d'informations sur les entrées et sorties attendues, consultez la documentation du référentiel.

Si vous ajoutez des actions personnalisées, vous devez déployer le SCSP à l'aide de `cdk deploy` ou`cdk synth + CloudFormation deploy`. Cela est dû au fait que le CloudFormation modèle de pile Quick Create est géré par les propriétaires du dépôt.

Déployez des contrôles d'accès basés sur des attributs de détection pour les sous-réseaux publics en utilisant AWS Config

Créée par Alberto Menendez (AWS)

Récapitulatif

Les architectures de réseau de périphérie distribuées reposent sur une sécurité de périphérie du réseau qui s'exécute parallèlement aux charges de travail dans leurs clouds privés virtuels (VPCs). Cela permet une évolutivité sans précédent par rapport à l'approche centralisée plus courante. Bien que le déploiement de sous-réseaux publics dans les comptes de charge de travail puisse présenter des avantages, il présente également de nouveaux risques de sécurité car il augmente la surface d'attaque. Nous vous recommandons de déployer uniquement des ressources Elastic Load Balancing, telles que des équilibreurs de charge d'application ou des passerelles NAT dans leurs sous-réseaux publics. VPCs L'utilisation d'équilibreurs de charge et de passerelles NAT dans des sous-réseaux publics dédiés vous permet de mettre en œuvre un contrôle précis du trafic entrant et sortant.

Nous vous recommandons de mettre en œuvre des contrôles préventifs et de détection afin de limiter les types de ressources pouvant être déployées dans les sous-réseaux publics. Pour plus d'informations sur l'utilisation du contrôle d'accès basé sur les attributs (ABAC) pour déployer des contrôles préventifs pour les sous-réseaux publics, voir Déployer des contrôles d'accès préventifs basés sur les attributs pour les sous-réseaux publics. Bien qu'ils soient efficaces dans la plupart des situations, ces contrôles préventifs peuvent ne pas répondre à tous les cas d'utilisation possibles. Par conséquent, ce modèle s'appuie sur l'approche ABAC et vous aide à configurer des alertes concernant les ressources non conformes déployées dans des sous-réseaux publics. La solution vérifie si les interfaces réseau élastiques appartiennent à une ressource non autorisée dans les sous-réseaux publics.

Pour ce faire, ce modèle utilise des règles AWS Config personnalisées et ABAC. La règle personnalisée traite la configuration d'une interface elastic network à chaque fois qu'elle est créée ou modifiée. À un niveau élevé, cette règle exécute deux actions pour déterminer si l'interface réseau est conforme :

1. Pour déterminer si l'interface réseau est couverte par la règle, celle-ci vérifie si le sous-réseau possède des AWS balises spécifiques indiquant qu'il s'agit d'un sous-réseau public. Par exemple, cette balise peut être`IsPublicFacing=True`.

2. Si l'interface réseau est déployée dans un sous-réseau public, la règle vérifie qui Service AWS a créé cette ressource. Si la ressource n'est pas une ressource Elastic Load Balancing ou une passerelle NAT, elle la marque comme non conforme.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- AWS Config, configuré dans le compte de charge de travail
- Autorisations pour déployer les ressources requises dans le compte de charge de travail
- Un VPC avec des sous-réseaux publics
- Balises correctement appliquées pour identifier les sous-réseaux publics cibles
- (Facultatif) Une organisation dans AWS Organizations
- (Facultatif) Un compte de sécurité central qui est l'administrateur délégué pour AWS Config et AWS Security Hub

Architecture

Architecture cible

Le diagramme illustre les éléments suivants :

1. Lorsqu'une ressource Elastic Network Interface (`AWS::EC2::NetworkInterface`) est déployée ou modifiée, elle AWS Config capture l'événement et la configuration.
2. AWS Config compare cet événement à la règle personnalisée utilisée pour évaluer la configuration.
3. La AWS Lambda fonction associée à cette règle personnalisée est invoquée. La fonction évalue la ressource et applique la logique spécifiée pour déterminer si la configuration de la ressource est `COMPLIANT` `NON_COMPLIANT` ou`NOT_APPLICABLE`.
4. S'il est déterminé qu'une ressource l'est`NON_COMPLIANT`, AWS Config envoie une alerte via Amazon Simple Notification Service (Amazon SNS).

> **Note**
>
> Si ce compte est un compte de membre AWS Organizations, vous pouvez envoyer des données de conformité à un compte de sécurité central via AWS Config ou AWS Security Hub.

Logique d'évaluation de la fonction Lambda

Le schéma suivant montre la logique appliquée par la fonction Lambda pour évaluer la conformité de l'interface Elastic Network.

Automatisation et mise à l'échelle

Ce modèle est une solution de détective. Vous pouvez également le compléter par une règle de correction afin de résoudre automatiquement les ressources non conformes. Pour plus d'informations, voir Corriger les ressources non conformes à l'aide AWS Config de règles.

Vous pouvez adapter cette solution en :

- Appliquer les AWS balises correspondantes que vous définissez pour identifier les sous-réseaux destinés au public. Pour plus d'informations, consultez la section Politiques relatives aux balises dans la AWS Organizations documentation.
- Configuration d'un compte de sécurité central qui applique la règle AWS Config personnalisée à chaque compte de charge de travail de l'organisation. Pour plus d'informations, consultez Automatiser la conformité des configurations à grande échelle dans AWS (article de AWS blog).
- AWS Config Intégrer AWS Security Hub afin de capturer, de centraliser et de notifier à grande échelle. Pour plus d'informations, consultez la section Configuration AWS Config dans la AWS Security Hub documentation.

Outils

- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier la façon dont les ressources sont liées les unes aux autres et comment leurs configurations ont évolué au fil du temps.

- Elastic Load Balancing répartit le trafic applicatif ou réseau entrant sur plusieurs cibles. Par exemple, vous pouvez répartir le trafic entre les instances, les conteneurs et les adresses IP d'Amazon Elastic Compute Cloud (Amazon EC2) dans une ou plusieurs zones de disponibilité.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Bonnes pratiques

Pour plus d'exemples et de bonnes pratiques en matière de développement de AWS Config règles personnalisées, consultez le référentiel de AWS Config règles officiel sur GitHub.

Épopées

Déployez la solution

Tâche	Description	Compétences requises
Créez la fonction Lambda.	1. Connectez-vous à la AWS Lambda console AWS Management Console, puis ouvrez-la. 2. Sur la page Fonctions , choisissez Créer une fonction. 3. Sélectionnez Créer à partir de zéro. 4. Dans le volet Informations de base, pour Nom de la fonction, entrez un nom.	AWS général

Tâche	Description	Compétences requises
	5. Pour Environnement d’exécution, sélectionnez Python 3.12. 6. Laissez l'architecture définie sur x86_64. 7. Choisissez Créer une fonction. 8. Cliquez sur l’onglet Code. 9. Dans l'explorateur de fichiers, choisissez lambda_function.py. 10. Collez l'exemple de code fourni dans la section Informations supplémentaires de ce modèle dans l'onglet lambda_function.py. Personnalisez l'exemple de code pour identifier toute logique d'évaluation personnalisée dans la `evaluate_change_notification_compliance` fonction. 11. Choisissez Déployer.	

Tâche	Description	Compétences requises
Ajoutez des autorisations au rôle d'exécution de la fonction Lambda.	1. Dans le volet de navigation, choisissez Fonctions. 2. Choisissez la fonction que vous venez de créer. 3. Choisissez Configura tion (Configuration), puis Permissions (Autorisations). 4. Choisissez le nom du rôle pour ouvrir le rôle dans la console AWS Identity and Access Management (IAM). 5. Sous Politiques d'autoris ations, choisissez Ajouter des autorisations, puis choisissez Créer une politique en ligne. 6. Choisissez JSON. 7. Collez la politique suivante dans l'éditeur de politique s. Cela permet à la fonction Lambda de : • Obtenez les détails des balises de sous-réseau. • Renvoyez le résultat de conformité à AWS Config. `{ "Version": "2012-10-17", "Statement": [ { "Action": [`	AWS général

Tâche	Description	Compétences requises

	<pre>"config:PutEvaluations",
	"ec2:DescribeSubnets"
	],
	"Resource": "*",
	"Effect": "Allow"
	}
	]
	}</pre>
	8. Choisissez Suivant.
	9. Entrez un nom pour la stratégie, puis choisissez Create policy (Créer une stratégie).	

Récupérez la fonction Lambda Amazon Resource Name (ARN).	1. Ouvrez la console Lambda. 2. Dans le volet de navigation, choisissez Fonctions. 3. Choisissez la fonction que vous venez de créer. 4. Dans la section Vue d'ensemble des fonctions, sous Function ARN, copiez la valeur.	AWS général

Tâche	Description	Compétences requises
Créez la règle AWS Config personnalisée.	1. Ouvrez la AWS Config console. 2. Sur la page Règles, choisissez Ajouter une règle. 3. Sur la page Spécifier le type de règle, choisissez Créer une règle Lambda personnalisée, puis cliquez sur Suivant. 4. Sur la page Configurer les règles, procédez comme suit : a. Entrez un nom et une description. b. Pour l'ARN de la AWS Lambda fonction, collez l'ARN que vous avez précédemment copié. c. Pour Type de déclencheur, choisissez Lors de changements de configuration. d. Pour Étendue des modifications, sélectionnez Ressources. e. Pour Type de ressource, choisissez AWS EC2 NetworkInterface. f. Choisissez Suivant.	AWS général

Tâche	Description	Compétences requises
	5. Sur la page Réviser et créer, vérifiez votre règle, puis choisissez Enregistrer.	
Configurez les notifications.	1. Suivez les instructions de la section Création d'une rubrique Amazon SNS afin de créer une rubrique Amazon SNS. 2. Suivez les instructions de la section Abonnement à une rubrique Amazon SNS pour configurer un point de terminaison qui reçoit des notifications pour la rubrique Amazon SNS. 3. Suivez les instructions de la section Comment puis-je être averti lorsqu'une AWS ressource n'est pas conforme ? AWS Config Pour configurer une EventBridge règle Amazon personnalisée pour vos ressources non conformes.	AWS général

Tester la solution

Tâche	Description	Compétences requises
Créez une ressource conforme.	1. Suivez les instructions suivantes pour créer l'une des ressources prises en	AWS général

Tâche	Description	Compétences requises
	charge dans un sous-rése au public : • Création d'une passerelle NAT • Mise en route avec les Network Load Balancers • Création d'un Application Load Balancer 2. Une fois la ressource créée, la règle AWS Config personnalisée évalue les interfaces réseau élastique s associées à la ressource . Il marque ces interfaces réseau commeCOMPLIANT . Vous pouvez consulter les ressources en AWS Config procédant comme suit : a. Ouvrez la AWS Config console. b. Sur la page Règles, choisissez votre règle. c. Sur la page détaillée de la règle, rendez-vous au bas de la page. d. Sous Ressources concernées, sélection nez Conforme. Vérifiez que vous voyez IDs les interfaces réseau créées. e. Pour plus de détails sur la configuration	

Tâche	Description	Compétences requises
	de l'interface réseau, choisissez l'ID de ressource.	

Tâche	Description	Compétences requises
Créez une ressource non conforme.	1. Suivez les instructions suivantes pour créer une ressource non conforme dans un sous-réseau public : • Lancer une EC2 instance Amazon • Création d'une instance de base de données Amazon Relationa l Database Service (Amazon RDS) • Création d'un point de terminaison VPC 2. Une fois la ressource créée, la règle AWS Config personnalisée évalue les interfaces réseau élastique s associées à la ressource . Il marque ces interfaces réseau commeNON_COMPL IANT . Vous pouvez consulter les ressources en AWS Config procédant comme suit : a. Ouvrez la AWS Config console. b. Sur la page Règles, choisissez votre règle. c. Sur la page détaillée de la règle, rendez-vous au bas de la page.	AWS général

Tâche	Description	Compétences requises
	d. Sous Ressources concernées, sélectionnez NonCompliant. Vérifiez que vous voyez IDs les interfaces réseau créées. e. Pour plus de détails sur la configuration de l'interface réseau, choisissez l'ID de ressource. 3. Vérifiez que vous recevez la notification sur le point de terminaison que vous avez configuré dans Amazon SNS.	
Créez une ressource qui ne s'applique pas.	1. Dans un sous-réseau privé, créez toute ressource nécessitant une interface Elastic Network. 2. Une fois la ressource créée, la règle AWS Config personnalisée évalue les interfaces réseau élastique s associées à la ressource . Il marque ces interfaces réseau comme`NOT_APPLICABLE` . Ces ressources ne sont pas affichées dans la AWS Config console.	AWS général

Ressources connexes

AWS documentation

- Configuration AWS Config
- AWS Config règles personnalisées
- ABAC pour AWS
- Déployez des contrôles d'accès préventifs basés sur les attributs pour les sous-réseaux publics

Autres AWS ressources

- Automatisez la conformité des configurations à grande échelle dans AWS
- Architectures d'inspection distribuées avec Gateway Load Balancer

Informations supplémentaires

Voici un exemple de fonction Lambda fourni à des fins de démonstration.

```
import boto3
import json
import os

# Init clients
config_client = boto3.client('config')
ec2_client = boto3.client('ec2')

def lambda_handler(event, context):

    # Init values
    compliance_value = 'NOT_APPLICABLE'
    invoking_event = json.loads(event['invokingEvent'])
    configuration_item = invoking_event['configurationItem']

    status = configuration_item['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']

    # First check if the event configuration applies. Ex. resource event is not delete
    if (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope:
        compliance_value = evaluate_change_notification_compliance(configuration_item)


    config_client.put_evaluations(
       Evaluations=[
           {
```

```
                'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
                'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
                'ComplianceType': compliance_value,
                'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
            },
        ],
        ResultToken=event['resultToken'])

# Function with the logs to evaluate the resource
def evaluate_change_notification_compliance(configuration_item):
    is_in_scope = is_in_scope_subnet(configuration_item['configuration']['subnetId'])

    if (configuration_item['resourceType'] != 'AWS::EC2::NetworkInterface') or not
 is_in_scope:
        return 'NOT_APPLICABLE'

    else:
        alb_condition = configuration_item['configuration']['requesterId'] in ['amazon-
elb']
        nlb_condition = configuration_item['configuration']['interfaceType'] in
 ['network_load_balancer']
        nat_gateway_condition = configuration_item['configuration']['interfaceType'] in
 ['nat_gateway']

        if alb_condition or nlb_condition or nat_gateway_condition:
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

# Function to check if elastic network interface is in public subnet
def is_in_scope_subnet(eni_subnet):

    subnet_description = ec2_client.describe_subnets(
        SubnetIds=[eni_subnet]
    )

    for subnet in subnet_description['Subnets']:
        for tag in subnet['Tags']:
            if tag['Key'] == os.environ.get('TAG_KEY') and tag['Value'] ==
 os.environ.get('TAG_VALUE'):
                return True
```

```
    return False
```

Déployez des contrôles d'accès préventifs basés sur les attributs pour les sous-réseaux publics

Créée par Joel Alfredo Nunez Gonzalez (AWS) et Samuel Ortega Sancho (AWS)

Récapitulatif

Dans les architectures réseau centralisées, les clouds privés virtuels d'inspection et de périphérie (VPCs) concentrent tout le trafic entrant et sortant, tel que le trafic à destination et en provenance d'Internet. Cela peut toutefois créer des goulots d'étranglement ou entraîner l'atteinte des limites des quotas de service AWS. Le déploiement de la sécurité périphérique du réseau en même temps que les charges de travail qu'il implique VPCs offre une évolutivité sans précédent par rapport à l'approche centralisée plus courante. C'est ce qu'on appelle une architecture de périphérie distribuée.

Bien que le déploiement de sous-réseaux publics dans les comptes de charge de travail puisse présenter des avantages, il présente également de nouveaux risques de sécurité car il augmente la surface d'attaque. Nous vous recommandons de déployer uniquement des ressources Elastic Load Balancing (ELB), telles que des équilibreurs de charge d'application ou des passerelles NAT dans leurs sous-réseaux publics. VPCs L'utilisation d'équilibreurs de charge et de passerelles NAT dans des sous-réseaux publics dédiés vous permet de mettre en œuvre un contrôle précis du trafic entrant et sortant.

Le contrôle d'accès basé sur les attributs (ABAC) consiste à créer des autorisations détaillées basées sur les attributs de l'utilisateur, tels que le département, le rôle du poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC pour AWS. ABAC peut fournir des garde-fous pour les sous-réseaux publics des comptes de charge de travail. Cela permet aux équipes d'application d'être agiles, sans compromettre la sécurité de l'infrastructure.

Ce modèle décrit comment sécuriser les sous-réseaux publics en implémentant l'ABAC par le biais d'une politique de contrôle des services (SCP) dans AWS Organizations et de politiques dans AWS Identity and Access Management (IAM). Vous appliquez le SCP à un compte membre d'une organisation ou à une unité organisationnelle (UO). Ces politiques ABAC permettent aux utilisateurs de déployer des passerelles NAT dans les sous-réseaux cibles et les empêchent de déployer d'autres ressources Amazon Elastic Compute Cloud (Amazon EC2), telles que des EC2 instances et des interfaces réseau élastiques.

Conditions préalables et limitations

Prérequis

- Une organisation dans AWS Organizations
- Accès administratif au compte racine d'AWS Organizations
- Dans l'organisation, un compte de membre actif ou une unité d'organisation pour tester le SCP

Limites

- Le SCP de cette solution n'empêche pas les services AWS qui utilisent un rôle lié à un service de déployer des ressources dans les sous-réseaux cibles. Elastic Load Balancing (ELB), Amazon Elastic Container Service (Amazon ECS) et Amazon Relational Database Service (Amazon RDS) sont des exemples de ces services. Pour plus d'informations, consultez les effets du SCP sur les autorisations dans la documentation d'AWS Organizations. Mettez en œuvre des contrôles de sécurité pour détecter ces exceptions.

Architecture

Pile technologique cible

- SCP appliqué à un compte AWS ou à une unité d'organisation dans AWS Organizations
- Les rôles IAM suivants :
  - `AutomationAdminRole`— Utilisé pour modifier les balises de sous-réseau et créer des ressources VPC après avoir implémenté le SCP
  - `TestAdminRole`— Utilisé pour vérifier si le SCP empêche les autres principaux IAM, y compris ceux disposant d'un accès administratif, d'effectuer les actions réservées au `AutomationAdminRole`

Architecture cible

1. Vous créez le rôle `AutomationAdminRole` IAM dans le compte cible. Ce rôle est autorisé à gérer les ressources réseau. Notez les autorisations suivantes qui sont exclusives à ce rôle :
   - Ce rôle peut créer VPCs des sous-réseaux publics.
   - Ce rôle peut modifier les attributions de balises pour les sous-réseaux cibles.
   - Ce rôle peut gérer ses propres autorisations.
2. Dans AWS Organizations, vous appliquez le SCP au compte ou à l'unité d'organisation AWS cible. Pour un exemple de politique, voir Informations supplémentaires sur ce modèle.

3. Un utilisateur ou un outil du pipeline CI/CD peut assumer le `AutomationAdminRole` rôle d'appliquer la `SubnetType` balise aux sous-réseaux cibles.
4. En assumant d'autres rôles IAM, les responsables IAM autorisés de votre organisation peuvent gérer les passerelles NAT dans les sous-réseaux cibles et les autres ressources réseau autorisées dans le compte AWS, telles que les tables de routage. Utilisez les politiques IAM pour accorder ces autorisations. Pour plus d'informations, consultez Gestion des identités et des accès pour Amazon VPC.

Automatisation et mise à l'échelle

Pour protéger les sous-réseaux publics, les balises AWS correspondantes doivent être appliquées. Une fois le SCP appliqué, les passerelles NAT sont le seul type de EC2 ressource Amazon que les utilisateurs autorisés peuvent créer dans les sous-réseaux dotés de cette balise. `SubnetType:IFA` (`IFA`désigne les actifs connectés à Internet.) Le SCP empêche la création d'autres EC2 ressources Amazon, telles que des instances et des interfaces réseau élastiques. Nous vous recommandons d'utiliser un pipeline CI/CD qui assume le `AutomationAdminRole` rôle de créer des ressources VPC afin que ces balises soient correctement appliquées aux sous-réseaux publics.

Outils

Services AWS

- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Organizations est un service de gestion de comptes qui vous aide à consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée. Dans AWS Organizations, vous pouvez mettre en œuvre des politiques de contrôle des services (SCPs), qui sont un type de politique que vous pouvez utiliser pour gérer les autorisations au sein de votre organisation.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous exploiteriez dans votre propre centre de données, avec les avantages liés à l'utilisation de l'infrastructure évolutive d'AWS.

Épopées

Appliquer le SCP

Tâche	Description	Compétences requises
Créez un rôle d'administrateur de test.	Créez un rôle IAM nommé `TestAdminRole` dans le compte AWS cible. Associez la politique IAM gérée par AdministratorAccessAWS au nouveau rôle. Pour obtenir des instructions, consultez la section Création d'un rôle pour déléguer des autorisations à un utilisateur IAM dans la documentation IAM.	Administrateur AWS
Créez le rôle d'administrateur d'automatisation.	1. Créez un rôle IAM nommé `AutomationAdminRole` dans le compte AWS cible. 2. Associez la politique IAM gérée par AdministratorAccessAWS au nouveau rôle. Voici un exemple de politique de confiance que vous pouvez utiliser pour tester le rôle à partir du `000000000000` compte. `{ "Version": "2012-10-17", "Statement": [`	Administrateur AWS

Tâche	Description	Compétences requises

	{
	"Effect": "Allow",
	"Principal": {
	"AWS": [
	"arn:aws:iam::000000000000:root"
	]
	},
	"Action": "sts:AssumeRole",
	"Condition": {}
	}
	]
	}	

Tâche	Description	Compétences requises
Créez et attachez le SCP.	1. À l'aide de l'exemple de code fourni dans la section Informations supplémentaires, créez une politique de contrôle de sécurité. Pour obtenir des instructions, consultez la section Création d'un SCP dans la documentation d'AWS Organizations. 2. Attachez le SCP au compte AWS ou à l'unité d'organisation cible. Pour obtenir des instructions, consultez la section Attacher et détacher des politiques de contrôle des services dans la documentation d'AWS Organizations.	Administrateur AWS

Testez le SCP

Tâche	Description	Compétences requises
Créez un VPC ou un sous-réseau.	1. Assumez le `TestAdmin Role` rôle dans le compte AWS cible. 2. Essayez de créer un VPC ou un nouveau sous-réseau public dans un VPC existant. Pour obtenir des instructions, consultez la section Créer un VPC, des	Administrateur AWS

Tâche	Description	Compétences requises
	sous-réseaux et d'autres ressources VPC dans la documentation Amazon VPC. Vous ne devriez pas être en mesure de créer ces ressources. 3. Assumez le `AutomationAdminRole` rôle et réessayez de passer à l'étape précédente. Vous devriez maintenant être en mesure de créer les ressources réseau.	

Tâche	Description	Compétences requises
Gérez les tags.	1. Assumez le `TestAdminRole` rôle dans le compte AWS cible. 2. Ajoutez une `SubnetType:IFA` balise à un sous-réseau public disponible. Vous devriez être en mesure d'ajouter cette balise. Pour obtenir des instructions sur la façon d'ajouter des balises via l'interface de ligne de commande AWS (AWS CLI), consultez la section create-tags dans le manuel de référence des commandes de l'AWS CLI. 3. Sans modifier vos informations d'identification, essayez de modifier la `SubnetType:IFA` balise attribuée à ce sous-réseau. Vous ne devriez pas être en mesure de modifier cette balise. 4. Assumez le `AutomationAdminRole` rôle et réessayez les étapes précédentes. Ce rôle doit être en mesure d'ajouter et de modifier cette balise.	Administrateur AWS

Tâche	Description	Compétences requises
Déployez des ressources dans les sous-réseaux cibles.	1. Assumez le `TestAdmin Role` rôle. 2. Pour un sous-réseau public doté de cette `SubnetTyp e:IFA` balise, essayez de créer une EC2 instance. Pour obtenir des instructi ons, consultez la section Lancer une instance dans la EC2 documentation Amazon. Dans ce sous-réseau, vous ne devriez pas être en mesure de créer, de modifier ou de supprimer des EC2 ressources Amazon, à l'exception des passerelles NAT. 3. Dans le même sous-rése au, créez une passerell e NAT. Pour obtenir des instructions, consultez la section Créer une passerell e NAT dans la documenta tion Amazon VPC. Vous devriez être en mesure de créer, de modifier ou de supprimer des passerelles NAT dans ce sous-réseau.	Administrateur AWS

Tâche	Description	Compétences requises
Gérez le AutomationAdminRole rôle.	1. Assumez le `TestAdminRole` rôle. 2. Essayez de modifier le `AutomationAdminRole` rôle. Pour obtenir des instructions, consultez la section Modification d'un rôle dans la documentation IAM. Vous ne devriez pas être en mesure de modifier ce rôle. 3. Assumez le `AutomationAdminRole` rôle et réessayez de passer à l'étape précédente. Vous devriez maintenant être en mesure de modifier le rôle.	Administrateur AWS

Nettoyage

Tâche	Description	Compétences requises
Nettoyez les ressources déployées.	1. Détachez le SCP du compte AWS ou de l'unité d'organisation. Pour obtenir des instructions, consultez la section Détacher un SCP dans la documentation d'AWS Organizations. 2. Supprimez la stratégie de contrôle de service. Pour obtenir des instructions, consultez Supprimer un	Administrateur AWS

Tâche	Description	Compétences requises
	SCP (documentation AWS Organizations). 3. Supprimez le `AutomationAdminRole` rôle et le `TestAdminRole` rôle. Pour obtenir des instructions, consultez la section Suppression de rôles dans la documentation IAM. 4. Supprimez toutes les ressources réseau, telles que VPCs les sous-réseaux, que vous avez créées pour cette solution.	

Ressources connexes

Documentation AWS

- Fixation et détachement SCPs
- Création, mise à jour et suppression SCPs
- Déployez des contrôles d'accès basés sur des attributs de détection pour les sous-réseaux publics à l'aide d'AWS Config
- Contrôles de détection
- Référence d'autorisation de service
- Tagging AWS resources
- Qu'est-ce qu'ABAC pour AWS ?

Références AWS supplémentaires

- Sécurisation des balises de ressources utilisées pour l'autorisation à l'aide d'une politique de contrôle des services dans AWS Organizations (article de blog AWS)

Informations supplémentaires

La politique de contrôle des services suivante est un exemple que vous pouvez utiliser pour tester cette approche dans votre organisation.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyVPCActions",
      "Effect": "Deny",
      "Action": [
        "ec2:CreateVPC",
        "ec2:CreateRoute",
        "ec2:CreateSubnet",
        "ec2:CreateInternetGateway",
        "ec2:DeleteVPC",
        "ec2:DeleteRoute",
        "ec2:DeleteSubnet",
        "ec2:DeleteInternetGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:*"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "AllowNATGWOnIFASubnet",
      "Effect": "Deny",
      "NotAction": [
        "ec2:CreateNatGateway",
        "ec2:DeleteNatGateway"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*"
      ],
      "Condition": {
        "ForAnyValue:StringEqualsIfExists": {
          "aws:ResourceTag/SubnetType": "IFA"
```

```
        },
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "DenyChangesToAdminRole",
      "Effect": "Deny",
      "NotAction": [
        "iam:GetContextKeysForPrincipalPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:ListInstanceProfilesForRole",
        "iam:ListRolePolicies",
        "iam:ListRoleTags"
      ],
      "Resource": [
        "arn:aws:iam::*:role/AutomationAdminRole"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN": ["arn:aws:iam::*:role/AutomationAdminRole"]
        }
      }
    },
    {
      "Sid": "allowbydefault",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Déployez les automatisations de sécurité pour la AWS WAF solution à l'aide de Terraform

Créée par le Dr Rahul Sharad Gaikwad (AWS) et Tamilselvan (AWS)

Récapitulatif

AWS WAF est un pare-feu d'applications Web qui aide à protéger les applications contre les exploits courants en utilisant des règles personnalisables, que vous définissez et déployez dans des listes de contrôle d'accès Web (ACLs). La configuration des AWS WAF règles peut s'avérer difficile, en particulier pour les entreprises qui ne disposent pas d'équipes de sécurité dédiées. Pour simplifier ce processus, Amazon Web Services (AWS) propose la AWS WAF solution Security Automations for, qui déploie automatiquement une seule ACL Web avec un ensemble de AWS WAF règles qui filtrent les attaques Web. Lors du déploiement de Terraform, vous pouvez spécifier les fonctionnalités de protection à inclure. Une fois que vous avez déployé cette solution, AWS WAF inspecte les requêtes Web adressées aux CloudFront distributions Amazon existantes ou aux équilibreurs de charge d'application, et bloque toutes les demandes non conformes aux règles.

La AWS WAF solution Security Automations for peut être déployée AWS CloudFormation conformément aux instructions du guide de mise en AWS WAF œuvre des automatisations de sécurité. Ce modèle fournit une option de déploiement alternative aux entreprises qui utilisent HashiCorp Terraform comme outil d'infrastructure en tant que code (IaC) préféré pour provisionner et gérer leur infrastructure cloud. Lorsque vous déployez cette solution, Terraform applique automatiquement les modifications dans le cloud et déploie et configure les AWS WAF paramètres et les fonctionnalités de protection.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS.
- AWS Command Line Interface (AWS CLI) version 2.4.25 ou ultérieure, installée et configurée avec les autorisations nécessaires. Pour plus d'informations, consultez la section Mise en route (AWS CLI documentation).
- Terraform version 1.1.9 ou ultérieure, installée et configurée. Pour plus d'informations, consultez Installer Terraform (documentation Terraform).

Architecture

Architecture cible

Ce modèle déploie les automatisations de sécurité pour AWS WAF la solution. Pour plus d'informations sur l'architecture cible, consultez la section Présentation de l'architecture dans le guide Security Automations for AWS WAF Implementation. Pour plus d'informations sur les AWS Lambda automatisations de ce déploiement, l'analyseur de journaux d'applications, l'analyseur de AWS WAF journaux, l'analyseur de listes d'adresses IP et le gestionnaire d'accès, consultez la section Détails des composants dans le guide de mise en œuvre des automatisations de sécurité. AWS WAF

Déploiement de Terraform

Lorsque vous exécutez`terraform apply`, Terraform effectue les opérations suivantes :

1. Terraform crée des rôles AWS Identity and Access Management (IAM) et des fonctions Lambda en fonction des entrées du fichier testing.tfvars.
2. Terraform crée des règles AWS WAF ACL et des ensembles d'adresses IP en fonction des entrées du fichier testing.tfvars.
3. Terraform crée les compartiments Amazon Simple Storage Service (Amazon S3), les règles AWS Glue Amazon, les tables de base de données et les groupes de travail EventBridge Amazon Athena en fonction des entrées du fichier testing.tfvars.
4. Terraform déploie la AWS CloudFormation pile pour fournir les ressources personnalisées.
5. Terraform crée les ressources Amazon API Gateway en fonction des entrées fournies par le fichier testing.tfvars.

Automatisation et mise à l'échelle

Vous pouvez utiliser ce modèle pour créer des AWS WAF règles pour plusieurs Comptes AWS et Régions AWS pour déployer les AWS WAF solutions Security Automations for dans l'ensemble de votre AWS Cloud environnement.

Outils

Services AWS

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.

- AWS WAFest un pare-feu d'applications Web qui vous aide à surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources protégées de votre application Web.

Autres services

- Git est un système de contrôle de version distribué et open source.
- HashiCorp Terraform est une application d'interface en ligne de commande qui vous aide à utiliser du code pour provisionner et gérer l'infrastructure et les ressources du cloud.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub AWS WAF Automation Using Terraform.

Bonnes pratiques

- Placez les fichiers statiques dans des compartiments Amazon S3 distincts.
- Évitez de coder des variables en dur.
- Limitez l'utilisation de scripts personnalisés.
- Adoptez une convention de dénomination.

Épopées

Configurez votre poste de travail local

Tâche	Description	Compétences requises
Installez Git.	Suivez les instructions de la section Mise en route (site Web Git) pour installer Git sur votre poste de travail local.	DevOps ingénieur
Pour cloner le référentiel.	Sur votre poste de travail local, entrez la commande suivante pour cloner le dépôt de code :	DevOps ingénieur

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/aws-waf-automation-terraform-samples.git`	
Mettez à jour les variables.	1. Accédez au répertoire cloné en saisissant la commande suivante : `cd terraform-aws-waf-automation` 2. Dans n'importe quel éditeur de texte, ouvrez le fichier testing.tfvars. 3. Mettez à jour les valeurs des variables dans le fichier testing.tfvars. 4. Enregistrez et fermez le fichier .	DevOps ingénieur

Provisionner l'architecture cible à l'aide de Terraform

Tâche	Description	Compétences requises
Initialisez la configuration Terraform.	Entrez la commande suivante pour initialiser votre répertoire de travail qui contient les fichiers de configuration Terraform : `terraform init`	DevOps ingénieur

Tâche	Description	Compétences requises
Prévisualisez le plan Terraform.	Entrez la commande suivante. Terraform évalue les fichiers de configuration pour déterminer l'état cible des ressources déclarées. Il compare ensuite l'état cible à l'état actuel et crée un plan : `terraform plan -var-file ="testing.tfvars"`	DevOps ingénieur
Vérifiez le plan.	Passez en revue le plan et confirmez qu'il configure l'architecture requise dans votre cible Compte AWS.	DevOps ingénieur
Déployez la solution.	1. Entrez la commande suivante pour appliquer le plan : `terraform apply -var-file="testing .tfvars"` 2. Saisissez `yes` pour confirmer. Terraform crée, met à jour ou détruit l'infrast ructure pour atteindre l'état cible déclaré dans les fichiers de configuration. Pour plus d'informations sur la séquence, consultez la section Déploiement de Terraform dans la section Architecture de ce modèle.	DevOps ingénieur

Valider et nettoyer

Tâche	Description	Compétences requises
Vérifiez les modifications.	1. Dans la console Terraform , vérifiez que les sorties correspondent aux résultats attendus. 2. Connectez-vous au AWS Management Console. 3. Vérifiez que les sorties de la console Terraform ont été déployées avec succès dans votre. Compte AWS	DevOps ingénieur
(Facultatif) Nettoyez l'infrast ructure.	Si vous souhaitez supprimer toutes les modifications de ressources et de configuration apportées par cette solution, procédez comme suit : 1. Dans la console Terraform , entrez la commande suivante : `terraform destroy -var-file="testing .tfvars”` 2. Saisissez `yes` pour confirmer.	DevOps ingénieur

Résolution des problèmes

Problème	Solution
`WAFV2 IPSet: WAFOptimisticLockException` Erreur	Si vous recevez cette erreur lorsque vous exécutez la `terraform destroy` commande, vous devez supprimer manuellement les ensembles d'adresses IP. Pour obtenir des instructions, consultez la section Suppression d'un ensemble d'adresses IP (AWS WAF documentation).

Ressources connexes

AWS références

- Guide d'automatisation de la sécurité pour la AWS WAF mise en œuvre
- Automatisations de sécurité pour AWS WAF (bibliothèque de AWS solutions)
- Automatisations de sécurité pour FAQ AWS WAF

Références Terraform

- Configuration du backend Terraform
- Terraform AWS Provider - Documentation et utilisation
- Terraform AWS Provider (référentiel) GitHub

Détectez les instances de base de données Amazon RDS et Aurora dont les certificats CA expirent

Créée par Stephen DiCato (AWS) et Eugene Shifer (AWS)

Récapitulatif

Pour des raisons de sécurité, il est recommandé de chiffrer les données en transit entre les serveurs d'applications et les bases de données relationnelles. Vous pouvez utiliser le protocole SSL ou TLS pour chiffrer une connexion à une instance ou à un cluster de base de données (DB). Ces protocoles contribuent à garantir la confidentialité, l'intégrité et l'authenticité entre une application et une base de données. La base de données utilise un certificat de serveur, délivré par une autorité de certification (CA) et utilisé pour vérifier l'identité du serveur. Le protocole SSL ou TLS vérifie l'authenticité du certificat en validant sa signature numérique et en s'assurant qu'il n'est pas expiré.

Dans le AWS Management Console, Amazon Relational Database Service (Amazon RDS) et Amazon Aurora fournissent des notifications concernant les instances de base de données qui nécessitent des mises à jour de certificats. Toutefois, pour vérifier l'existence de ces notifications, vous devez vous connecter à chacune d'elles Compte AWS et accéder à la console de service correspondante Région AWS. Cette tâche devient plus complexe si vous devez évaluer la validité des certificats dans de nombreuses Comptes AWS entreprises gérées en tant qu'organisation dans AWS Organizations.

En provisionnant l'infrastructure sous forme de code (iAc) fournie dans ce modèle, vous pouvez détecter l'expiration des certificats CA pour toutes les instances de base de données Amazon RDS et Aurora de votre organisation ou de votre Compte AWS organisation. AWS Le AWS CloudFormationmodèle fournit une AWS Config règle, une AWS Lambda fonction et les autorisations nécessaires. Vous pouvez le déployer dans un compte unique sous forme de pile, ou vous pouvez le déployer dans l'ensemble de AWS l'organisation sous forme de stack set.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Si vous effectuez un déploiement en un seul Compte AWS :
  - Vérifiez que vous êtes autorisé à créer des CloudFormation piles.
  - Activez AWS Config dans le compte cible.

  - (Facultatif) Activez AWS Security Hub dans le compte cible.
- Si vous effectuez un déploiement au sein d'une AWS organisation :
  - Assurez-vous que vous êtes autorisé à créer des ensembles de CloudFormation piles.
  - Activez Security Hub grâce à AWS Organizations l'intégration.
  - Activez cette option AWS Config dans les comptes sur lesquels vous déployez cette solution.
  - Désignez un Compte AWS administrateur délégué pour AWS Config Land Security Hub.

Limites

- Si vous effectuez un déploiement sur un compte individuel sur lequel Security Hub n'est pas activé, vous pouvez l'utiliser AWS Config pour évaluer les résultats.
- Si vous effectuez un déploiement dans une organisation qui ne dispose pas d'un administrateur délégué pour AWS Config Security Hub, vous devez vous connecter aux comptes des membres individuels pour consulter les résultats.
- Si vous avez l' AWS Control Tower habitude de gérer et de gouverner les comptes de votre organisation, déployez l'iAc selon ce modèle en utilisant Customizations for AWS Control Tower (CfCT). L'utilisation de la CloudFormation console créera une dérive de AWS Control Tower configuration et vous obligera à réinscrire les unités organisationnelles (OUs) ou les comptes gérés.
- Certains Services AWS ne sont pas disponibles du tout Régions AWS. Pour connaître la disponibilité des régions, consultez la page Points de terminaison et quotas du service, puis cliquez sur le lien du service.

Architecture

Déploiement chez un individu Compte AWS

Le schéma d'architecture suivant montre le déploiement des AWS ressources au sein d'une même architecture Compte AWS. Il est implémenté en utilisant un CloudFormation modèle directement via la CloudFormation console. Si Security Hub est activé, vous pouvez consulter les résultats dans Security Hub AWS Config ou dans Security Hub. Si Security Hub n'est pas activé, vous pouvez afficher les résultats uniquement dans la AWS Config console.

Le schéma montre les étapes suivantes :

1. Vous créez une CloudFormation pile. Cela déploie une fonction Lambda et AWS Config une règle. La règle et la fonction sont configurées avec les autorisations AWS Identity and Access Management (IAM) requises pour publier les évaluations des ressources dans AWS Config et les journaux.
2. La AWS Config règle fonctionne en mode d'évaluation par détection et s'exécute toutes les 24 heures.
3. Security Hub reçoit tous les AWS Config résultats.
4. Vous pouvez consulter les résultats dans Security Hub ou dans AWS Config, selon la configuration du compte.

Déploiement au AWS sein d'une organisation

Le schéma suivant montre l'évaluation de l'expiration des certificats sur plusieurs comptes gérés via AWS Organizations et AWS Control Tower. Vous déployez le CloudFormation modèle via CfCT. Les résultats de l'évaluation sont centralisés dans Security Hub, dans le compte administrateur délégué. Le AWS CodePipeline flux de travail décrit dans le diagramme montre les étapes d'arrière-plan qui se produisent lors du déploiement de CfCT.

Le schéma montre les étapes suivantes :

1. Selon la configuration de CfCT, dans le compte de gestion, vous transférez l'iAC vers un AWS CodeCommit référentiel ou vous chargez un fichier compressé (ZIP) de l'iAc dans un bucket Amazon Simple Storage Service (Amazon S3).
2. Le pipeline CFct décompresse le fichier, exécute les vérifications cfn-nag (GitHub) et le déploie sous forme de stack set. CloudFormation
3. En fonction de la configuration spécifiée dans le fichier manifeste CFct, CloudFormation StackSets déploie les piles dans des comptes individuels ou spécifiées. OUs Cela déploie une fonction Lambda et AWS Config une règle dans les comptes cibles. La règle et la fonction sont configurées avec les autorisations IAM requises pour publier les évaluations des ressources dans AWS Config et les journaux.
4. La AWS Config règle fonctionne en mode d'évaluation par détection et s'exécute toutes les 24 heures.
5. AWS Config transmet tous les résultats à Security Hub.
6. Les résultats du Security Hub sont agrégés dans le compte d'administrateur délégué.
7. Vous pouvez consulter les résultats dans Security Hub dans le compte d'administrateur délégué.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps. Une AWS Config règle définit les paramètres de configuration idéaux pour une ressource et AWS Config permet d'évaluer si vos AWS ressources sont conformes aux conditions de vos règles.
- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques prescriptives. Les personnalisations pour AWS Control Tower (CfCT) vous aident à personnaliser votre zone AWS Control Tower d'atterrissage et à respecter les AWS meilleures pratiques. Les personnalisations sont mises en œuvre à l'aide CloudFormation de modèles et de politiques de contrôle des services (SCPs).
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.

Autres outils

- Python est un langage de programmation informatique polyvalent.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Detect Amazon RDS instances dont les certificats CA expirent.

Bonnes pratiques

Nous vous recommandons de suivre les meilleures pratiques décrites dans les ressources suivantes :

- Bonnes pratiques pour les unités organisationnelles avec AWS Organizations (blog AWS sur les opérations et les migrations dans le cloud)
- Conseils pour établir une base initiale à l'aide de AWS Control Tower on AWS (bibliothèque de AWS solutions)
- Conseils pour créer et modifier AWS Control Tower des ressources (AWS Control Tower documentation)
- Considérations relatives au déploiement du CfCT (AWS Control Tower documentation)

Épopées

Passez en revue la solution et le code

Tâche	Description	Compétences requises
Déterminez votre stratégie de déploiement.	Passez en revue la solution et le code pour déterminer comment vous allez les déployer dans votre AWS environnement. Déterminez si vous comptez effectuer le déploiement dans un seul compte ou dans une AWS organisation.	Propriétaire de l'application, General AWS
Pour cloner le référentiel.	Entrez la commande suivante pour cloner le référentiel de certificats CA Detect Amazon RDS avec expiration. `git clone https://github.com/aws-samp`	Développeur d'applications, propriétaire de l'application

Tâche	Description	Compétences requises
	`les/config-rds-ca-expiry.git`	
Validez la version de Python.	1. Accédez au répertoire de premier niveau du référentiel cloné. `cd config-rds-ca-expiry` 2. Ouvrez le fichier config-rds-ca-expiry.yaml. 3. Dans la `CertExpirationCheckLambdaFunction` ressource, vérifiez que la version de Python est compatible avec votre cible Régions AWS. Par défaut, cette fonction utilise Python 3.12. Pour plus d'informations, consultez la section AWS Lambda Ajout du support pour Python 3.12. Si nécessaire, mettez à jour la version de Python. 4. Enregistrez et fermez le config-rds-ca-expiryfichier .yaml.	Développeur d'applications, propriétaire de l'application

Déployez la solution

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Déployez le CloudFormation modèle dans votre AWS environnement. Effectuez l'une des actions suivantes : • Si vous effectuez un déploiement sur un modèle unique Compte AWS, suivez les instructions de la section Création d'une pile. • Si vous effectuez un déploiement dans une organisation qui n'est pas gérée par AWS Control Tower, suivez les instructi ons de la section Créer un stack set. • Si vous effectuez un déploiement dans une organisation gérée par AWS Control Tower, consultez les instructions de la section Créez vos propres personnalisations.	Développeur d'applications, administrateur AWS, AWS général
Vérifier le déploiement.	Dans la CloudFormation console, vérifiez que la pile ou l'ensemble de piles a été déployé avec succès.	Administrateur AWS, propriéta ire de l'application

Passez en revue les résultats

Tâche	Description	Compétences requises
Consultez les résultats des AWS Config règles.	Dans Security Hub, procédez comme suit pour afficher la liste des résultats individuels : 1. Ouvrez la console Security Hub. 2. Dans le volet de navigation, choisissez Conclusions. 3. Dans la zone Ajouter des filtres, ajoutez les filtres suivants : • Le statut de conformité est `FAILED` • Le titre est `rds-has-expiring-ca` 4. Choisissez Appliquer. Dans Security Hub, procédez comme suit pour afficher la liste des résultats totaux regroupés par Compte AWS : 1. Ouvrez la console Security Hub. 2. Dans le panneau de navigation, choisissez Insights. 3. Choisissez Create insight (Créer une information).	Administrateur AWS, administrateur système AWS, administrateur cloud

Tâche	Description	Compétences requises
	4. Pour sélectionner l'attribut de regroupement pour l'aperçu : a. Choisissez le champ de recherche pour afficher les options de filtre. b. Choisissez Group by (Regrouper par). c. Sélectionnez AwsAccountId. d. Choisissez Appliquer. 5. Dans la zone Ajouter des filtres, ajoutez les filtres suivants : • Le titre est `rds-has-expiring-ca` • Le statut de conformité est `FAILED` 6. Choisissez Create insight (Créer une information). 7. Entrez un nom d'aperçu, puis choisissez Créer un aperçu. Dans AWS Config, pour consulter la liste des résultats, suivez les instructions de la section Affichage des informations de conformité et des résultats d'évaluation de la AWS Config documentation.	

Résolution des problèmes

Problème	Solution
CloudFormation échec de la création ou de la suppression d'un ensemble de piles	Lorsqu'il AWS Control Tower est déployé, il applique les garde-fous nécessaires et assume le contrôle des AWS Config agrégateurs et des règles. Cela inclut la prévention de toute modification directe par le biais de CloudForm ation. Pour déployer ou supprimer correctement ce CloudFormation modèle, y compris toutes les ressources associées, vous devez utiliser CfCT.
CfCT ne parvient pas à supprimer le modèle CloudFormation	Si le CloudFormation modèle persiste même après avoir apporté les modifications nécessaires au fichier manifeste et supprimé les fichiers modèles, vérifiez que le fichier manifeste contient le `enable_stack_set_d eletion` paramètre et que la valeur est définie sur`false`. Pour plus d'informations, consultez Supprimer un ensemble de piles dans la documentation CfCT.

Ressources connexes

- Utilisation du protocole SSL/TLS pour chiffrer une connexion à une instance ou un cluster de base de données (documentation Amazon RDS)
- AWS Config Règles personnalisées (AWS Config documentation)

Générez dynamiquement une politique IAM avec IAM Access Analyzer à l'aide de Step Functions

Créée par Thomas Scott (AWS), Adil El Kanabi (AWS), Koen van Blijderveen (AWS) et Rafal Pawlaszek (AWS)

Récapitulatif

Remarque : n' AWS CodeCommit est plus disponible pour les nouveaux clients. Les clients existants de AWS CodeCommit peuvent continuer à utiliser le service normalement. En savoir plus.

Le principe du moindre privilège est la meilleure pratique de sécurité qui consiste à accorder les autorisations minimales requises pour effectuer une tâche. La mise en œuvre de l'accès avec le moindre privilège dans un compte Amazon Web Services (AWS) déjà actif peut s'avérer difficile, car vous ne voulez pas empêcher involontairement les utilisateurs d'effectuer leurs tâches en modifiant leurs autorisations. Avant de mettre en œuvre des modifications de politique AWS Identity and Access Management (IAM), vous devez comprendre les actions et les ressources effectuées par les utilisateurs du compte.

Ce modèle est conçu pour vous aider à appliquer le principe du moindre privilège d'accès, sans bloquer ni ralentir la productivité de l'équipe. Il décrit comment utiliser IAM Access Analyzer et comment AWS Step Functions générer dynamiquement une politique up-to-date IAM pour votre rôle, en fonction des actions actuellement effectuées dans le compte. La nouvelle politique est conçue pour autoriser l'activité en cours mais supprimer tous les privilèges élevés inutiles. Vous pouvez personnaliser la politique générée en définissant des règles d'autorisation et de refus, et la solution intègre vos règles personnalisées.

Ce modèle inclut des options pour implémenter la solution avec AWS Cloud Development Kit (AWS CDK) ou HashiCorp CDK pour Terraform (CDKTF). Vous pouvez ensuite associer la nouvelle politique au rôle à l'aide d'un pipeline d'intégration et de livraison continues (CI/CD). Si vous disposez d'une architecture multi-comptes, vous pouvez déployer cette solution sur n'importe quel compte sur lequel vous souhaitez générer des politiques IAM mises à jour pour les rôles, renforçant ainsi la sécurité de l'ensemble AWS Cloud de votre environnement.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS avec un AWS CloudTrail trail activé.

- Autorisations IAM pour les éléments suivants :
  - Créez et déployez des flux de travail Step Functions. Pour plus d'informations, consultez Actions, ressources et clés de condition pour AWS Step Functions (documentation Step Functions).
  - Créez des AWS Lambda fonctions. Pour plus d'informations, consultez Rôle d'exécution et autorisations utilisateur (documentation Lambda).
  - Création des rôles IAM. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un utilisateur IAM (documentation IAM).
- npm installé. Pour plus d'informations, consultez Téléchargement et installation de Node.js et de npm (documentation npm).
- Si vous déployez cette solution avec AWS CDK (option 1) :
  - AWS CDK Boîte à outils, installée et configurée. Pour plus d'informations, consultez Installer le AWS CDK (AWS CDK documentation).
- Si vous déployez cette solution avec CDKTF (option 2) :
  - CDKTF, installé et configuré. Pour plus d'informations, consultez Installer le CDK pour Terraform (documentation CDKTF).
  - Terraform, installé et configuré. Pour plus d'informations, consultez Get Started (documentation Terraform).
- AWS Command Line Interface (AWS CLI) installé et configuré localement pour votre Compte AWS. Pour plus d'informations, voir Installation ou mise à jour de la dernière version de AWS CLI (AWS CLI documentation).

Limites

- Ce modèle n'applique pas la nouvelle politique IAM au rôle. À la fin de cette solution, la nouvelle politique IAM est stockée dans un AWS CodeCommit référentiel. Vous pouvez utiliser un pipeline CI/CD pour appliquer des politiques aux rôles de votre compte.

Architecture

Architecture cible

1. Une règle d' EventBridge événement Amazon régulièrement planifiée lance un flux de travail Step Functions. Vous définissez ce programme de régénération dans le cadre de la configuration de cette solution.

2. Dans le flux de travail Step Functions, une fonction Lambda génère les plages de dates à utiliser lors de l'analyse de l'activité du compte dans les CloudTrail journaux.
3. L'étape suivante du flux de travail appelle l'API IAM Access Analyzer pour commencer à générer la politique.
4. À l'aide de l'Amazon Resource Name (ARN) du rôle que vous spécifiez lors de la configuration, IAM Access Analyzer analyse les CloudTrail journaux pour détecter toute activité dans les délais spécifiés. Sur la base de l'activité, IAM Access Analyzer génère une politique IAM qui autorise uniquement les actions et les services utilisés par le rôle pendant la plage de dates spécifiée. Lorsque cette étape est terminée, elle génère un identifiant de tâche.
5. L'étape suivante du flux de travail vérifie l'ID de la tâche toutes les 30 secondes. Lorsque l'ID de tâche est détecté, cette étape utilise l'ID de tâche pour appeler l'API IAM Access Analyzer et récupérer la nouvelle politique IAM. IAM Access Analyzer renvoie la politique sous forme de fichier JSON.
6. L'étape suivante du flux de travail place le <IAM role name>fichier /policy.json dans un compartiment Amazon Simple Storage Service (Amazon S3). Vous définissez ce compartiment S3 dans le cadre de la configuration de cette solution.
7. Une notification d'événement Amazon S3 lance une fonction Lambda.
8. La fonction Lambda extrait la politique du compartiment S3, intègre les règles personnalisées que vous définissez dans les fichiers allow.json et deny.json, puis transmet la politique mise à jour vers. CodeCommit Vous définissez le chemin du CodeCommit référentiel, de la branche et du dossier dans le cadre de la configuration de cette solution.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS CDK Toolkit est un kit de développement cloud en ligne de commande qui vous permet d'interagir avec votre AWS Cloud Development Kit (AWS CDK) application.
- AWS CloudTrailvous aide à auditer la gouvernance, la conformité et le risque opérationnel de votre Compte AWS
- AWS CodeCommitest un service de contrôle de version qui vous permet de stocker et de gérer de manière privée des référentiels Git, sans avoir à gérer votre propre système de contrôle de source.

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser. Ce modèle utilise IAM Access Analyzer, une fonctionnalité d'IAM, pour analyser vos CloudTrail journaux afin d'identifier les actions et les services utilisés par une entité IAM (utilisateur ou rôle), puis de générer une politique IAM basée sur cette activité.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise. Dans ce modèle, vous utilisez les intégrations de services du AWS SDK dans Step Functions pour appeler des actions d'API de service depuis votre flux de travail.

Autres outils

- CDK for Terraform (CDKTF) vous aide à définir l'infrastructure en tant que code (IaC) en utilisant des langages de programmation courants, tels que Python et Typescript.
- Lerna est un système de compilation permettant de gérer et de publier plusieurs TypeScript packages JavaScript ou packages à partir du même référentiel.
- Node.js est un environnement d' JavaScript exécution piloté par les événements conçu pour créer des applications réseau évolutives.
- npm est un registre de logiciels qui s'exécute dans un environnement Node.js et est utilisé pour partager ou emprunter des packages et gérer le déploiement de packages privés.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub Automated IAM Access Analyzer Role Policy Generator.

Épopées

Préparation au déploiement

Tâche	Description	Compétences requises
Clonez le dépôt.	La commande suivante clone le référentiel Automated IAM Access Analyzer Role Policy Generator ()GitHub. `git clone https://github.com/aws-samples/automated-iam-access-analyzer.git`	Développeur d'applications
Installez Lerna.	La commande suivante installe Lerna. `npm i -g lerna`	Développeur d'applications

Configurez les dépendances.	La commande suivante installe les dépendances du référentiel.
	`cd automated-iam-access-analyzer/`
	`npm install && npm run bootstrap`
		Développeur d'applications

Créez le code.	La commande suivante teste, construit et prépare les packages zip des fonctions Lambda.
	`npm run test:code`
	`npm run build:code`
		Développeur d'applications

Tâche	Description	Compétences requises
	`npm run pack:code`	
Construisez les constructions.	La commande suivante crée l'infrastructure en synthétisant les applications, à la fois pour CDKTF AWS CDK et pour CDKTF. `npm run build:infra`	
Configurez toutes les autorisations personnalisées.	Dans le dossier repo du référentiel cloné, modifiez les fichiers allow.json et deny.json pour définir les autorisations personnalisées pour le rôle. Si les fichiers allow.json et deny.json contiennent la même autorisation, l'autorisation de refus est appliquée.	Administrateur AWS, développeur d'applications

Option 1 — Déployez la solution à l'aide de AWS CDK

Tâche	Description	Compétences requises
Déployez la AWS CDK pile.	La commande suivante déploie l'infrastructure via AWS CloudFormation. Définissez les paramètres suivants : • `<NAME_OF_ROLE>` — L'ARN du rôle IAM pour lequel vous créez une nouvelle politique.	Développeur d’applications

Tâche	Description	Compétences requises

	• <TRAIL_ARN> — L'ARN du journal CloudTrail dans lequel l'activité du rôle est stockée.
	• <CRON_EXPRESSION_TO_RUN_SOLUTION> — Expression Cron qui définit le calendrier de régénération de la politique. Le flux de travail Step Functions s'exécute selon ce calendrier.
	• <TRAIL_LOOKBACK> — La période, en jours, pendant laquelle il est nécessaire de revenir sur le parcours lors de l'évaluation des autorisations relatives aux rôles.
	
	`cd infra/cdk`
	`cdk deploy –-parameters roleArn=<NAME_OF_ROLE> \`
	`–-parameters trailArn=<TRAIL_ARN> \`
	`--parameters schedule=<CRON_EXPRESSION_TO_RUN_SOLUTION> \`
	`[ --parameters trailLookBack=<TRAIL_LOOKBACK> ]`	

Tâche	Description	Compétences requises
	Note Les crochets indiquent des paramètres facultatifs.	
(Facultatif) Attendez la nouvelle politique.	Si le journal ne contient pas une quantité raisonnable d'activité historique pour le rôle, attendez de vous assurer que l'activité enregistrée est suffisante pour qu'IAM Access Analyzer puisse générer une politique précise. Si le rôle est actif sur le compte depuis un certain temps, cette période d'attente n'est peut-être pas nécessaire.	Administrateur AWS
Vérifiez manuellement la politique générée.	Dans votre CodeCommit référentiel, passez en revue le <ROLE_ARN>fichier .json généré pour vérifier que les autorisations d'autorisation et de refus sont adaptées au rôle.	Administrateur AWS

Option 2 — Déployer la solution à l'aide de CDKTF

Tâche	Description	Compétences requises
Synthétisez le modèle Terraform.	La commande suivante synthétise le modèle Terraform.	Développeur d’applications

Tâche	Description	Compétences requises
	`lerna exec cdktf synth --scope @aiaa/tfm`	

Tâche	Description	Compétences requises
Déployez le modèle Terraform .	La commande suivante permet d'accéder au répertoire qui contient l'infrastructure définie par CDKTF. `cd infra/cdktf` La commande suivante déploie l'infrastructure dans la cible Compte AWS. Définissez les paramètres suivants : • `<account_ID>` — L'identifiant du compte cible. • `<region>`- La cible Région AWS. • `<selected_role_ARN>` — L'ARN du rôle IAM pour lequel vous créez une nouvelle politique. • `<trail_ARN>` — L'ARN du journal CloudTrail dans lequel l'activité du rôle est stockée. • `<schedule_expression>` — Expression Cron qui définit le calendrier de régénération de la politique . Le flux de travail Step Functions s'exécute selon ce calendrier. • `<trail_look_back>` — La période, en jours, pendant laquelle il est	Développeur d’applications

Tâche	Description	Compétences requises
	nécessaire de revenir sur le parcours lors de l'évaluation des autorisations relatives aux rôles. `TF_VAR_accountId=<account_ID> \ TF_VAR_region=<region> \ TF_VAR_roleArns=<selected_role_ARN> \ TF_VAR_trailArn=<trail_ARN> \ TF_VAR_schedule=<schedule_expression> \ [ TF_VAR_trailLookBack=<trail_look_back> ] \ cdktf deploy` **Note** Les crochets indiquent des paramètres facultatifs.	

Tâche	Description	Compétences requises
(Facultatif) Attendez la nouvelle politique.	Si le journal ne contient pas une quantité raisonnable d'activité historique pour le rôle, attendez de vous assurer que l'activité enregistrée est suffisante pour qu'IAM Access Analyzer puisse générer une politique précise. Si le rôle est actif sur le compte depuis un certain temps, cette période d'attente n'est peut-être pas nécessaire.	Administrateur AWS
Vérifiez manuellement la politique générée.	Dans votre CodeCommit référentiel, passez en revue le <ROLE_ARN>fichier .json généré pour vérifier que les autorisations d'autorisation et de refus sont adaptées au rôle.	Administrateur AWS

Ressources connexes

AWS resources

- Points de terminaison et quotas IAM Access Analyzer
- Configuration du AWS CLI
- Commencer à utiliser le AWS CDK
- Autorisations relatives au moindre privilège

Autres ressources

- CDK pour Terraform (site Web de Terraform)

Activez Amazon de GuardDuty manière conditionnelle à l'aide de modèles AWS CloudFormation

Créée par Ram Kandaswamy (AWS)

Récapitulatif

Vous pouvez activer Amazon GuardDuty sur un compte Amazon Web Services (AWS) à l'aide d'un AWS CloudFormation modèle. Par défaut, s' GuardDuty il est déjà activé lorsque vous essayez de l' CloudFormation activer, le déploiement de la pile échoue. Toutefois, vous pouvez utiliser les conditions de votre CloudFormation modèle pour vérifier s'il GuardDuty est déjà activé. CloudFormation prend en charge l'utilisation de conditions qui comparent des valeurs statiques ; il ne prend pas en charge l'utilisation de la sortie d'une autre propriété de ressource dans le même modèle. Pour plus d'informations, consultez la section Conditions dans la CloudFormation documentation.

Dans ce modèle, vous utilisez une ressource CloudFormation personnalisée soutenue par une AWS Lambda fonction à activer de manière conditionnelle GuardDuty si ce n'est pas déjà fait. Si cette option GuardDuty est activée, la pile capture le statut et l'enregistre dans la section de sortie de la pile. S'il n' GuardDuty est pas activé, la pile l'active.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Rôle AWS Identity and Access Management (IAM) autorisé à créer, mettre à jour et supprimer des piles CloudFormation
- AWS Command Line Interface (AWS CLI), installé et configuré

Limites

S'il GuardDuty a été désactivé manuellement pour un Compte AWS ou Région AWS, ce modèle ne s'active pas GuardDuty pour ce compte ou cette région cible.

Architecture

Pile technologique cible

Le modèle est utilisé CloudFormation pour l'infrastructure en tant que code (IaC). Vous utilisez une ressource CloudFormation personnalisée soutenue par une fonction Lambda pour obtenir la fonctionnalité d'activation dynamique des services.

Architecture cible

Le schéma d'architecture de haut niveau suivant montre le processus d'activation GuardDuty par le déploiement d'un CloudFormation modèle :

1. Vous déployez un CloudFormation modèle pour créer une CloudFormation pile.
2. La pile crée un rôle IAM et une fonction Lambda.
3. La fonction Lambda assume le rôle IAM.
4. Si GuardDuty ce n'est pas déjà le cas sur la cible Compte AWS, la fonction Lambda l'active.

Automatisation et mise à l'échelle

Vous pouvez utiliser cette AWS CloudFormation StackSet fonctionnalité pour étendre cette solution à plusieurs Comptes AWS et Régions AWS. Pour plus d'informations, consultez la section Travailler avec AWS CloudFormation StackSets dans la CloudFormation documentation.

Outils

- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les journaux afin d'identifier les activités inattendues et potentiellement non autorisées dans votre AWS environnement.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos AWS ressources en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

Épopées

Création du CloudFormation modèle et déploiement de la pile

Tâche	Description	Compétences requises
Créez le CloudFormation modèle.	1. Copiez le code dans le CloudFormation modèle dans la section Informations supplémentaires. 2. Collez le code dans un éditeur de texte. 3. Enregistrez le fichier `sample.yaml` sur votre poste de travail.	AWS DevOps
Créez la CloudFormation pile.	1. Dans le AWS CLI, entrez la commande suivante. Cela crée une nouvelle CloudFormation pile à l'aide du `sample.yaml` fichier. Pour plus d'informations, consultez la section Création d'une pile dans la CloudFormation documentation. `aws cloudformation create-stack \ --stack-name guardduty-cf-stack \ --template-body file://sample.yaml` 2. Vérifiez que la valeur suivante apparaît dans le AWS CLI, indiquant que la pile a été créée avec	AWS DevOps

Tâche	Description	Compétences requises
	succès. Le temps nécessaire à la création de la pile peut varier. `"StackStatus": "CREATE_COMPLETE",`	
Validez que cette option GuardDuty est activée pour le Compte AWS.	1. Connectez-vous à la GuardDuty console AWS Management Console et ouvrez-la. 2. Vérifiez que le GuardDuty service est activé.	Administrateur du cloud, administrateur AWS
Configurez des comptes ou des régions supplémentaires.	Selon les besoins de votre cas d'utilisation, utilisez cette CloudFormation StackSet fonctionnalité pour étendre cette solution à plusieurs Comptes AWS et Régions AWS. Pour plus d'informations, consultez la section Travailler avec AWS CloudFormation StackSets dans la CloudFormation documentation.	Administrateur du cloud, administrateur AWS

Ressources connexes

Références

- AWS CloudFormation documentation
- AWS Lambda référence de type de ressource
- CloudFormation type de ressource : :IAM AWS : :Role

- CloudFormation type de ressource : AWS : GuardDuty : :Detector
- Quatre façons de récupérer n'importe quelle propriété AWS de service en utilisant AWS CloudFormation (article de blog)

Tutoriels et vidéos

- Simplifiez la gestion de votre infrastructure à l'aide de AWS CloudFormation(didacticiel)
- Utilisez Amazon GuardDuty AWS Security Hub pour sécuriser plusieurs comptes (AWS re:Invent 2020)
- Bonnes pratiques en matière de création AWS CloudFormation (AWS re:Invent 2019)
- Détection des menaces sur AWS : présentation d'Amazon GuardDuty (AWS Re:InForce 2019)

Informations supplémentaires

CloudFormation modèle

```
AWSTemplateFormatVersion: 2010-09-09
Resources:
  rLambdaLogGroup:
    Type: 'AWS::Logs::LogGroup'
    DeletionPolicy: Delete
    Properties:
      RetentionInDays: 7
      LogGroupName: /aws/lambda/resource-checker
  rLambdaCheckerLambdaRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Sub 'resource-checker-lambda-role-${AWS::Region}'
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: lambda.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: /
      Policies:
        - PolicyName: !Sub 'resource-checker-lambda-policy-${AWS::Region}'
          PolicyDocument:
            Version: 2012-10-17
```

```
            Statement:
              - Sid: CreateLogGroup
                Effect: Allow
                Action:
                  - 'logs:CreateLogGroup'
                  - 'logs:CreateLogStream'
                  - 'logs:PutLogEvents'
                  - 'iam:CreateServiceLinkedRole'
                  - 'cloudformation:CreateStack'
                  - 'cloudformation:DeleteStack'
                  - 'cloudformation:Desc*'
                  - 'guardduty:CreateDetector'
                  - 'guardduty:ListDetectors'
                  - 'guardduty:DeleteDetector'
                Resource: '*'
  resourceCheckerLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Description: Checks for resource type enabled and possibly name to exist
      FunctionName: resource-checker
      Handler: index.lambda_handler
      Role: !GetAtt
        - rLambdaCheckerLambdaRole
        - Arn
      Runtime: python3.13
      MemorySize: 128
      Timeout: 180
      Code:
        ZipFile: |
          import boto3
          import os
          import json
          from botocore.exceptions import ClientError
          import cfnresponse


          guardduty=boto3.client('guardduty')
          cfn=boto3.client('cloudformation')


          def lambda_handler(event, context):
              print('Event: ', event)
              if 'RequestType' in event:
                if event['RequestType'] in ["Create","Update"]:
```

```
                    enabled=False
                    try:
                      response=guardduty.list_detectors()
                      if "DetectorIds" in response and len(response["DetectorIds"])>0:
                        enabled="AlreadyEnabled"
                      elif "DetectorIds" in response and
 len(response["DetectorIds"])==0:
                        cfn_response=cfn.create_stack(
                          StackName='guardduty-cfn-stack',
                          TemplateBody='{ "AWSTemplateFormatVersion": "2010-09-09",
 "Description": "A sample template",    "Resources": { "IRWorkshopGuardDutyDetector": {
  "Type": "AWS::GuardDuty::Detector",    "Properties": {   "Enable": true  }   } } }'
                          )
                        enabled="True"
                    except Exception as e:
                        print("Exception: ",e)
                    responseData = {}
                    responseData['status'] = enabled
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
 "CustomResourcePhysicalID" )
                elif event['RequestType'] == "Delete":
                    cfn_response=cfn.delete_stack(
                            StackName='guardduty-cfn-stack')
                    cfnresponse.send(event, context, cfnresponse.SUCCESS, {})
  CheckResourceExist:
    Type: 'Custom::LambdaCustomResource'
    Properties:
      ServiceToken: !GetAtt
        - resourceCheckerLambda
        - Arn
Outputs:
  status:
    Value: !GetAtt
      - CheckResourceExist
      - status
```

Option de code alternative pour la ressource Lambda

Le CloudFormation modèle fourni utilise un code en ligne pour référencer la ressource Lambda, afin de faciliter les références et les conseils. Vous pouvez également placer le code Lambda dans un bucket Amazon Simple Storage Service (Amazon S3) et le référencer dans le modèle. CloudFormation Le code intégré ne prend pas en charge les dépendances de packages ni les

bibliothèques. Vous pouvez les prendre en charge en plaçant le code Lambda dans un compartiment Amazon S3 et en le référençant dans le modèle. CloudFormation

Remplacez les lignes de code suivantes :

```
Code:
         ZipFile: |
```

avec les lignes de code suivantes :

```
Code:
      S3Bucket: <bucket name>
      S3Key: <python file name>
      S3ObjectVersion: <version>
```

La `S3ObjectVersion` propriété peut être omise si vous n'utilisez pas le versionnement dans votre compartiment Amazon S3. Pour plus d'informations, consultez la section Utilisation du versionnement dans les compartiments Amazon S3 dans la documentation Amazon S3.

Activez le chiffrement transparent des données dans Amazon RDS for SQL Server

Créée par Ranga Cherukuri (AWS)

Récapitulatif

Ce modèle décrit comment implémenter le chiffrement transparent des données (TDE) dans Amazon Relational Database Service (Amazon RDS) pour SQL Server afin de chiffrer les données au repos.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Une instance de base de données Amazon RDS pour SQL Server

Versions du produit

Amazon RDS prend actuellement en charge le TDE pour les versions et éditions de SQL Server suivantes :

- SQL Server 2016 Enterprise Edition
- SQL Server 2017 Enterprise Edition
- SQL Server 2019 Standard Edition et Enterprise Edition
- Éditions Standard et Enterprise de SQL Server 2022

Pour obtenir les dernières informations sur les versions et éditions prises en charge, consultez Support for Transparent Data Encryption in SQL Server dans la documentation Amazon RDS.

Architecture

Pile technologique

- Amazon RDS for SQL Server

Architecture

Outils

- Microsoft SQL Server Management Studio (SSMS) est un environnement intégré permettant de gérer une infrastructure SQL Server. Il fournit une interface utilisateur et un groupe d'outils dotés d'éditeurs de script riches qui interagissent avec SQL Server.

Épopées

Création d'un groupe d'options dans la console Amazon RDS

Tâche	Description	Compétences requises
Ouvrez la console Amazon RDS.	Connectez-vous à l'AWS Management Console et ouvrez la console Amazon RDS.	Développeur, DBA
Créez un groupe d'options.	Dans le volet de navigation, choisissez Groupes d'options , puis Créer un groupe. Choisissez sqlserver-ee comme moteur de base de données, puis sélectionnez la version du moteur.	Développeur, DBA
Ajoutez l'option TRANSPARENT_DATA_ENCRYPTION.	Modifiez le groupe d'options que vous avez créé et ajoutez l'option appeléeTRANSPARENT_DATA_ENCRYPTION .	Développeur, DBA

Associer un groupe d'options à une instance de base de données

Tâche	Description	Compétences requises
Choisissez l'instance de base de données.	Dans la console Amazon RDS, dans le volet de navigation, choisissez Databases, puis choisissez l'instance de base de données que vous souhaitez associer au groupe d'options.	Développeur, DBA
Associez l'instance de base de données au groupe d'options.	Choisissez Modifier, puis utilisez le paramètre du groupe d'options pour associer l'instance de base de données SQL Server au groupe d'options que vous avez créé précédemment.	Développeur, DBA
Appliquez les modifications.	Appliquez les modifications immédiatement ou lors de la fenêtre de maintenance suivante, selon vos besoins.	Développeur, DBA

Obtenez le nom du certificat.	Obtenez le nom du certificat par défaut à l'aide de la requête suivante.
	`USE [master]`
	`GO`
	`SELECT name FROM sys.certificates WHERE name LIKE 'RDSTDECertificate%'`
	`GO`
		Développeur, DBA

Création de la clé de chiffrement de la base de données

Tâche	Description	Compétences requises
Connectez-vous à l'instance de base de données Amazon RDS for SQL Server à l'aide de SSMS.	Pour obtenir des instructions, consultez la section Utilisation de SSMS dans la documentation Microsoft.	Développeur, DBA

Créez la clé de chiffrement de base de données à l'aide du certificat par défaut.	Créez une clé de chiffrement de base de données en utilisant le nom de certificat par défaut que vous avez obtenu précédemment. Utilisez la requête T-SQL suivante pour créer une clé de chiffrement de base de données. Vous pouvez spécifier l'algorithme AES_256 au lieu de l'algorithme AES_128.
	`USE [Databasename]`
	`GO`
	`CREATE DATABASE ENCRYPTION KEY`
	`WITH ALGORITHM = AES_128`
	`ENCRYPTION BY SERVER CERTIFICATE [certificatename]`
	`GO`
		Développeur, DBA

Activez le chiffrement sur la base de données.	Utilisez la requête T-SQL suivante pour activer le chiffrement de base de données. `ALTER DATABASE [Database Name]`	Développeur, DBA

Tâche	Description	Compétences requises
	`SET ENCRYPTION ON` `GO`	
Vérifiez l'état du chiffrement.	Utilisez la requête T-SQL suivante pour vérifier l'état du chiffrement. `SELECT DB_NAME(database_id) AS DatabaseName, encryption_state, percent_complete FROM sys.dm_database_encryption_keys`	Développeur, DBA

Ressources connexes

- Support pour le chiffrement transparent des données dans SQL Server (documentation Amazon RDS)
- Utilisation de groupes d'options (documentation Amazon RDS)
- Modification d'une instance de base de données Amazon RDS (documentation Amazon RDS)
- Chiffrement transparent des données pour SQL Server (documentation Microsoft)
- Utilisation de SSMS (documentation Microsoft)

Assurez-vous que les équilibreurs de charge AWS utilisent des protocoles d'écoute sécurisés (HTTPS, SSL/TLS)

Créée par Chandini Penmetsa (AWS) et Purushotham GK (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), Elastic Load Balancing distribue automatiquement le trafic applicatif entrant sur plusieurs cibles, telles que les instances Amazon Elastic Compute Cloud (Amazon EC2), les conteneurs, les adresses IP et les fonctions AWS Lambda. Les équilibreurs de charge utilisent des écouteurs pour définir les ports et les protocoles utilisés par l'équilibreur de charge pour accepter le trafic provenant des utilisateurs. Les équilibreurs de charge d'application prennent les décisions de routage au niveau de la couche application et utilisent leHTTP/HTTPS protocols. Network Load Balancers make routing decisions at the transport layer and use the Transmission Control Protocol (TCP), Transport Layer Security (TLS), User Datagram Protcol (UDP), or TCP_UDP protocols. Classic Load Balancers make routing decisions at either the transport layer, using TCP or Secure Sockets Layer (SSL) protocols, or at the application layer, using HTTP/HTTPS.

Votre entreprise a peut-être une exigence de sécurité ou de conformité selon laquelle les équilibreurs de charge n'acceptent le trafic provenant des utilisateurs que sur des protocoles sécurisés, tels que HTTPS ou SSL/TLS.

Ce modèle fournit un contrôle de sécurité qui utilise une EventBridge règle Amazon pour surveiller les appels d'`ModifyListener`API pour les équilibreurs de charge d'application `CreateListener` et les équilibreurs de charge réseau, et les appels d'API et d'`CreateLoadBalancer`API pour les `CreateLoadBalancerListeners` équilibreurs de charge classiques. Si HTTP, TCP/UDP ou TCP_UDP est utilisé pour le protocole d'écoute de l'équilibreur de charge, le contrôle invoque une fonction Lambda. La fonction Lambda publie un message dans une rubrique Amazon Simple Notification Service (Amazon SNS) pour envoyer une notification contenant les détails de l'équilibreur de charge.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Adresse e-mail à laquelle vous souhaitez recevoir la notification de violation

- Un bucket Amazon Simple Storage Service (Amazon S3) pour stocker le fichier .zip du code Lambda

Limites

- Ce contrôle de sécurité ne vérifie pas les équilibreurs de charge existants à moins qu'une mise à jour ne soit apportée aux écouteurs des équilibreurs de charge.
- Ce contrôle de sécurité est régional et doit être déployé dans les régions AWS que vous souhaitez surveiller.

Architecture

Pile technologique cible

- fonction Lambda
- Rubrique Amazon SNS
- EventBridge règle

Architecture cible

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez qu'il surveille.

Outils

- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer les ressources AWS en utilisant l'infrastructure sous forme de code.
- Amazon EventBridge — Amazon EventBridge fournit un flux de données en temps réel à partir de vos propres applications, d'applications SaaS (software as a service) et de services AWS, en acheminant ces données vers des cibles telles que les fonctions Lambda.
- AWS Lambda — Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Bonnes pratiques

Assurez-vous que la rubrique SNS utilisée n'est pas accessible au public. Pour plus d'informations, consultez la documentation AWS.

Épopées

Téléchargez le code Lambda

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Votre compartiment S3 doit se trouver dans la même région que l'équilibreur de charge en cours d'évaluation.	Architecte du cloud
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le fichier .zip de code Lambda fourni dans la section « Pièces jointes »	Architecte du cloud

Tâche	Description	Compétences requises
	dans le compartiment S3 défini.	
Déployez le CloudFormation modèle AWS.	Sur la CloudFormation console AWS, dans la même région AWS que le compartiment S3, déployez le modèle fourni dans la section « Pièces jointes ». Dans l'épopée suivante, indiquez les valeurs des paramètres.	Architecte du cloud

CloudFormation paramètres

Tâche	Description	Compétences requises
Nommez le compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud
Indiquez le préfixe Amazon S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,). `<directory>/<file-name>.zip`	Architecte du cloud
Indiquez l'ARN de la rubrique SNS.	Indiquez le sujet Amazon Resource Name (ARN) du SNS si vous souhaitez utiliser un sujet SNS existant pour les notifications de violation . Pour créer une nouvelle rubrique SNS, conservez la	Architecte du cloud

Tâche	Description	Compétences requises
	valeur comme `None` (valeur par défaut).	
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événement s d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Téléchargez le modèle .	Téléchargez le CloudForm ation modèle fourni dans la section Pièces jointes.	Architecte du cloud
Créez la pile.	Dans la même région que le compartiment S3, accédez à la console de CloudFormation service et déployez le modèle téléchargé. Reportez-vous à	Architecte du cloud

Tâche	Description	Compétences requises
	l'épopée précédente pour plus de détails sur les paramètres.	
Vérifiez les ressources.	Une fois la pile complètem ent créée, accédez à l'onglet Ressources et vérifiez les ressources. Le modèle créera les ressources suivantes : • EventBridge règle • fonction Lambda • Rôle d'exécution Lambda • Autorisation d'appel Lambda	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, si une nouvelle rubrique SNS a été créée, un e-mail d'abonnement est envoyé à l'adresse e-mail fournie dans les paramètre s. Vous devez confirmer cet abonnement par e-mail pour recevoir des notifications de violation.	Architecte du cloud

Résolution des problèmes

Problème	Solution
La création de la pile a échoué. Une erreur s'est produite pendant GetObject. Code d'erreur S3 : PermanentRedirect. Message d'erreur S3 : Le compartiment se trouve dans cette région : xx-xxxx-1. Veuillez utiliser cette région pour réessayer la demande.	Assurez-vous que la région du compartiment S3 et la région dans laquelle la pile est déployée sont identiques.
La création de la pile a échoué. Le paramètre d'exécution de python3.6 n'est plus pris en charge pour créer ou mettre à jour des fonctions AWS Lambda.	Mettez à jour le modèle téléchargé à la ligne 186 de la version 3.6 de Python à la version 3.9.

Ressources connexes

- Création d'une pile sur la CloudFormation console AWS
- AWS Lambda
- Qu'est-ce qu'un équilibreur de charge Classic Load Balancer ?
- Qu'est-ce qu'un équilibreur de charge Application Load Balancer ?
- Qu'est-ce qu'un équilibreur de charge Network Load Balancer ?
- Bonnes pratiques d'utilisation des fonctions AWS Lambda
- Bonnes CloudFormation pratiques AWS

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Assurez-vous que le chiffrement des données Amazon EMR au repos est activé au lancement

Créée par Priyanka Chaudhary (AWS)

Récapitulatif

Ce modèle fournit un contrôle de sécurité pour surveiller le chiffrement des clusters Amazon EMR sur Amazon Web Services (AWS).

Le chiffrement des données vous permet d'empêcher les utilisateurs non autorisés de lire les données d'un cluster et celles des systèmes de stockage de données associés. Cela inclut les données susceptibles d'être interceptées lorsqu'elles circulent sur le réseau, appelées données en transit, et les données enregistrées sur un support persistant, appelées données au repos. Les données inactives dans Amazon Simple Storage Service (Amazon S3) peuvent être chiffrées de deux manières.

- Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
- Chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), configurées selon des politiques adaptées à Amazon EMR.

Ce contrôle de sécurité surveille les appels d'API et lance un événement Amazon CloudWatch Events le RunJobFlow. Le déclencheur invoque AWS Lambda, qui exécute un script Python. La fonction extrait l'ID du cluster EMR à partir de l'entrée JSON de l'événement et détermine s'il existe une violation de sécurité en effectuant les vérifications suivantes.

1. Vérifiez si un cluster EMR est associé à une configuration de sécurité spécifique à Amazon EMR.
2. Si une configuration de sécurité spécifique à Amazon EMR est associée au cluster EMR, vérifiez qu'elle Encryption-at-Rest est activée.
3. S'il n' Encryption-at-Restest pas activé, envoyez une notification Amazon Simple Notification Service (Amazon SNS) qui inclut le nom du cluster EMR, les détails de la violation, la région AWS, le compte AWS et le nom de ressource Lambda Amazon (ARN) d'où provient cette notification.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Un compartiment S3 pour le fichier .zip de code Lambda
- Adresse e-mail à laquelle vous souhaitez recevoir la notification de violation
- La journalisation Amazon EMR est désactivée afin que tous les journaux d'API puissent être récupérés

Limites

- Ce contrôle de détection est régional et doit être déployé dans les régions AWS que vous souhaitez surveiller.

Versions du produit

- Amazon EMR version 4.8.0 et versions ultérieures

Architecture

Pile technologique cible

- Amazon EMR
- Événement Amazon CloudWatch Events
- fonction Lambda
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Outils

- AWS CloudFormation est un service qui vous aide à modéliser et à configurer les ressources AWS en utilisant l'infrastructure sous forme de code.
- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux ressources AWS.
- Amazon EMR est une plate-forme de cluster gérée qui simplifie l'exécution des infrastructures de Big Data.
- AWS Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs.
- Amazon S3 est un service de stockage d'objets hautement évolutif qui peut être utilisé pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

- Les fichiers EMREncryption AtRest .zip et EMREncryption AtRest .yml de ce projet sont disponibles sous forme de pièce jointe.

Épopées

Définissez le compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Votre	Architecte du cloud

Tâche	Description	Compétences requises
	compartiment S3 doit se trouver dans la même région que le cluster Amazon EMR en cours d'évaluation.	

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le fichier .zip de code Lambda fourni dans la section « Pièces jointes » dans le compartiment S3 défini.	Architecte du cloud

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle AWS.	Sur la CloudFormation console AWS, dans la même région que votre compartiment S3, déployez le CloudForm ation modèle AWS fourni en pièce jointe à ce modèle. Dans l'épopée suivante, indiquez les valeurs des paramètres. Pour plus d'informations sur le déploiement CloudFormation de modèles AWS, consultez la section « Ressources associées ».	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Nommez le compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud
Fournissez la clé Amazon S3.	<directory><file-name>Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,/.zip).	Architecte du cloud
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. « Info » désigne des messages d'information détaillés sur le déroulement de l'application. Le terme « Erreur » désigne les événements d'erreur susceptibles de permettre à l'application de continuer à fonctionner. Le terme « Avertissement » désigne des situations potentiellement dangereuses.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail fournie. Vous devez confirmer cet abonnement par e-mail pour recevoir des notifications de violation.	Architecte du cloud

Ressources connexes

- Création d'une pile sur la CloudFormation console AWS
- AWS Lambda
- Options de chiffrement Amazon EMR

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Assurez-vous qu'un profil IAM est associé à une instance EC2

Créée par Mansi Suratwala (AWS)

Récapitulatif

Ce modèle fournit un modèle de contrôle de CloudFormation sécurité AWS qui configure une notification automatique lorsqu'une violation du profil AWS Identity and Access Management (IAM) se produit pour une instance Amazon Elastic Compute Cloud (Amazon EC2).

Un profil d'instance est un conteneur pour un rôle IAM que vous pouvez utiliser pour transmettre des informations de rôle à une EC2 instance lorsque celle-ci démarre.

Amazon CloudWatch Events lance cette vérification lorsqu'AWS CloudTrail enregistre les appels d' EC2 API Amazon sur la base des `ReplaceIamInstanceProfileAssociation` actions `RunInstancesAssociateIamInstanceProfile`, et. Le déclencheur appelle une fonction AWS Lambda, qui utilise un événement Amazon CloudWatch Events pour vérifier la présence d'un profil IAM.

Si aucun profil IAM n'existe, la fonction Lambda lance une notification par e-mail Amazon Simple Notification Service (Amazon SNS) qui inclut l'identifiant du compte Amazon Web Services (AWS) et la région AWS.

S'il existe un profil IAM, la fonction Lambda vérifie la présence d'entrées génériques dans les documents de politique. Si les entrées génériques existent, lance une notification de violation Amazon SNS, ce qui vous aide à mettre en œuvre une sécurité renforcée. La notification contient le nom du profil IAM, l'événement, l'ID d' EC2 instance, le nom de la politique gérée, la violation, l'ID du compte et la région.

Conditions préalables et limitations

Prérequis

- Un compte actif
- Un bucket Amazon Simple Storage Service (Amazon S3) pour le fichier .zip de code Lambda

Limites

- Le CloudFormation modèle AWS doit être déployé uniquement pour les `ReplaceIamInstanceProfileAssociation` actions `RunInstancesAssociateIamInstanceProfile`, et.
- Le contrôle de sécurité ne surveille pas le détachement des profils IAM.
- Le contrôle de sécurité ne vérifie pas la modification des politiques IAM associées au profil IAM de l' EC2 instance.
- Le contrôle de sécurité ne prend pas en compte les autorisations au niveau des ressources non prises en charge qui nécessitent l'utilisation de. `"Resource":*`

Architecture

Pile technologique cible

- Amazon EC2
- AWS CloudTrail
- Amazon CloudWatch
- AWS Lambda
- Amazon S3
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Vous pouvez utiliser le CloudFormation modèle AWS à plusieurs reprises pour différents comptes et régions AWS. Vous ne devez lancer le modèle qu'une seule fois pour chaque compte ou région.

Outils

Outils

- Amazon EC2 — Amazon EC2 fournit une capacité de calcul évolutive (serveurs virtuels) dans le cloud AWS.

- AWS CloudTrail — AWS vous CloudTrail aide à activer la gouvernance, la conformité et l'audit opérationnel et des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — AWS Lambda est un service de calcul que vous pouvez utiliser pour exécuter du code sans mettre en service ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon S3 fournit un stockage d'objets hautement évolutif que vous pouvez utiliser pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon SNS permet aux applications et aux appareils d'envoyer et de recevoir des notifications depuis le cloud.

Code

- Un fichier .zip du projet est disponible en pièce jointe.

Épopées

Définissez le compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Pour héberger le fichier .zip de code Lambda, choisissez ou créez un compartiment S3 avec un nom unique qui ne contient pas de barres obliques en tête. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Votre compartiment S3 doit se	Architecte du cloud

Tâche	Description	Compétences requises
	trouver dans la même région que l' EC2 instance en cours d'évaluation.	

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le code Lambda fourni dans la section Pièces jointes dans le compartim ent S3. Le compartiment S3 doit se trouver dans la même région que l' EC2 instance évaluée.	Architecte du cloud

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle AWS.	Déployez le CloudFormation modèle AWS fourni en pièce jointe à ce modèle. Dans l'épopée suivante, indiquez les valeurs des paramètres.	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Nommez le compartiment S3.	Entrez le nom du compartim ent S3 que vous avez créé	Architecte du cloud

Tâche	Description	Compétences requises
	dans le premier épisode épique.	
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,). `<directory>/<file-name>.zip`	Architecte du cloud
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événements d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situations potentiellement dangereuses.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse	Architecte du cloud

Tâche	Description	Compétences requises
	e-mail fournie. Vous devez confirmer cet abonnement par e-mail pour recevoir des notifications de violation.	

Ressources connexes

- Création d'un compartiment S3
- Téléchargement de fichiers dans un compartiment S3
- Utilisation de profils d'instance
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Assurez-vous qu'un cluster Amazon Redshift est chiffré lors de sa création

Créée par Mansi Suratwala (AWS)

Récapitulatif

Ce modèle fournit un CloudFormation modèle AWS qui vous envoie une notification automatique lorsqu'un nouveau cluster Amazon Redshift est créé sans chiffrement.

Le CloudFormation modèle AWS crée un événement Amazon CloudWatch Events et une fonction AWS Lambda. L'événement surveille la création ou la restauration de tout cluster Amazon Redshift à partir d'un instantané via AWS. CloudTrail Si le cluster est créé sans chiffrement AWS Key Management Service (AWS KMS) ou HSM (Cloud Hardware Security Model) dans le compte AWS, CloudWatch lance une fonction Lambda qui vous envoie une notification Amazon Simple Notification Service (Amazon SNS) vous informant de la violation.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un cloud privé virtuel (VPC) avec un groupe de sous-réseaux de clusters et un groupe de sécurité associé.

Limites

- Le CloudFormation modèle AWS ne peut être déployé que pour les `RestoreFromClusterSnapshot` actions `CreateCluster` et.

Architecture

Pile technologique cible

- Amazon Redshift
- AWS CloudTrail
- Amazon CloudWatch

- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Vous pouvez utiliser le CloudFormation modèle AWS à plusieurs reprises pour différents comptes et régions AWS. Vous ne devez l'exécuter qu'une seule fois dans chaque région ou compte.

Outils

Outils

- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données entièrement géré de plusieurs pétaoctets dans le cloud. Amazon Redshift est intégré à votre lac de données, ce qui vous permet d'utiliser vos données pour acquérir de nouvelles informations pour votre entreprise et vos clients.
- AWS CloudTrail — AWS CloudTrail est un service AWS qui vous aide à mettre en œuvre la gouvernance, la conformité et l'audit opérationnel et des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — AWS Lambda prend en charge l'exécution de code sans provisionner ni gérer de serveurs. AWS Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon S3 est un service de stockage d'objets hautement évolutif que vous pouvez utiliser pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon SNS est un service Web qui coordonne et gère la distribution ou l'envoi de messages entre éditeurs et clients, y compris les serveurs Web et les adresses e-mail.

Code

- Un fichier .zip du projet est disponible en pièce jointe.

Épopées

Définissez le compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3. Ce compartiment S3 hébergera le fichier .zip du code Lambda. Votre compartiment S3 doit se trouver dans la même région que le cluster Amazon Redshift en cours d'évaluation. Le nom du compartiment S3 ne peut pas contenir de barres obliques en tête.	Architecte du cloud

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda dans le compartiment S3.	Téléchargez le code Lambda fourni dans la section Pièces jointes dans le compartim ent S3. Le compartiment S3 doit se trouver dans la même région que le cluster Amazon Redshift en cours d'évaluation.	Architecte du cloud

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle AWS.	Déployez le CloudFormation modèle AWS fourni en pièce jointe à ce modèle. Dans l'épopée suivante, indiquez les valeurs des paramètres.	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Nommez le compartiment S3.	Entrez le nom du compartim ent S3 que vous avez créé dans le premier épisode épique.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,). `<directory>/<file-name>.zip`	Architecte du cloud
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événement	Architecte du cloud

Tâche	Description	Compétences requises
	s d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail fournie. Vous devez confirmer cet abonnement par e-mail pour recevoir des notifications de violation.	Architecte du cloud

Ressources connexes

- Création d'un compartiment S3
- Téléchargement de fichiers dans un compartiment S3
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail
- Création d'un cluster Amazon Redshift

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Exportez un rapport sur les identités d'AWS IAM Identity Center et leurs attributions en utilisant PowerShell

Créée par Jorge Pava (AWS), Tchad Miles (AWS), Frank Allotta (AWS) et Manideep Reddy Gillela (AWS)

Récapitulatif

Lorsque vous utilisez AWS IAM Identity Center (successeur d'AWS Single Sign-On) pour gérer de manière centralisée l'accès par authentification unique (SSO) à tous vos comptes Amazon Web Services (AWS) et à vos applications cloud, le reporting et l'audit de ces attributions via l'AWS Management Console peuvent s'avérer fastidieux et chronophages. Cela est particulièrement vrai si vous signalez les autorisations accordées à un utilisateur ou à un groupe sur des dizaines ou des centaines de comptes AWS.

Pour de nombreuses personnes, l'outil idéal pour consulter ces informations serait un tableur tel que Microsoft Excel. Cela peut vous aider à filtrer, rechercher et visualiser les données de l'ensemble de votre organisation, gérées par AWS Organizations.

Ce modèle décrit comment utiliser les outils AWS PowerShell pour générer un rapport sur les configurations d'identité SSO dans IAM Identity Center. Le rapport est formaté sous forme de fichier CSV et inclut le nom de l'identité (principal), le type d'identité (utilisateur ou groupe), les comptes auxquels l'identité peut accéder et les ensembles d'autorisations. Après avoir généré ce rapport, vous pouvez l'ouvrir dans votre application préférée pour rechercher, filtrer et auditer les données selon vos besoins. L'image suivante montre des exemples de données dans un tableur.

> **Important**
>
> Ce rapport contenant des informations sensibles, nous vous recommandons vivement de le stocker en toute sécurité et de ne le partager que sur une need-to-know base limitée.

Conditions préalables et limitations

Prérequis

- IAM Identity Center et AWS Organizations, configurés et activés.
- PowerShell, installé et configuré. Pour plus d'informations, consultez la section Installation PowerShell (documentation Microsoft).
- Outils AWS pour PowerShell, installés et configurés. Pour des raisons de performances, nous vous recommandons vivement d'installer la version modulaire d'AWS Tools for PowerShell, appeléeAWS.Tools. Chaque service AWS est pris en charge par son propre petit module. Dans le PowerShell shell, entrez les commandes suivantes pour installer les modules nécessaires à ce modèle : AWS.Tools.InstallerOrganizations,SSOAdmin, etIdentityStore.

```
Install-Module AWS.Tools.Installer
Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore
```

  Pour plus d'informations, consultez Installer AWS.tools sous Windows ou Installer AWS.tools sous Linux ou macOS (outils AWS pour la documentation). PowerShell Si vous recevez un message d'erreur lors de l'installation des modules, consultez la section Dépannage de ce modèle.
- L'interface de ligne de commande AWS (AWS CLI) ou le SDK AWS doivent être préalablement configurés avec des informations d'identification fonctionnelles en effectuant l'une des opérations suivantes :
  - Utilisez l'interface de ligne de commande AWS `aws configure` Pour plus d'informations, consultez la section Configuration rapide (documentation de l'interface de ligne de commande AWS).
  - Configurez l'AWS CLI ou le AWS Cloud Development Kit (AWS CDK) pour obtenir un accès temporaire via un rôle AWS Identity and Access Management (IAM). Pour plus d'informations, voir Obtenir les informations d'identification du rôle IAM pour l'accès à la CLI (documentation IAM Identity Center).
- Un profil nommé pour la CLI AWS qui a enregistré les informations d'identification d'un principal IAM qui :
  - A accès au compte de gestion AWS Organizations ou au compte d'administrateur délégué pour IAM Identity Center
  - Les politiques gérées par `AWSSSODirectoryReadOnly` AWS `AWSSSOReadOnly` et celles gérées par AWS s'y sont-elles appliquées ?

  Pour plus d'informations, consultez les sections Utilisation de profils nommés (documentation de l'interface de ligne de commande AWS) et politiques gérées par AWS (documentation IAM).

Limites

- Les comptes AWS cibles doivent être gérés en tant qu'organisation dans AWS Organizations.

Versions du produit

- Pour tous les systèmes d'exploitation, il est recommandé d'utiliser PowerShell la version 7.0 ou ultérieure.

Architecture

Architecture cible

1. L'utilisateur exécute le script dans une ligne de PowerShell commande.
2. Le script utilise le profil nommé pour l'AWS CLI. Cela donne accès à IAM Identity Center.
3. Le script récupère les configurations d'identité SSO auprès d'IAM Identity Center.
4. Le script génère un fichier CSV dans le même répertoire sur le poste de travail local où le script est enregistré.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.
- AWS IAM Identity Center vous aide à gérer de manière centralisée l'accès par authentification unique (SSO) à tous vos comptes AWS et applications cloud.
- Les outils AWS pour PowerShell sont un ensemble de PowerShell modules qui vous aident à créer des scripts pour des opérations sur vos ressources AWS à partir de la ligne de PowerShell commande.

Autres outils

- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS.

Épopées

Générer le rapport

Tâche	Description	Compétences requises
Préparez le script.	1. Copiez le PowerShell script dans la section Informations supplémentaires de ce modèle. 2. Dans la `Param` section, pour votre environnement AWS, définissez les valeurs des variables suivantes : • `OutputFile` — Le nom de fichier du rapport. • `ProfileName` — Le profil nommé de la CLI AWS que vous souhaitez utiliser pour générer le rapport. • `Region`— La région AWS dans laquelle le centre d'identité IAM est déployé. Pour une liste complète des régions et de leurs codes, consultez la section Points de terminaison régionaux. 3. Enregistrez le script avec le nom du fichier`SSO-Report.ps1` .	Administrateur du cloud

Tâche	Description	Compétences requises

Exécutez le script.	Il est recommandé d'exécuter votre script personnalisé dans le PowerShell shell à l'aide de la commande suivante.
	`.\SSO-Report.ps1`
	Vous pouvez également exécuter le script depuis un autre shell en saisissant la commande suivante.
	`pwsh .\SSO-Report.ps1`
	Le script génère un fichier CSV dans le même répertoire que le fichier de script.
		Administrateur du cloud

Analysez les données du rapport.	Le fichier CSV de sortie comporte les en-têtes AccountNamePermissionSet, Principal et Type. Ouvrez ce fichier dans votre tableur préféré. Vous pouvez créer une table de données pour filtrer et trier la sortie.	Administrateur du cloud

Résolution des problèmes

Problème	Solution
`The term 'Get-<parameter>' is not recognized as the name of a`	Les outils AWS pour PowerShell ou ses modules ne sont pas installés. Dans le PowerShell shell, entrez les commandes

Problème	Solution

`cmdlet, function, script file, or operable program.`Erreur	suivantes pour installer les outils AWS PowerShell et les modules nécessaires pour ce modèle : `AWS.Tools.Installer Organizations` ,`SSOAdmin`, et`IdentityStore` .
	
	`Install-Module AWS.Tools.Installer`
	`Install-AWSToolsModule -Name Organizations, SSOAdmin, IdentityStore`

`No credentials specified or obtained from persisted/shell defaults`Erreur	Dans Préparer le script dans la section Epics, vérifiez que vous avez correctement saisi les `Region` variables `ProfileName` et. Assurez-vous que les paramètres et les informations d'identification du profil nommé disposent des autorisations suffisantes pour administrer IAM Identity Center.
`Authenticode Issuer …` erreur lors de l'installation des modules AWS.tools	Ajoutez le `-SkipPublisherCheck` paramètre à la fin de la `Install-AWSToolsModule` commande.

Problème	Solution

`Get-ORGAccountList : Assembly AWSSDK.SSO could not be found or loaded.`Erreur	Cette erreur peut se produire lorsque des profils d'interface de ligne de commande AWS nommés sont spécifiés, que l'interface de ligne de commande AWS est configurée pour authentifier les utilisateurs auprès d'IAM Identity Center et que l'interface de ligne de commande AWS est configurée pour récupérer automatiq uement des jetons d'authentification actualisé s. Pour résoudre cette erreur, procédez comme suit :
	1. Entrez la commande suivante pour confirmer que les `SSOOIDC` modules `SSO` et sont installés.
	`Install-AWSToolsModule SSO, SSOOIDC`
	2. Insérez les lignes suivantes dans le script situé sous le `param()` bloc.
	`Import-Module AWS.Tools.SSO`
	`Import-Module AWS.Tools.SSOOIDC`

Ressources connexes

- Où sont stockés les paramètres de configuration ? (documentation de la CLI AWS)
- Configuration de l'interface de ligne de commande AWS pour utiliser AWS IAM Identity Center (documentation de l'interface de ligne de commande AWS)
- Utilisation de profils nommés (documentation de l'AWS CLI)

Informations supplémentaires

Dans le script suivant, déterminez si vous devez mettre à jour les valeurs des paramètres suivants :

- Si vous utilisez un profil nommé dans l'AWS CLI pour accéder au compte dans lequel IAM Identity Center est configuré, mettez à jour la `$ProfileName` valeur.
- Si le centre d'identité IAM est déployé dans une région AWS différente de la région par défaut pour la configuration de votre interface de ligne de commande AWS ou de votre kit SDK AWS, mettez à jour la `$Region` valeur pour utiliser la région dans laquelle le centre d'identité IAM est déployé.
- Si aucune de ces situations ne s'applique, aucune mise à jour du script n'est requise.

```
param (
    # The name of the output CSV file
    [String] $OutputFile  = "SSO-Assignments.csv",
    # The AWS CLI named profile
    [String] $ProfileName = "",
    # The AWS Region in which IAM Identity Center is configured
    [String] $Region      = ""
)
$Start = Get-Date; $OrgParams = @{}
If ($Region){ $OrgParams.Region = $Region}
if ($ProfileName){$OrgParams.ProfileName = $ProfileName}
$SSOParams   = $OrgParams.Clone(); $IdsParams = $OrgParams.Clone()
$AccountList = Get-ORGAccountList @OrgParams | Select-Object Id, Name
$SSOinstance = Get-SSOADMNInstanceList @OrgParams
$SSOParams['InstanceArn']       = $SSOinstance.InstanceArn
$IdsParams['IdentityStoreId']   = $SSOinstance.IdentityStoreId
$PSsets       = @{}; $Principals   = @{}
$Assignments  = @(); $AccountCount = 1; Write-Host ""
foreach ($Account in $AccountList) {
    $Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
    Write-Host "`r$Duration - Account $AccountCount of $($AccountList.Count)
 (Assignments:$($Assignments.Count))        " -NoNewline
    $AccountCount++
    foreach ($PS in Get-SSOADMNPermissionSetsProvisionedToAccountList -AccountId
 $Account.Id @SSOParams) {
        if (-not $PSsets[$PS]) {$PSsets[$PS] = (Get-SSOADMNPermissionSet @SSOParams -
PermissionSetArn $PS).Name;$APICalls++}
        $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id
```

```
        if ($AssignmentsResponse.NextToken) {$AccountAssignments =
 $AssignmentsResponse.AccountAssignments}
        else {$AccountAssignments = $AssignmentsResponse}
        While ($AssignmentsResponse.NextToken) {
            $AssignmentsResponse = Get-SSOADMNAccountAssignmentList @SSOParams -
PermissionSetArn $PS -AccountId $Account.Id -NextToken $AssignmentsResponse.NextToken
            $AccountAssignments += $AssignmentsResponse.AccountAssignments}
        foreach ($Assignment in $AccountAssignments) {
            if (-not $Principals[$Assignment.PrincipalId]) {
                $AssignmentType = $Assignment.PrincipalType.Value
                $Expression     = "Get-IDS"+$AssignmentType+" @IdsParams -"+
$AssignmentType+"Id "+$Assignment.PrincipalId
                $Principal      = Invoke-Expression $Expression
                if ($Assignment.PrincipalType.Value -eq "GROUP")
 { $Principals[$Assignment.PrincipalId] = $Principal.DisplayName }
                else { $Principals[$Assignment.PrincipalId] = $Principal.UserName }
            }
            $Assignments += [PSCustomObject]@{
                AccountName     = $Account.Name
                PermissionSet   = $PSsets[$PS]
                Principal       = $Principals[$Assignment.PrincipalId]
                Type            = $Assignment.PrincipalType.Value}
        }
    }
}
$Duration = New-Timespan -Start $Start -End (Get-Date) | ForEach-Object
 {[Timespan]::New($_.Days, $_.Hours, $_.Minutes, $_.Seconds)}
Write-Host "`r$($AccountList.Count) accounts done in $Duration. Outputting result to
 $OutputFile"
$Assignments | Sort-Object Account | Export-CSV -Path $OutputFile -Force
```

Surveiller et corriger la suppression planifiée des clés AWS KMS

Créée par Mikesh Khanal (AWS) et Ramya Pulipaka (AWS)

Récapitulatif

Sur le cloud Amazon Web Services (AWS), la suppression d'une clé AWS Key Management Services (AWS KMS) peut entraîner une perte de données. La suppression entraîne la suppression du contenu clé et de toutes les métadonnées associées à la clé AWS KMS, et elle est irréversible. Après la suppression d'une clé AWS KMS, vous ne pouvez plus déchiffrer les données chiffrées sous cette clé AWS KMS, de sorte que les données ne peuvent pas être récupérées.

Ce modèle configure la surveillance, avec des notifications lorsqu'une application ou un utilisateur planifie la suppression d'une clé AWS KMS. Si vous recevez une notification, vous souhaiterez peut-être annuler la suppression de la clé AWS KMS et reconsidérer votre décision de la supprimer. Le modèle utilise le manuel d'automatisation d'AWS Systems Manager AWSConfigRemediation-CancelKeyDeletionpour faciliter l'annulation de la suppression d'une clé AWS KMS.

> **Note**
>
> Le modèle du CloudFormation modèle doit être déployé dans toutes les régions AWS où vous souhaitez surveiller la suppression des clés AWS KMS.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Compréhension des services AWS suivants :
  - Amazon EventBridge
  - AWS KMS
  - Amazon Simple Notification Service (Amazon SNS)
  - AWS Systems Manager

Limites

- Toute personnalisation de la solution nécessite une connaissance des CloudFormation modèles AWS et des services AWS utilisés dans ce modèle.
- Actuellement, cette solution utilise le bus d'événements par défaut, et elle peut être personnalisée en fonction des besoins. Pour plus d'informations sur le bus d'événements personnalisé, consultez la documentation AWS.

Architecture

Pile technologique cible

- Amazon EventBridge
- AWS KMS
- Amazon SNS
- AWS Systems Manager
- Automatisation à l'aide des éléments suivants :
  - Interface de ligne de commande AWS (AWS CLI) ou kit SDK AWS
  - CloudFormation pile AWS

Architecture cible

1. La suppression d'une clé AWS KMS est planifiée.
2. L'événement de suppression planifiée est évalué par une règle. EventBridge
3. La EventBridge règle concerne la rubrique Amazon SNS.
4. La EventBridge règle initie l'automatisation et les runbooks de Systems Manager.
5. Les runbooks annulent la suppression.

Automatisation et mise à l'échelle

La CloudFormation pile déploie toutes les ressources et tous les services nécessaires au bon fonctionnement de cette solution. Le modèle peut être exécuté indépendamment dans un seul compte ou exécuté à l'aide d'AWS CloudFormation StackSets pour plusieurs comptes indépendants ou pour une organisation.

```
aws cloudformation create-stack --stack-name  <stack-name>\
```

```
    --template-body file://<Full-Path-of-file> \
    --parameters ParameterKey=,ParameterValue= \
    --capabilities CAPABILITY_NAMED_IAM
```

Outils

Outils

- AWS CloudFormation — AWS CloudFormation est un service qui vous aide à modéliser et à configurer vos ressources Amazon Web Services afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications exécutées sur AWS. Vous pouvez utiliser un CloudFormation modèle pour créer des piles dans un compte AWS dans une région AWS. Le modèle décrit toutes les ressources AWS que vous souhaitez, et CloudFormation fournit et configure ces ressources pour vous.
- AWS CLI — L'interface de ligne de commande AWS (AWS CLI) est un outil open source que vous pouvez utiliser pour interagir avec les services AWS à l'aide de commandes dans votre shell de ligne de commande.
- Amazon EventBridge — Amazon EventBridge est un service de bus d'événements sans serveur qui connecte vos applications à des données provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications et services AWS, et achemine ces données vers des cibles telles qu'AWS Lambda. EventBridge simplifie le processus de création d'architectures pilotées par les événements.
- AWS KMS — AWS Key Management Service (AWS KMS) est un service géré permettant de créer et de contrôler les clés AWS KMS, les clés de chiffrement utilisées pour chiffrer vos données.
- AWS SDKs — Les outils AWS vous SDKs permettent de développer et de gérer des applications sur AWS dans le langage de programmation de votre choix.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages aux abonnés (également appelés producteurs et consommateurs). Les éditeurs communiquent de façon asynchrone avec les abonnés en envoyant un message à une rubrique, qui est un point d'accès logique et un canal de communication.
- AWS Systems Manager — AWS Systems Manager est un service AWS que vous pouvez utiliser pour visualiser et contrôler votre infrastructure sur AWS. À l'aide de la console Systems Manager, vous pouvez automatiser les tâches opérationnelles sur l'ensemble de vos ressources AWS. Systems Manager vous aide à maintenir la sécurité et la conformité en analysant vos Instances gérées et en signalant toute infraction à la politique (ou en prenant des mesures correctives pour y remédier).

Code

- Le `alerting_ct_logs.yaml` CloudFormation modèle du projet est joint.

Épopées

Préparez le compte AWS

Tâche	Description	Compétences requises
Installez et configurez l'AWS CLI.	Installez la version 2 de l'interface de ligne de commande AWS. Configure z ensuite les paramètres des informations d'identification de sécurité pour une identité, le format de sortie par défaut et la région AWS par défaut que l'AWS CLI utilise pour interagir avec AWS. L'identité doit disposer des autorisations requises pour effectuer les tâches.	Développeur, ingénieur en sécurité

Déployer le CloudFormation modèle AWS

Tâche	Description	Compétences requises
Téléchargez le CloudForm ation modèle.	Téléchargez la pièce jointe sur un chemin local sur votre ordinateur et extrayez le fichier `alerting_ct_logs.y aml` modèle.	Développeur, ingénieur en sécurité
Déployez le modèle.	Dans la fenêtre du terminal où le profil du compte AWS	Développeur, ingénieur en sécurité

Tâche	Description	Compétences requises
	a été configuré, exécutez la commande suivante. `aws cloudformation create-stack --stack-name <stack_name> \ --capabilities <Value> \ --template-body file://<Full_Path> \ --parameters ParameterKey=DestinationEmailAddress,ParameterValue=<Value> \ ParameterKey=SNSTopicName,ParameterValue=<Value> \ ParameterKey=EnableRemediation ,ParameterValue=<Value> \ ParameterKey=AutomationAssumeRole, ParameterValue=<Value>` À l'étape suivante, entrez des valeurs pour les paramètres du modèle.	

Tâche	Description	Compétences requises
Complétez les paramètres du modèle.	Entrez les valeurs requises pour les paramètres. • `DestinationEmailAddress` — Adresse e-mail pour recevoir une alerte lorsqu'il est prévu de supprimer une clé AWS KMS. • `SNSTopicName` — Le nom de la rubrique Amazon SNS. • `EnableRemediation` — Annulation de la suppression planifiée des clés à l'aide d'un runbook de Systems Manager. Les valeurs autorisées sont `true` et `false`. • `AutomationAssumeRole` — L'Amazon Resource Name (ARN) du rôle qui permet à Systems Manager Automation d'effectuer les actions en votre nom. Pour plus d'informations, consultez la section Autorisations IAM requises dans la AWSConfigRemediation-CancelKeyDeletiondocumentation. • `Capabilities` — CloudFormation Pour qu'AWS puisse créer la pile, vous devez explicite	Développeur, ingénieur en sécurité

Tâche	Description	Compétences requises
	ment reconnaître que votre modèle de pile contient certaines fonctionnalités.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Vérifiez votre boîte e-mail et choisissez Confirmer l'abonnement dans le message électronique que vous recevez d'Amazon SNS. Une fenêtre de navigateur Web s'ouvre et affiche une confirmation d'abonnement ainsi que votre identifiant d'abonnement.	Développeur, ingénieur en sécurité

Ressources connexes

Références

- Création d'une règle pour un service AWS
- Création d'une CloudWatch alarme Amazon pour détecter l'utilisation d'une clé AWS KMS en attente de suppression

Tutoriels et vidéos

- Comment démarrer avec Amazon EventBridge
- Présentation approfondie d'Amazon EventBridge (AWS Online Tech Talks)

Atelier AWS

- Travailler avec des EventBridge règles

Informations supplémentaires

Le code suivant fournit des exemples d'extension de la solution afin de surveiller et de vous informer de toute modification apportée à un service AWS. Les exemples incluent des modèles prédéfinis et des modèles personnalisés. Pour plus d'informations, consultez la section Événements et modèles d'événements dans EventBridge.

```
EventPattern:
        source:
        - aws.kms
        detail-type:
        - AWS API Call via CloudTrail
        detail:
          eventSource:
          - kms.amazonaws.com
          eventName:
          - ScheduleKeyDeletion
```

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Identifiez les compartiments Amazon S3 publics à l'aide AWS Organizations de Security Hub

Créée par Mourad Cherfaoui (AWS), Arun Chandapillai (AWS) et Parag Nagwekar (AWS)

Récapitulatif

Ce modèle vous montre comment créer un mécanisme permettant d'identifier les compartiments publics Amazon Simple Storage Service (Amazon S3) dans vos comptes. AWS Organizations Le mécanisme fonctionne en utilisant les contrôles de la norme AWS Foundational Security Best Practices (FSBP) AWS Security Hub pour surveiller les buckets Amazon S3. Vous pouvez utiliser Amazon EventBridge pour traiter les résultats du Security Hub, puis les publier sur une rubrique Amazon Simple Notification Service (Amazon SNS). Les parties prenantes de votre organisation peuvent s'abonner au sujet et recevoir des notifications immédiates par e-mail concernant les résultats.

Les nouveaux compartiments Amazon S3 et leurs objets n'autorisent pas l'accès public par défaut. Vous pouvez utiliser ce modèle dans les scénarios où vous devez modifier les configurations par défaut d'Amazon S3 en fonction des exigences de votre organisation. Par exemple, il peut s'agir d'un scénario dans lequel vous avez un compartiment Amazon S3 hébergeant un site Web destiné au public ou des fichiers que tout le monde sur Internet doit pouvoir lire à partir de votre compartiment Amazon S3.

Security Hub est souvent déployé en tant que service central pour consolider tous les résultats de sécurité, y compris ceux liés aux normes de sécurité et aux exigences de conformité. Il en existe d'autres Services AWS que vous pouvez utiliser pour détecter les buckets Amazon S3 publics, mais ce modèle utilise un déploiement de Security Hub existant avec une configuration minimale.

Conditions préalables et limitations

Prérequis

- Une configuration AWS multi-comptes avec un compte administrateur Security Hub dédié
- Security Hub et AWS Config, activé dans le Région AWS système que vous souhaitez surveiller

> **Note**
>
> Vous devez activer l'agrégation entre régions dans Security Hub si vous souhaitez surveiller plusieurs régions à partir d'une seule région d'agrégation.

- Autorisations utilisateur pour accéder au compte administrateur Security Hub et le mettre à jour, accès en lecture à tous les compartiments Amazon S3 de l'organisation et autorisations pour désactiver l'accès public (si nécessaire)

Architecture

Le schéma suivant montre une architecture permettant d'utiliser Security Hub pour identifier les buckets Amazon S3 publics.

Le diagramme montre le flux de travail suivant :

1. Security Hub surveille la configuration des compartiments Amazon S3 dans tous les AWS Organizations comptes (y compris le compte administrateur) à l'aide des contrôles S3.2 et S3.3 de la norme de sécurité FSBP, et détecte si un compartiment est configuré comme public.
2. Le compte administrateur du Security Hub accède aux résultats (y compris ceux des versions 3.2 et 3.3) à partir de tous les comptes membres.
3. Security Hub envoie automatiquement tous les nouveaux résultats et toutes les mises à jour des résultats existants EventBridge sous la forme d'événements Security Hub Findings - Imported. Cela inclut les événements relatifs aux résultats provenant à la fois des comptes administrateur et membre.
4. Une EventBridge règle filtre les résultats des S3.2 et S3.3 qui ont un statut de type « of »`FAILED`, un statut `ComplianceStatus` de flux de travail « de » et un `RecordState` « of `NEW` ». `ACTIVE`
5. Les règles utilisent les modèles d'événements pour identifier les événements et les envoyer à une rubrique Amazon SNS une fois qu'ils correspondent.
6. Une rubrique Amazon SNS envoie les événements à ses abonnés (par e-mail, par exemple).
7. Les analystes de sécurité désignés pour recevoir les notifications par e-mail examinent le compartiment Amazon S3 en question.
8. Si l'accès public au bucket est approuvé, l'analyste de sécurité définit le statut du flux de travail de la découverte correspondante dans Security Hub sur`SUPPRESSED`. Dans le cas contraire,

l'analyste définit le statut surNOTIFIED. Cela élimine les futures notifications pour le compartiment Amazon S3 et réduit le bruit des notifications.

9. Si le statut du flux de travail est défini surNOTIFIED, l'analyste de sécurité examine le résultat avec le propriétaire du bucket afin de déterminer si l'accès public est justifié et conforme aux exigences de confidentialité et de protection des données. L'enquête aboutit soit à la suppression de l'accès public au compartiment, soit à l'approbation de l'accès public. Dans ce dernier cas, l'analyste de sécurité définit le statut du flux de travail surSUPPRESSED.

> **Note**
>
> Le schéma d'architecture s'applique à la fois aux déploiements d'agrégation à région unique et aux déploiements d'agrégation entre régions. Dans les comptes A, B et C du diagramme, Security Hub peut appartenir à la même région que le compte administrateur ou appartenir à des régions différentes si l'agrégation entre régions est activée.

Outils

- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. EventBridge fournit un flux de données en temps réel à partir de vos propres applications, d'applications logicielles en tant que service (SaaS) et Services AWS. EventBridge achemine ces données vers des cibles telles que les rubriques et les AWS Lambda fonctions Amazon SNS si les données répondent aux règles définies par l'utilisateur.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Security Hub vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité. Security Hub collecte des données de sécurité provenant de l'ensemble Comptes AWS des services et des produits partenaires tiers pris en

charge, puis aide à analyser les tendances en matière de sécurité et à identifier les problèmes de sécurité les plus prioritaires.

Épopées

Configuration des comptes Security Hub

Tâche	Description	Compétences requises
Activez Security Hub dans AWS Organizations les comptes.	Pour activer Security Hub dans les comptes d'organisation dans lesquels vous souhaitez surveiller les compartiments Amazon S3, consultez les directives relatives à la désignation d'un compte administrateur Security Hub (console) et à la gestion des comptes de membres appartenant à une organisation dans la documentation du Security Hub.	Administrateur AWS
(Facultatif) Activez l'agrégation entre régions.	Si vous souhaitez surveiller les compartiments Amazon S3 dans plusieurs régions à partir d'une seule région, configurez l'agrégation entre régions.	Administrateur AWS
Activez les contrôles S3.2 et S3.3 pour la norme de sécurité FSBP.	Vous devez activer les contrôles S3.2 et S3.3 pour la norme de sécurité FSBP. 1. Pour activer les contrôles S3.2, suivez les instructions de [S3.2] Les compartim	Administrateur AWS

Tâche	Description	Compétences requises
	ents S3 devraient interdire l'accès public en lecture dans la documentation de Security Hub. 2. Pour activer les contrôles S3.3, suivez les instructi ons de [3] Les compartim ents S3 devraient interdire l'accès public en écriture dans la documentation de Security Hub.	

Configuration de l'environnement

Tâche	Description	Compétences requises
Configurez la rubrique Amazon SNS et l'abonnement par e-mail.	1. Connectez-vous à la console Amazon SNS AWS Management Console et ouvrez-la. 2. Dans le panneau de navigation, choisissez Rubriques, puis Créer une rubrique. 3. Pour Type, choisissez Standard. 4. Dans Nom, entrez le nom de votre sujet (par exemple, public-s3-buckets). 5. Choisissez Créer une rubrique.	Administrateur AWS

Tâche	Description	Compétences requises
	6. Dans l'onglet Abonnements de votre sujet, choisissez Créer un abonnement. 7. Pour Protocol, sélectionnez Email. 8. Pour Endpoint, entrez l'adresse e-mail qui recevra les notifications. Vous pouvez utiliser l'adresse e-mail d'un AWS administrateur, d'un professionnel de l'informatique ou d'un professionnel Infosec. 9. Choisissez Créer un abonnement. Pour créer des abonnements par e-mail supplémentaires, répétez les étapes 6 à 8 selon les besoins.	

Tâche	Description	Compétences requises
Configurez la EventBridge règle.	1. Ouvrez la EventBridge console. 2. Dans la section Commencer, sélectionnez EventBridge Règle, puis choisissez Créer une règle. 3. Sur la page de détail de la règle, dans Nom, entrez le nom de votre règle (par exemple, public-s3 -buckets). Choisissez Suivant. 4. Dans la section Modèle d'événement, choisissez Modifier le modèle. 5. Copiez le code suivant, collez-le dans l'éditeur de code de modèle d'événement, puis choisissez Next. `{ "source": ["aws.securityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Compliance": { "Status": ["FAILED"] }, "RecordState": ["ACTIVE"], "Workflow": {`	Administrateur AWS

Tâche	Description	Compétences requises
	<pre>"Status": ["NEW"] }, "ProductFields": { "ControlId": ["S3.2", "S3.3"] } } }</pre> 6. Sur la page Sélectionner une ou plusieurs cibles, pour Sélectionner une cible, sélectionnez le sujet SNS comme cible, puis sélectionnez le sujet que vous avez créé précédemment. 7. Choisissez Suivant, sélectionnez à nouveau Suivant, puis choisissez Créer une règle.	

Résolution des problèmes

Problème	Solution
J'ai un compartiment Amazon S3 dont l'accès public est activé, mais je ne reçois pas de notifications par e-mail à ce sujet.	Cela peut être dû au fait que le bucket a été créé dans une autre région et que l'agrégation entre régions n'est pas activée dans le compte administrateur du Security Hub. Pour résoudre ce problème, activez l'agrégation entre régions ou implémentez la solution de ce modèle dans la région où réside actuellement votre compartiment Amazon S3.

Ressources connexes

- Qu'est-ce que c'est AWS Security Hub ? (documentation du Security Hub)
- AWS Norme FSBP (Foundational Security Best Practices) (documentation Security Hub)
- AWS Security Hub scripts d'activation multi-comptes (AWS Labs)
- Bonnes pratiques de sécurité pour Amazon S3 (documentation Amazon S3)

Informations supplémentaires

Flux de travail pour la surveillance des buckets Amazon S3 publics

Le flux de travail suivant illustre la manière dont vous pouvez surveiller les compartiments Amazon S3 publics au sein de votre organisation. Le flux de travail suppose que vous avez suivi les étapes décrites dans la rubrique Configurer l'Amazon SNS et dans l'article sur l'abonnement par e-mail à propos de ce modèle.

1. Vous recevez une notification par e-mail lorsqu'un compartiment Amazon S3 est configuré avec un accès public.
   - Si l'accès public au bucket est approuvé, définissez le statut du flux de travail de la découverte correspondante sur le compte administrateur du Security Hub. `SUPPRESSED` Cela empêche Security Hub d'émettre d'autres notifications pour ce compartiment et peut éliminer les alertes dupliquées.
   - Si l'accès public au bucket n'est pas approuvé, définissez le statut du flux de travail de la recherche correspondante dans le compte administrateur du Security Hub sur`NOTIFIED`. Cela empêche Security Hub d'émettre d'autres notifications pour ce compartiment depuis Security Hub et peut éliminer le bruit.
2. Si le compartiment peut contenir des données sensibles, désactivez immédiatement l'accès public jusqu'à ce que la révision soit terminée. Si vous désactivez l'accès public, Security Hub change le statut du flux de travail en`RESOLVED`. Ensuite, des notifications par e-mail pour le bucket stop.
3. Recherchez l'utilisateur qui a configuré le bucket comme public (par exemple, en utilisant AWS CloudTrail) et lancez une révision. L'examen aboutit soit à la suppression de l'accès public au compartiment, soit à l'approbation de l'accès public. Si l'accès public est approuvé, définissez le statut du flux de travail du résultat correspondant sur`SUPPRESSED`.

Ingérez et analysez les journaux de sécurité AWS dans Microsoft Sentinel

Créée par Ivan Girardi (AWS) et Sebastian Wenzel (AWS)

Récapitulatif

Ce modèle décrit comment automatiser l'ingestion des journaux de AWS sécurité, tels que les journaux, AWS CloudTrail les données Amazon Logs, CloudWatch les données Amazon VPC Flow Logs et les GuardDuty résultats d'Amazon, dans Microsoft Sentinel. Si votre entreprise utilise Microsoft Sentinel comme système de gestion des informations et des événements de sécurité (SIEM), cela vous permet de surveiller et d'analyser les journaux de manière centralisée afin de détecter les événements liés à la sécurité. Dès que les journaux sont disponibles, ils sont automatiquement envoyés dans un compartiment Amazon Simple Storage Service (Amazon S3) en moins de 5 minutes. Cela peut vous aider à détecter rapidement les événements de sécurité dans votre AWS environnement.

Microsoft Sentinel ingère CloudTrail les journaux dans un format tabulaire qui inclut l'horodatage d'origine de l'enregistrement de l'événement. La structure des journaux ingérés permet des fonctionnalités de requête en utilisant le langage de requête Kusto dans Microsoft Sentinel.

Le schéma déploie une solution de surveillance et d'alerte qui détecte les défaillances d'ingestion en moins d'une minute. Il inclut également un système de notification que le SIEM externe peut surveiller. Vous utilisez AWS CloudFormation pour déployer les ressources requises dans le compte de journalisation.

Public cible

Ce modèle est recommandé aux utilisateurs expérimentés avec AWS Control Tower, AWS Organizations CloudFormation, AWS Identity and Access Management (IAM) et AWS Key Management Service (AWS KMS).

Conditions préalables et limitations

Prérequis

Les conditions préalables au déploiement de cette solution sont les suivantes :

- Comptes AWS Actifs gérés en tant qu'organisation dans une zone d'atterrissage AWS Organizations et faisant partie d'une zone AWS Control Tower d'atterrissage. L'organisation doit

inclure un compte dédié pour la journalisation. Pour obtenir des instructions, consultez la section Création et configuration d'une organisation dans la AWS Organizations documentation.

- Un CloudTrail journal qui enregistre les événements pour l'ensemble de l'organisation et stocke les journaux dans un compartiment Amazon S3 du compte de journalisation. Pour obtenir des instructions, consultez la section Création d'un suivi pour une organisation.
- Dans le compte de journalisation, autorisations permettant d'assumer un rôle IAM existant doté des autorisations suivantes :
  - Déployez les ressources définies dans le CloudFormation modèle fourni.
  - Déployez le CloudFormation modèle fourni.
  - Modifiez la politique en matière de AWS KMS clés si les journaux sont chiffrés à l'aide d'une clé gérée par le client.
- AWS Command Line Interface (AWS CLI), installé et configuré.
- Un compte Microsoft Azure avec un abonnement pour utiliser Microsoft Sentinel.
- Activez et configurez Microsoft Sentinel. Pour obtenir des instructions, consultez la section Activer Microsoft Sentinel ainsi que les fonctionnalités et le contenu initiaux de la documentation Microsoft Sentinel.
- Répondez aux conditions requises pour configurer le connecteur Microsoft Sentinel S3.

Limites

- Cette solution transmet les journaux de sécurité d'un compartiment Amazon S3 du compte de journalisation à Microsoft Sentinel. Les instructions relatives à l'envoi des journaux à Amazon S3 ne sont pas explicitement fournies.
- Ce modèle fournit des instructions pour le déploiement dans une zone AWS Control Tower d'atterrissage. Cependant, l'utilisation de n' AWS Control Tower est pas obligatoire.
- Cette solution est compatible avec un environnement dans lequel le compartiment de journalisation Amazon S3 est limité par des politiques de contrôle des services (SCPs), telles que Interdire les modifications apportées à la politique de compartiment pour les compartiments Amazon S3 AWS Control Tower créés dans Log Archive.
- Ce modèle fournit des instructions pour le transfert CloudTrail des journaux, mais vous pouvez adapter cette solution pour envoyer d'autres journaux pris en charge par Microsoft Sentinel, tels que les CloudWatch journaux provenant de Logs, Amazon VPC Flow Logs et. GuardDuty
- Les instructions utilisent le AWS CLI pour déployer le CloudFormation modèle, mais vous pouvez également utiliser le AWS Management Console. Pour obtenir des instructions, consultez la section

Utilisation de la AWS CloudFormation console. Si vous utilisez la console pour déployer la pile, déployez-la au même endroit Région AWS que le bucket de journalisation.

- Cette solution déploie une file d'attente Amazon Simple Queue Service (Amazon SQS) pour envoyer les notifications Amazon S3. La file d'attente contient des messages indiquant les chemins des objets chargés dans le compartiment Amazon S3, et non des données réelles. La file d'attente utilise le chiffrement SSE-SQS pour protéger le contenu des messages. Si vous souhaitez chiffrer la file d'attente SQS avec SSE-KMS, vous pouvez utiliser une clé KMS gérée par le client. Pour plus d'informations, consultez la section Chiffrement au repos dans Amazon SQS.

Architecture

Cette section fournit une vue d'ensemble de haut niveau de l'architecture établie par l'exemple de code. Le schéma suivant montre les ressources déployées dans le compte de journalisation afin d'ingérer les journaux d'un compartiment Amazon S3 existant dans Microsoft Sentinel.

Le schéma d'architecture montre les interactions entre les ressources suivantes :

1. Dans le compte de journalisation, Microsoft Sentinel assume un rôle IAM via OpenID Connect (OIDC) pour accéder aux journaux d'un compartiment Amazon S3 et d'une file d'attente Amazon SQS spécifiques.
2. Amazon Simple Notification Service (Amazon SNS) et Amazon S3 AWS KMS sont utilisés pour le chiffrement.
3. Amazon S3 envoie des messages de notification à la file d'attente Amazon SQS chaque fois qu'il reçoit de nouveaux journaux.
4. Microsoft Sentinel vérifie la présence de nouveaux messages sur Amazon SQS. La file d'attente Amazon SQS utilise le chiffrement SSE-SQS. La période de conservation des messages est fixée à 14 jours.
5. Microsoft Sentinel extrait les messages de la file d'attente Amazon SQS. Les messages contiennent le chemin des objets Amazon S3 chargés. Microsoft Sentinel ingère ces objets du compartiment Amazon S3 dans le compte Microsoft Azure.
6. Une CloudWatch alarme surveille la file d'attente Amazon SQS. Si aucun message n'est reçu et est supprimé de la file d'attente Amazon SQS dans les 5 minutes, une notification Amazon SNS est envoyée par e-mail.

AWS Control Tower vous aide à configurer la structure de l'unité organisationnelle (UO) de base et centralise les CloudTrail journaux dans le compte de journalisation. Il implémente également SCPs l'obligation de protéger le bucket de journalisation.

Nous avons fourni l'architecture cible dans une zone AWS Control Tower d'atterrissage, mais cela n'est pas strictement obligatoire. Dans ce diagramme, les ressources du compte de gestion reflètent un AWS Control Tower déploiement et un suivi qui CloudTrail enregistre les événements pour l'ensemble de l'organisation.

Ce modèle se concentre sur le déploiement des ressources dans le compte de journalisation. Si les journaux stockés dans Amazon S3 dans votre zone de AWS Control Tower landing zone sont chiffrés à l'aide d'une clé KMS gérée par le client, vous devez mettre à jour la politique relative aux clés pour permettre à Microsoft Sentinel de déchiffrer les journaux. Dans une zone de AWS Control Tower landing zone, vous gérez la politique des clés depuis le compte de gestion, où la clé a été créée.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie dans toutes Comptes AWS les régions.
- Amazon vous CloudWatch aide à surveiller les indicateurs de vos AWS ressources et des applications que vous utilisez AWS en temps réel.
- AWS Control Towervous aide à configurer et à gérer un environnement AWS multi-comptes, conformément aux meilleures pratiques.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques afin de protéger vos données.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- Amazon Simple Queue Service (Amazon SQS) fournit une file d'attente hébergée sécurisée, durable et disponible qui vous permet d'intégrer et de dissocier les systèmes et composants logiciels distribués.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- Microsoft Sentinel est un système SIEM natif du cloud qui assure l'orchestration, l'automatisation et la réponse en matière de sécurité (SOAR).

Référentiel de code

Le code de ce modèle est disponible dans le référentiel d' GitHub ingestion et d'analyse des journaux AWS de sécurité de Microsoft Sentinel.

Bonnes pratiques

- Respectez le principe du moindre privilège (documentation IAM).
- Suivez les meilleures pratiques pour AWS Control Tower les administrateurs (AWS Control Tower documentation).
- Suivez les AWS CloudFormation meilleures pratiques (CloudFormation documentation).
- Utilisez des outils d'analyse de code, tels que cfn_nag, pour scanner les modèles générés. CloudFormation L'outil cfn_nag identifie les problèmes de sécurité potentiels dans les CloudFormation modèles en recherchant des modèles.

Épopées

Connect Microsoft Sentinel à Amazon S3

Tâche	Description	Compétences requises
Préparez le connecteur Microsoft Sentinel S3.	1. Dans Microsoft Sentinel, choisissez Data connectors. 2. Dans la galerie de connecteurs de données, choisissez Amazon Web Services S3. **Note** Si le connecteur n'apparaît pas, installez la solution Amazon Web	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	Services depuis le Content Hub de Microsoft Sentinel. 3. Dans le volet de détails du connecteur, choisissez Ouvrir la page du connecteur. 4. Dans la section Configuration, copiez l'ID externe. Vous aurez besoin de cet identifiant plus tard.	

Déployez la CloudFormation pile

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Dans un shell bash, entrez la commande suivante. Cela clone l'ingestion et analyse les journaux de AWS sécurité dans le référentiel Microsoft Sentinel. `git clone https://github.com/aws-samples/ingest-and-analyze-aws-security-logs-in-microsoft-sentinel.git`	DevOps ingénieur, AWS général
Assumez le rôle IAM dans le compte de journalisation.	Dans le compte de journalisation, assumez le rôle IAM autorisé à déployer la CloudFormation pile. Pour	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	plus d'informations sur l'attribution d'un rôle IAM dans le AWS CLI, voir Utiliser un rôle IAM dans le. AWS CLI	

Tâche	Description	Compétences requises
Déployez la pile.	Pour déployer la CloudFormation pile, entrez la commande suivante, où : • `<Bucket name>` est le nom du compartiment Amazon S3 de journalisation. • `<Sentinel external ID>` est l'ID externe du connecteur Amazon S3 dans Microsoft Sentinel. • `<Email address>` est une adresse e-mail valide à laquelle vous souhaitez recevoir des notifications. • `<Customer managed key ARN>` est le nom de ressource Amazon (ARN) de la clé KMS gérée par le client. Fournissez ce paramètre uniquement si les journaux sont chiffrés à l'aide d'une clé KMS gérée par le client. • `<Suffix>` est un paramètre facultatif pour éviter les conflits de noms de ressources. • `<ARN for the OIDC provider>` est l'ARN du fournisseur OIDC s'il existe déjà. Si vous ne fournissez pas ce paramètre	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	, CloudFormation crée le fournisseur OIDC. **Important** Si l' AWS organisation est surveillée à l'aide de Microsoft Code Defender, le fournisseur OIDC pour Microsoft a déjà été déployé. Vous devez fournir ce paramètre ainsi que l'ARN du fournisseur existant. `aws cloudformation deploy --stack-name cloudtrail-sentinel-integration \ --no-fail-on-empty-changeset \ --template-file template.yml \ --capabilities CAPABILITY_IAM CAPABILITY_NAMED_IAM CAPABILITY_AUTO_EXPAND \ --parameter-overrides \ ControlTowerS3BucketName="<Bucket name>" \`	

Tâche	Description	Compétences requises
	`AzureWorkspaceID="<Sentinel external ID>" \ EmailAddress="<Email address>" \ KMSKeyArn="<Customer managed key ARN>" \ Suffix="<Suffix to avoid name conflicts>" \ OIDCProviderArn="<ARN for the OIDC provider>"`	
Copiez les sorties.	À partir de la sortie de la CloudFormation pile, copiez les valeurs pour `SentinelRoleArn` et`SentinelSQS` . Vous utiliserez ces valeurs ultérieurement pour terminer la configuration dans Microsoft Sentinel.	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
Modifiez la politique clé.	Si vous n'utilisez pas de clé KMS gérée par le client pour chiffrer les journaux du compartiment Amazon S3, vous pouvez ignorer cette étape. Si les journaux sont chiffrés à l'aide d'une clé KMS gérée par le client, modifiez la politique relative aux clés pour autoriser Microsoft Sentinel à déchiffrer les journaux. Voici un exemple de stratégie de clé. Cet exemple de politique autorise l'accès entre comptes si la clé KMS se trouve dans un autre Compte AWS. `{ "Version": "2012-10-17", "Id": "key-policy", "Statement": [ ... { "Sid": "Grant access to decrypt", "Effect": "Allow", "Principal": { "AWS": "<SentinelRoleArn>" }, "Action": "kms:Decrypt",`	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	"Resource": "<KeyArn>" }] }	

Configurer le connecteur dans Microsoft Sentinel

Tâche	Description	Compétences requises
Terminez la configuration dans Microsoft Sentinel.	1. Dans Microsoft Sentinel, choisissez Data connectors. 2. Dans la galerie de connecteurs de données, choisissez Amazon Web Services S3. 3. Dans le volet de détails du connecteur, choisisse z Ouvrir la page du connecteur. 4. Dans la section Configura tion, procédez comme suit : a. Dans Rôle à ajouter, entrez la `SentinelR oleArn` valeur que vous avez copiée. b. Dans URL SQS, entrez la `SentinelSQS` valeur que vous avez copiée. c. Dans la liste du tableau Destination, sélection nez`AWSCloudTrail` .	DevOps ingénieur

Tâche	Description	Compétences requises
	5. Choisissez Add Connection (Ajouter une connexion).	
Envoyez des notifications d'événements Amazon S3 à Amazon SQS.	Suivez les instructions de la section Activation et configuration des notifications d'événements à l'aide de la console Amazon S3 pour configurer le compartiment de journalisation Amazon S3 afin d'envoyer des notifications d'événements à la file d'attente Amazon SQS. S'il CloudTrail a été configuré pour l'ensemble de l'organisation, les journaux de ce compartiment portent le préfixe`<OrgID>/AWSLogs/<OrgID>/` , où se `<OrgID>` trouve l'ID de l'organisation. Pour plus d'informations, consultez la section Affichage des informations relatives à votre organisation.	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
Vérifiez que les journaux sont ingérés.	1. Attendez que les journaux soient ingérés dans Microsoft Sentinel. Cela peut prendre plusieurs minutes. 2. Dans Microsoft Sentinel, ouvrez la page Amazon S3 Data Connector, puis effectuez les opérations suivantes : • Vérifiez que le statut du connecteur de données Amazon S3 est `Connected` . • Vérifiez le volume de données dans le graphique des données reçues. Pour plus d'informations sur l'inspection de l'activité du connecteur de données, consultez la section Connecteur de données dans la documentation Microsoft.	DevOps ingénieur

Validez la solution

Tâche	Description	Compétences requises
Journaux CloudWatch de comparaison et de Sentinel.	Dans la configuration par défaut de AWS Control Tower, CloudTrail les journaux sont	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	envoyés à Amazon CloudWatch et stockés dans le compte AWS Control Tower de gestion. Pour plus d'informations, consultez la section Connexion et surveillance AWS Control Tower. Suivez les étapes suivantes pour vérifier que les journaux sont automatiquement ingérés dans Microsoft Sentinel : 1. Ouvrez la CloudWatch console. 2. Dans le panneau de navigation, choisissez Logs (Journaux), puis Logs Insights. 3. Pour Sélectionner un ou plusieurs groupes de journaux, sélectionnez le groupe de journaux dans lequel les CloudTrail journaux sont stockés, par exemple`aws-controltower/CloudTrailLogs` . 4. Dans la zone de l'éditeur de requêtes, entrez`fields eventID`. 5. Choisissez Exécuter la requête. 6. Choisissez Exporter les résultats, puis Copier le	

Tâche	Description	Compétences requises
	tableau dans le presse-papiers (CSV). 7. Collez les résultats dans un éditeur de texte. 8. Modifiez le format de la sortie afin qu'elle puisse être utilisée dans une requête Microsoft Sentinel. Voici un exemple qui utilise le langage de requête Kusto : `AWSCloudTrail	where AwsEventId in ('aa08b5fe-3bfb-391a-a14e-5fcebe14dab2', '9decd805-269c-451c-b75b-762f5dce59f9')` 9. Dans Microsoft Sentinel, ouvrez la page Amazon S3 Data Connector. À côté du graphique des données reçues, choisissez Accéder aux analyses du journal. 10. Dans la zone de l'éditeur de requêtes, entrez la requête, puis choisissez Exécuter. 11. Dans Microsoft Sentinel et CloudWatch, vérifiez que le nombre d'entrées est identique. Adaptez la plage horaire si nécessaire.	

Ressources connexes

AWS documentation et ressources

- AWS CLI Référence de commande (AWS CLI documentation)
- Configuration facultative AWS KMS keys (AWS Control Tower documentation)
- Chiffrement au repos dans Amazon SQS (documentation Amazon SQS)
- Comment empêcher les destinataires de mes listes de diffusion de désinscrire toutes les personnes figurant sur la liste de mes e-mails thématiques Amazon SNS ? (Centre de AWS connaissances)

Documentation Microsoft

- Connectez Microsoft Sentinel à Amazon Web Services pour ingérer les données des journaux AWS de service
- Langage de requête Kusto dans Microsoft Sentinel

Gérez AWS Organizations les politiques sous forme de code en utilisant AWS CodePipeline Amazon Bedrock

Créée par André Cavalcante (AWS) et Mariana Pessoa de Queiroz (AWS)

Récapitulatif

Vous pouvez utiliser les politiques d'autorisation AWS Organizations pour configurer et gérer de manière centralisée l'accès des principaux et des ressources dans vos comptes de membres. Les politiques de contrôle des services (SCPs) définissent les autorisations maximales disponibles pour les rôles AWS Identity and Access Management (IAM) et les utilisateurs de votre organisation. Les politiques de contrôle des ressources (RCPs) définissent le maximum d'autorisations disponibles pour les ressources de votre organisation.

Ce modèle vous permet de gérer SCPs et d'assimiler l'infrastructure RCPs sous forme de code (IaC) que vous déployez par le biais d'un pipeline d'intégration et de déploiement continus (CI/CD). En utilisant AWS CloudFormation ou Hashicorp Terraform pour gérer ces politiques, vous pouvez réduire la charge associée à la création et à la maintenance de plusieurs politiques d'autorisation.

Ce modèle inclut les fonctionnalités suivantes :

- Vous créez, supprimez et mettez à jour les politiques d'autorisation à l'aide de fichiers manifestes (`scp-management.jsonetrcp-management.json`).
- Vous travaillez avec des barrières de sécurité plutôt que des politiques. Vous définissez vos barrières de sécurité et leurs cibles dans les fichiers manifestes.
- Le pipeline, qui utilise AWS CodeBuild AWS CodePipeline, fusionne et optimise les garde-fous contenus dans les fichiers manifestes. Pour chaque instruction du fichier manifeste, le pipeline combine les barrières de sécurité en un seul SCP ou RCP, puis l'applique aux cibles définies.
- AWS Organizations applique les politiques à vos cibles. Une cible peut être une Compte AWS unité organisationnelle (UO), un environnement (qui est un groupe de comptes ou OUs que vous définissez dans le `environments.json` fichier) ou un groupe de comptes partageant un AWS tag.
- Amazon Bedrock lit les journaux du pipeline et résume tous les changements de politique.
- Le pipeline nécessite une approbation manuelle. L'approbateur peut consulter le résumé élaboré par Amazon Bedrock, qui l'aide à comprendre les modifications.

Conditions préalables et limitations

Prérequis

- Plusieurs Comptes AWS entités gérées en tant qu'organisation dans AWS Organizations. Pour plus d'informations, consultez la section Création d'une organisation.
- Les fonctionnalités SCP et RCP sont activées dans. AWS Organizations Pour plus d'informations, consultez la section Activation d'un type de politique.
- La version 1.9.8 ou ultérieure de Terraform est installée.
- Si vous ne déployez pas cette solution via un pipeline Terraform, le fichier d'état Terraform doit être stocké dans un bucket Amazon Simple Storage Service (Amazon S3) dans Compte AWS lequel vous déployez le pipeline de gestion des politiques.
- La version 3.13.3 ou ultérieure de Python est installée.

Limites

- Vous ne pouvez pas utiliser ce modèle pour gérer SCPs ou RCPs qui a été créé en dehors de ce pipeline CI/CD. Toutefois, vous pouvez recréer les politiques existantes par le biais du pipeline. Pour plus d'informations, consultez la section Migration des politiques existantes vers le pipeline dans la section Informations supplémentaires de ce modèle.
- Le nombre de comptes et OUs les politiques de chaque compte sont soumis aux quotas et aux limites de service pour AWS Organizations.
- Ce modèle ne peut pas être utilisé pour configurer des politiques de gestion AWS Organizations, telles que des politiques de sauvegarde, des politiques de balises, des politiques d'applications de chat ou des politiques déclaratives.

Architecture

Le schéma suivant montre le flux de travail du pipeline de gestion des politiques et de ses ressources associées.

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur valide les modifications apportées aux fichiers `scp-management.json` ou aux fichiers `rcp-management.json` manifestes dans la branche principale du référentiel distant.

2. La modification de la `main` branche initie le pipeline. AWS CodePipeline
3. CodePipeline lance le `Validate-Plan` CodeBuild projet. Ce projet utilise un script Python dans le référentiel distant pour valider les politiques et les fichiers manifestes de politiques. Ce CodeBuild projet effectue les opérations suivantes :
   a. Vérifie que les fichiers manifestes SCP et RCP contiennent une instruction unique IDs ()`Sid`.
   b. Utilise les scripts `scp-policy-processor/main.py` et `rcp-policy-processor/main.py` Python pour concaténer les glissières de sécurité du dossier des barres de sécurité en une seule politique RCP ou SCP. Il combine des rambardes qui ont les mêmes `ResourceAction`, et. `Condition`
   c. Utilisée AWS Identity and Access Management Access Analyzer pour valider la politique finale optimisée. S'il y a des découvertes, le pipeline s'arrête.
   d. Crée `scps.json` des `rcps.json` fichiers, que Terraform utilise pour créer des ressources.
   e. Exécute la `terraform plan` commande, qui crée un plan d'exécution Terraform.
4. (Facultatif) Le `Validate-Plan` CodeBuild projet utilise le `bedrock-prompt/prompt.py` script pour envoyer une invite à Amazon Bedrock. Vous définissez l'invite dans le `bedrock-prompt/prompt.txt` fichier. Amazon Bedrock utilise Anthropic Claude Sonnet 3.5 pour générer un résumé des modifications proposées en analysant les logs Terraform et Python.
5. CodePipeline utilise une rubrique Amazon Simple Notification Service (Amazon SNS) afin d'informer les approbateurs que les modifications doivent être révisées. Si Amazon Bedrock a généré un résumé des modifications, la notification inclut ce résumé.
6. Un approbateur de politique approuve l'action dans. CodePipeline Si Amazon Bedrock a généré un résumé des modifications, l'approbateur peut consulter le résumé CodePipeline avant de l'approuver.
7. CodePipeline lance le `Apply` CodeBuild projet. Ce projet utilise Terraform pour appliquer les modifications du RCP et du SCP dans. AWS Organizations

Le modèle IaC associé à cette architecture déploie également les ressources suivantes qui prennent en charge le pipeline de gestion des politiques :

- Un compartiment Amazon S3 pour stocker les CodePipeline artefacts et les scripts, tels que `scp-policy-processor/main.py` et `bedrock-prompt/prompt.py`
- Une clé AWS Key Management Service (AWS KMS) qui chiffre les ressources créées par cette solution

Outils

Services AWS

- Amazon Bedrock est un service d'intelligence artificielle entièrement géré qui met à disposition de nombreux modèles de base très performants via une API unifiée.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Autres outils

- HashiCorp Terraform est un outil IaC qui vous aide à utiliser du code pour provisionner et gérer l'infrastructure et les ressources du cloud.

Référentiel de code

Le code de ce modèle est disponible dans le organizations-policy-pipeline GitHub référentiel. Les fichiers clés contenus dans le `sample-repository` dossier sont les suivants :

- Le `environments` dossier `environments.json` contient une liste d'environnements. Les environnements sont un groupe de cibles, et ils peuvent contenir Compte AWS IDs des unités organisationnelles (OUs).
- Dans le `rcp-management` dossier :
  - Le `guardrails` dossier contient les rambardes individuelles pour votre RCPs
  - Le `policies` dossier contient la personne RCPs
  - Le fichier `rcp-management.json` manifeste vous permet de gérer les barrières de sécurité RCP complètes et leurs RCPs cibles associées.

- Dans le `scp-management` dossier :
  - Le `guardrails` dossier contient les rambardes individuelles pour votre SCPs
  - Le `policies` dossier contient la personne SCPs
  - Le fichier `scp-management.json` manifeste vous permet de gérer les barrières SCP complètes et leurs SCPs cibles associées.
- Le `utils` dossier contient des scripts qui peuvent vous aider à migrer vos fichiers actuels SCPs et vous RCPs permettre de les gérer tout au long du pipeline. Pour plus d'informations, consultez la section Informations supplémentaires de ce modèle.

Bonnes pratiques

- Avant de configurer le pipeline, nous vous recommandons de vérifier que vous n'avez pas atteint les limites de vos AWS Organizations quotas.
- Nous vous recommandons d'utiliser le compte AWS Organizations de gestion uniquement pour les tâches qui doivent être effectuées dans ce compte. Pour plus d'informations, consultez la section Meilleures pratiques pour le compte de gestion.

Épopées

Configurer le compte cible

Tâche	Description	Compétences requises
Créer un référentiel .	Créez un référentiel à partir duquel votre équipe des opérations de sécurité gérera les politiques. Utilisez l'un des fournisseurs de référentiels tiers pris en AWS CodeConnections charge.	DevOps ingénieur
Déléguer l'administration des politiques.	Déléguez l'administration des AWS Organizations politiques au compte membre sur lequel vous déployez	Administrateur AWS

Tâche	Description	Compétences requises
	le pipeline. Pour obtenir des instructions, voir Créer une politique de délégation basée sur les ressources avec. AWS Organizations Pour un exemple de politique, voir Exemple de stratégie de délégation basée sur les ressources dans la section Informations supplémentaires de ce modèle.	
(Facultatif) Activez le modèle de base.	Si vous souhaitez générer des résumés des modifications apportées aux politiques, autorisez l'accès au modèle de base Anthropic Claude 3.5 Sonnet dans Amazon Bedrock, Compte AWS là où vous déployez le pipeline. Pour obtenir des instructions, consultez Ajouter ou supprimer l'accès aux modèles de fondation Amazon Bedrock.	AWS général

Déployer les ressources pour le pipeline

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Entrez la commande suivante pour cloner le organizations-policy-pipeline référentiel à partir de GitHub :	DevOps ingénieur

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/organizations-policy-pipeline.git`	

Tâche	Description	Compétences requises
Définissez votre méthode de déploiement.	1. Dans le référentiel cloné, ouvrez le `variables.tf` fichier. 2. Pour`project_name` , entrez le préfixe que vous souhaitez appliquer aux noms des ressources déployées. 3. Pour`provider_type` , entrez le fournisseur du référentiel distant. Des valeurs valides sont fournies dans le fichier. 4. Pour`full_repo sitory_name` , entrez le nom du référentiel distant. 5. Pour`branch_name` , entrez le nom de la branche Git que vous utiliserez pour déployer les politiques. Un push ou une fusion dans cette branche démarre le pipeline. Il s'agit généralem ent de la branche principal e. 6. Pour`terraform _version` , entrez la version de Terraform que vous utilisez. 7. Pour`enable_bedrock` , entrez `true` si vous souhaitez qu'Amazon Bedrock récapitule les	DevOps ingénieur

Tâche	Description	Compétences requises
	modifications. Entrez `false` si vous ne souhaitez pas générer de résumé des modifications. 8. Pour `tags`, entrez les paires clé-valeur que vous souhaitez attribuer sous forme de balises aux ressources déployées. 9. Enregistrez et fermez le fichier `variables.tf` .	

Déployez le pipeline.	1. Entrez la commande suivante pour créer un plan et passer en revue les modifications :
	`terraform plan`
	2. Entrez la commande suivante pour appliquer le plan et créer l'infrastructure du pipeline :
	`terraform apply`
		DevOps ingénieur, Terraform

Tâche	Description	Compétences requises
Connectez le référentiel distant.	À l'étape précédente, Terraform a créé une CodeConnections connexion au référentiel tiers. Dans la console AWS Developer Tools, modifiez le statut de la connexion de `PENDING` à`AVAILABLE` . Pour obtenir des instructions, voir Mettre à jour une connexion en attente.	AWS DevOps
Abonnez-vous à la rubrique Amazon SNS.	Terraform a créé une rubrique Amazon SNS. Abonnez un point de terminaison au sujet et confirmez l'abonnement afin que les approbateurs reçoivent des notifications concernant les actions d'approbation en attente dans le pipeline. Pour obtenir des instructions, consultez la section Création d'un abonnement à une rubrique Amazon SNS.	AWS général

Définissez vos garde-fous et vos politiques

Tâche	Description	Compétences requises
Remplissez le référentiel distant.	Depuis le dépôt cloné, copiez le contenu du `sample-repository` dossier dans votre dépôt distant. Cela inclut les `utils` dossiers	DevOps ingénieur

Tâche	Description	Compétences requises
	`environments rcp-management scp-management` ,, et.	

Tâche	Description	Compétences requises
Définissez vos environnements.	1. Dans le `environments` dossier, ouvrez le `environments.json` fichier. Il s'agit du fichier dans lequel vous définissez la cible Comptes AWS et OUs pour votre RCPs et SCPs. 2. Supprimez les exemples d'environnements. 3. Ajoutez vos environnements cibles au format suivant : `[ { "ID": "<environment-name>", "Target": [ "<ou-name>:<ou-id>", "<account-name>:<account-id>" ] } ]` Où : • `<environment-name>` est le nom que vous attribuez au groupe OUs de comptes AWS. Vous pouvez utiliser ce nom dans le fichier manifeste	DevOps ingénieur

Tâche	Description	Compétences requises
	pour définir l'endroit où vous souhaitez appliquer vos politiques. • `<ou-name>` est le nom de l'unité d'organisation cible. • `<ou-id>`est l'ID de l'unité d'organisation cible. • `<account-name>` est le nom de la cible Compte AWS. • `<account-id>` est l'ID de la cible Compte AWS. Pour des exemples, consultez le référentiel de code source. 4. Enregistrez et fermez le fichier `environments.json` .	

Tâche	Description	Compétences requises
Définissez vos rambardes.	1. Accédez au `rcp-management/guardrails` dossier de votre référentiel distant. Il s'agit du dossier dans lequel vous définissez les barrières de sécurité pour votre fichier manifeste RCP. Chaque garde-corps doit figurer dans un dossier individuel. Les fichiers Guardrail peuvent contenir une ou plusieurs instructions. **Note** Vous pouvez utiliser le même garde-fou dans plusieurs instructions des fichiers manifestes pour SCPs et. RCPs Si vous modifiez le garde-corps, toutes les politiques qui incluent ce garde-corps sont affectées . 2. Supprimez tous les exemples de garde-corps copiés depuis le référentiel du code source.	DevOps ingénieur

Tâche	Description	Compétences requises
	3. Créez un nouveau fichier .json et donnez-lui un nom descriptif. 4. Ouvrez le fichier .json que vous avez créé. 5. Définissez le garde-corps au format suivant : `[ { "Sid": "<guardrail-name>", "Effect": "<effect-value>", "Action": [ "<action-name>" ], "Resource": "<resource-arn>", "Condition": { "<condition-operator>": { "<condition-key>": [ "<condition-value>" ] } } } ]` Où : • `<guardrail-name>` est un nom unique pour le garde-corps. Ce	

Tâche	Description	Compétences requises
	nom ne peut être utilisé pour aucun autre garde-corps. • `<effect-value>` doit être `Allow` ou`Deny`. Pour plus d'informations, consultez la section Effet. • `<action-name>` doit être le nom valide d'une action prise en charge par le service. Pour plus d'informations, consultez la section Action. • `<resource-arn>` est le nom de ressource Amazon (ARN) de la ressource à laquelle s'applique le garde-corps. Vous pouvez également utiliser des caractères génériques, tels que `*` ou`?`. Pour plus d'informations, consultez la section Ressource. • `<condition-operator>` est un opérateur de condition valide. Pour plus d'informations, consultez la section Opérateurs de condition. • `<condition-key>` est une clé de contexte de condition globale valide ou une clé de contexte	

Tâche	Description	Compétences requises
	spécifique à un service. Pour plus d'informations, consultez la section Condition. • `<condition-value>` est la valeur spécifique utilisée dans une condition pour évaluer si un garde-corps s'applique. Pour plus d'informations, consultez la section Condition. Par exemple, les garde-corps RCP, consultez le référentiel de code source. 6. Enregistrez et fermez le fichier .json. 7. Répétez ces étapes pour créer autant de garde-corps RCP que nécessaire. 8. Répétez ces étapes dans le `scp-management/guardrails` dossier pour créer autant de garde-corps que nécessaire pour votre. SCPs Par exemple, les garde-corps SCP, consultez le référentiel du code source.	

Tâche	Description	Compétences requises
Définissez vos politiques.	1. Accédez au `rcp-management/policies` dossier de votre référentiel distant. Il s'agit du dossier dans lequel vous définissez les politiques complètes pour votre fichier manifeste RCP. Chaque politique doit être un fichier individuel. **Note** Si vous modifiez une politique dans ce dossier, les modifications de stratégie affectent tous les comptes ou tous les comptes OUs auxquels cette politique est appliquée, comme défini dans le fichier manifeste. 2. Supprimez tous les exemples de politiques copiés depuis le référentiel de code source. 3. Créez un nouveau fichier .json et donnez-lui un nom descriptif. 4. Ouvrez le fichier .json que vous avez créé.	DevOps ingénieur

Tâche	Description	Compétences requises
	5. Définissez le RCP. Par exemple RCPs, consultez le référentiel de code source ou consultez les exemples de politiques de contrôle des ressources dans la AWS Organizations documentation. 6. Enregistrez et fermez le fichier .json. 7. Répétez ces étapes pour en créer RCPs autant que nécessaire. 8. Répétez ces étapes dans le `scp-management/policies` dossier pour en créer SCPs autant que nécessaire. Par exemple SCPs, consultez le référentiel de code source ou consultez les exemples de politiques de contrôle des services dans la AWS Organizations documentation.	

Utiliser le fichier manifeste pour gérer les politiques

Tâche	Description	Compétences requises
Configurez les fichiers manifestes.	1. Dans le `rcp-management` dossier, ouvrez le `rcp-management.json` fichier. Il s'agit du fichier	DevOps ingénieur

Tâche	Description	Compétences requises
	dans lequel vous définissez les garde-fous RCP qui RCPs s'appliquent pleinement à vos environnements cibles. Pour un exemple de ce fichier, consultez le référentiel de code source. 2. Supprimez l'exemple de déclaration. 3. Ajoutez une nouvelle déclaration au format suivant : `[ { "SID": "<statement-name>", "Target": { "Type": "<target-type>", "ID": "<target-name>" }, "Guardrails": [ "<guardrail-name>" ], "Policy": "<policy-name>", "Comments": "<comment-text>" } ]` Où :	

Tâche	Description	Compétences requises

	• `<statement-name>`est un nom unique pour la déclaration.
	• `<target-type>` est le type de cible auquel vous souhaitez appliquer la politique. Les valeurs valides sont `Account`, `OU`, `Environment` ou `Tag`.
	• `<target-name>` est l'identifiant de la cible à laquelle vous souhaitez appliquer la politique . Indiquez l'un des éléments suivants :
	  • Pour un Compte AWS, entrez l'identifiant sous la forme`<account-name>:<account-id>` .
	  • Pour une unité d'organisation, entrez l'identifiant sous la forme`<OU-name>:<ou-id>` .
	  • Pour un environnement, entrez le nom unique que vous avez défini dans le `environments.json` fichier.	

Tâche	Description	Compétences requises
	• Pour une balise, entrez la paire clé-valeur sous la forme. `<tag-key>:<tag-value>` • `<guardrail-name>`est le nom unique du garde-corps RCP que vous avez défini dans le dossier. `rcp-management/guardrails` Vous pouvez ajouter plusieurs rambardes dans cet élément. Vous pouvez laisser ce champ vide si vous ne souhaitez pas installer de garde-corps. • `<policy-name>` est le nom unique du RCP que vous avez défini dans le `rcp-management/policies` dossier. Vous ne pouvez ajouter qu'une seule politique dans cet élément. Vous pouvez laisser ce champ vide si vous ne souhaitez pas appliquer de politique. • `<comment-text>` est une description que vous pouvez saisir à des fins de documentation. Ce champ n'est pas utilisé pendant le traitement du pipeline. Vous pouvez	

Tâche	Description	Compétences requises
	laisser ce champ vide si vous ne souhaitez pas ajouter de commentaire. 4. Répétez ces étapes pour ajouter autant d'instructions que nécessaire à configure r RCPs pour votre organisat ion. 5. Enregistrez et fermez le fichier `rcp-manag ement.json` . 6. Dans le `scp-manag ement` dossier, répétez ces étapes dans le `scp-management.json` fichier. Il s'agit du fichier dans lequel vous définisse z les garde-corps SCP qui SCPs s'appliquent pleinement à vos environne ments cibles. Pour un exemple de ce fichier, consultez le référentiel de code source.	

Tâche	Description	Compétences requises
Démarrez le pipeline.	Validez et envoyez les modifications à la branche du référentiel distant que vous avez définie dans le `variables.tf` fichier. Il s'agit généralement de la `main` branche. Le pipeline CI/CD démarre automatiq uement. En cas d'erreur de pipeline, consultez la section Dépannage de ce modèle.	DevOps ingénieur
Approuvez les modifications.	Lorsque le `Validate-Plan` CodeBuild projet est terminé, les approbateurs des politique s reçoivent une notification via la rubrique Amazon SNS que vous avez précédemment configurée. Procédez comme suit : 1. Ouvrez le message de notification. 2. Le cas échéant, consultez le résumé des modifications apportées aux politiques. 3. Suivez les instructions de la section Approuver ou rejeter une action d'approba tion dans CodePipeline.	AWS général, approbateur de politiques

Tâche	Description	Compétences requises
Validez le déploiement.	1. Connectez-vous à la AWS Organizations console avec le compte dont vous êtes l'administrateur délégué AWS Organizations. 2. Sur la page Politiques de contrôle des services, vérifiez que les politique s SCPs que vous avez créées sont répertoriées. 3. Choisissez un SCP géré via le pipeline et confirmez qu'il s'applique aux cibles prévues. 4. Sur la page Politiques de contrôle des ressources, vérifiez que celles RCPs que vous avez créées sont répertoriées. 5. Choisissez un RCP géré via le pipeline et vérifiez qu'il s'applique aux cibles prévues.	AWS général

Résolution des problèmes

Problème	Solution
Erreurs de fichiers manifestes dans la `Validate-Plan` phase du pipeline	Un message « Erreurs de pipeline lors de la phase de validation et de planification pour les fichiers manifestes » apparaît dans la sortie du pipeline en cas d'erreur dans les `rcp-management.json` fichiers `scp-manag`

Problème	Solution
	`ement.json` ou. Les erreurs possibles incluent un nom d'environnement incorrect, des champs ou des valeurs dupliqués SIDs ou non valides. Procédez comme suit : 1. Suivez les instructions de la section Afficher les détails de la version dans AWS CodeBuild. 2. Dans le journal de construction, recherche z l'erreur de validation. L'erreur fournit plus d'informations sur la cause de l'échec de la compilation. 3. Mettez à jour le fichier .json correspondant. 4. Validez et transférez le fichier mis à jour vers le référentiel distant. Le pipeline redémarre. 5. Surveillez l'état pour confirmer que l'erreur de validation est résolue.

Problème	Solution
Conclusions d'IAM Access Analyzer au `Validate-Plan` cours de la phase du pipeline	Un message « Résultats trouvés dans IAM Access Analyzer pendant la phase de validation et de planification » apparaît dans la sortie du pipeline en cas d'erreur dans le garde-fou ou dans les définitions des politiques. Ce modèle utilise IAM Access Analyzer pour valider la politique finale. Procédez comme suit : 1. Suivez les instructions de la section Afficher les détails de la version dans AWS CodeBuild. 2. Dans le journal de compilation, recherchez l'erreur de validation d'IAM Access Analyzer. L'erreur fournit plus d'informations sur la cause de l'échec de la compilation. Pour plus d'informations sur les types de recherche , consultez la référence de vérification de validation des politiques IAM. 3. Mettez à jour le fichier .json correspondant au garde-corps ou à la politique. 4. Validez et transférez le fichier mis à jour vers le référentiel distant. Le pipeline redémarre. 5. Surveillez l'état pour confirmer que l'erreur de validation est résolue.

Ressources connexes

- Référence des éléments de politique JSON (documentation IAM)
- Politiques de contrôle des ressources (AWS Organizations documentation)
- Politiques de contrôle des services (AWS Organizations documentation)
- Ajouter ou supprimer l'accès aux modèles de fondation Amazon Bedrock (documentation Amazon Bedrock)

- Approuver ou rejeter une action d'approbation dans CodePipeline (CodePipeline documentation)

Informations supplémentaires

Exemple de politique de délégation basée sur les ressources

Voici un exemple de politique de délégation basée sur les ressources pour. AWS Organizations Il permet au compte d'administrateur délégué de gérer SCPs et RCPs pour l'organisation. Dans l'exemple de politique suivant, remplacez-le `<MEMBER_ACCOUNT_ID>` par l'ID du compte sur lequel vous déployez le pipeline de gestion des politiques.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegationToAudit",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<MEMBER_ACCOUNT_ID>:root"
      },
      "Action": [
        "organizations:ListTargetsForPolicy",
        "organizations:CreatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:DisablePolicyType",
        "organizations:EnablePolicyType",
        "organizations:UpdatePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:DescribePolicy",
        "organizations:DescribeResourcePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

Migration des politiques existantes vers le pipeline

Si vous en avez SCPs un existant ou RCPs que vous souhaitez migrer et gérer via ce pipeline, vous pouvez utiliser les scripts Python dans le `sample-repository/utils` dossier du référentiel de code. Ces scripts incluent :

- `check-if-scp-exists-in-env.py`— Ce script vérifie si une politique spécifiée s'applique à des cibles dans un environnement spécifique, que vous définissez dans le `environments.json` fichier. Entrez la commande suivante pour exécuter ce script :

  ```
  python3 check-if-scp-exists-in-env.py \
     --policy-type <POLICY_TYPE> \
     --policy-name <POLICY_NAME> \
     --env-id <ENV_ID>
  ```

  Remplacez le texte suivant dans cette commande :

  - <POLICY_TYPE> est `scp` ou `rcp`
  - <POLICY_NAME>est le nom du SCP ou du RCP
  - <ENV_ID>est l'ID de l'environnement que vous avez défini dans le `environments.json` fichier
- `create-environments.py`— Ce script crée un fichier environments.json en fonction de l'environnement actuel SCPs et RCPs de votre environnement. Cela exclut les politiques déployées via AWS Control Tower. Entrez la commande suivante pour exécuter ce script, où se <POLICY_TYPE> trouve `scp` ou `rcp` :

  ```
  python create-environments.py --policy-type <POLICY_TYPE>
  ```
- `verify-policies-capacity.py`— Ce script vérifie chaque environnement que vous définissez afin de déterminer la capacité restante pour chaque quota AWS Organizations lié aux politiques. Vous définissez les environnements à archiver dans le `environments.json` fichier. Entrez la commande suivante pour exécuter ce script, où se <POLICY_TYPE> trouve `scp` ou `rcp` :

  ```
  python verify-policies-capacity.py --policy-type <POLICY_TYPE>
  ```

Gérez les ensembles AWS IAM Identity Center d'autorisations sous forme de code en utilisant AWS CodePipeline

Créée par André Cavalcante (AWS) et Claison Amorim (AWS)

Récapitulatif

AWS IAM Identity Center vous permet de gérer de manière centralisée l'accès par authentification unique (SSO) à toutes vos applications Comptes AWS et applications. Vous pouvez créer et gérer les identités des utilisateurs dans IAM Identity Center, ou vous pouvez connecter une source d'identité existante, telle qu'un domaine Microsoft Active Directory ou un fournisseur d'identité externe (IdP). IAM Identity Center fournit une expérience d'administration unifiée permettant de définir, de personnaliser et d'attribuer un accès précis à votre AWS environnement à l'aide d'ensembles d'autorisations. Les ensembles d'autorisations s'appliquent aux utilisateurs et aux groupes fédérés à partir de votre banque d'identités IAM Identity Center ou de votre IdP externe.

Ce modèle vous aide à gérer les ensembles d'autorisations IAM Identity Center sous forme de code dans votre environnement multi-comptes géré en tant qu'organisation dans. AWS Organizations Avec ce modèle, vous pouvez obtenir les résultats suivants :

- Création, suppression et mise à jour d'ensembles d'autorisations
- Créez, mettez à jour ou supprimez des attributions d'ensembles d'autorisations pour Target Comptes AWS, les unités organisationnelles (OUs) ou la racine de votre organisation.

Pour gérer les autorisations et les attributions d'IAM Identity Center sous forme de code, cette solution déploie un pipeline d'intégration et de livraison continues (CI/CD) qui utilise et. AWS CodeBuild AWS CodePipeline Vous gérez les ensembles d'autorisations et les attributions dans les modèles JSON que vous stockez dans un référentiel distant. Lorsque EventBridge les règles Amazon détectent une modification du référentiel ou détectent des modifications apportées aux comptes dans l'unité d'organisation cible, une AWS Lambda fonction démarre. La fonction Lambda lance le pipeline CI/CD qui met à jour les ensembles d'autorisations et les attributions dans IAM Identity Center.

Conditions préalables et limitations

Prérequis

- Un environnement multi-comptes géré en tant qu'organisation dans AWS Organizations. Pour plus d'informations, consultez la section Création d'une organisation.

- IAM Identity Center, activé et configuré avec une source d'identité. Pour plus d'informations, consultez Getting Started dans la documentation d'IAM Identity Center.
- Un compte de membre enregistré en tant qu'administrateur délégué pour les tâches suivantes Services AWS :
  - IAM Identity Center : pour obtenir des instructions, voir Enregistrer un compte membre dans la documentation du IAM Identity Center.
  - AWS Organizations — Pour obtenir des instructions, consultez la section Administrateur délégué pour AWS Organizations. Ce compte doit être autorisé à répertorier et à décrire les comptes et OUs.

> **Note**
>
> Vous devez utiliser le même compte que l'administrateur délégué pour les deux services.

- Autorisations permettant de déployer AWS CloudFormation des piles dans le compte d'administrateur délégué d'IAM Identity Center et dans le compte de gestion de l'organisation. Pour plus d'informations, consultez la section Contrôle de l'accès dans la CloudFormation documentation.
- Un compartiment Amazon Simple Storage Service (Amazon S3) dans le compte d'administrateur délégué d'IAM Identity Center. Vous chargez le code de l'artefact dans ce compartiment. Pour obtenir des instructions, consultez la section Création d'un compartiment dans la documentation Amazon S3.
- L'identifiant du compte de gestion de l'organisation. Pour obtenir des instructions, consultez la section Trouver votre Compte AWS identifiant.
- Un référentiel dans votre hébergeur de code source, tel que GitHub.

Limites

- Ce modèle ne peut pas être utilisé pour gérer ou attribuer des ensembles d'autorisations pour des environnements à compte unique ou pour des comptes qui ne sont pas gérés en tant qu'organisation dans AWS Organizations.
- Les noms des ensembles d'autorisations, les IDs attributions et les principaux types de centres d'identité IAM IDs ne peuvent pas être modifiés après le déploiement.
- Ce modèle vous permet de créer et de gérer des autorisations personnalisées. Vous ne pouvez pas utiliser ce modèle pour gérer ou attribuer des autorisations prédéfinies.

- Ce modèle ne peut pas être utilisé pour gérer un ensemble d'autorisations pour le compte de gestion de l'organisation.

Architecture

Architecture cible

Le schéma suivant illustre le flux de travail suivant :

1. Un utilisateur effectue l'une des modifications suivantes :
   - Valide une ou plusieurs modifications apportées au référentiel distant, telles que GitHub
   - Modifie les comptes de l'unité d'organisation dans AWS Organizations
2. Si l'utilisateur a transféré une modification du référentiel distant à la branche principale, le pipeline démarre.

   Si l'utilisateur a modifié les comptes dans l'unité d'organisation, la `MoveAccount` EventBridge règle détecte le changement et lance une fonction Lambda dans le compte de gestion de l'organisation.
3. La fonction Lambda initiée démarre le pipeline CI/CD dans. CodePipeline
4. CodePipeline lance le `TemplateValidation` CodeBuild projet. Le `TemplateValidation` CodeBuild projet utilise un script Python dans le référentiel distant pour valider les modèles d'ensembles d'autorisations. CodeBuild valide les éléments suivants :
   - Les noms des ensembles d'autorisations sont uniques.
   - Les instructions d'affectation IDs (`Sid`) sont uniques.
   - Définitions de politique dans le `CustomPolicy` paramètre et valides. (Cette validation utilise AWS Identity and Access Management Access Analyzer.)
   - Les Amazon Resource Names (ARNs) des politiques gérées sont valides.
5. Le groupe `PermissionSet` d'actions du `Deploy` CodeBuild projet permet de AWS SDK pour Python (Boto3) supprimer, de créer ou de mettre à jour les ensembles d'autorisations dans IAM Identity Center. Seuls les ensembles d'autorisations comportant le `SSOPipeline:true` tag sont concernés. Tous les ensembles d'autorisations gérés via ce pipeline possèdent cette balise.
6. Le groupe `Assignments` d'action du `Deploy` CodeBuild projet utilise Terraform pour supprimer, créer ou mettre à jour les attributions dans IAM Identity Center. Les fichiers d'état du backend Terraform sont stockés dans un compartiment Amazon S3 du même compte.

7. CodeBuild met à jour les ensembles d'autorisations et les attributions dans IAM Identity Center.

Automatisation et mise à l'échelle

Étant donné que tous les nouveaux comptes d'un environnement multi-comptes sont déplacés vers une unité organisationnelle spécifique AWS Organizations, cette solution s'exécute automatiquement et accorde les ensembles d'autorisations requis à tous les comptes que vous spécifiez dans les modèles d'attribution. Aucune automatisation ou action de dimensionnement supplémentaire n'est nécessaire.

Dans les grands environnements, le nombre de demandes d'API adressées à IAM Identity Center peut ralentir le fonctionnement de cette solution. Terraform et Boto3 gèrent automatiquement la régulation afin de minimiser toute dégradation des performances.

Outils

Services AWS

- AWS CloudFormationvous aide à configurer les AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie, de bout Comptes AWS en bout Régions AWS.
- AWS CodeBuildest un service de génération entièrement géré qui vous aide à compiler le code source, à exécuter des tests unitaires et à produire des artefacts prêts à être déployés.
- AWS CodePipelinevous permet de modéliser et de configurer rapidement les différentes étapes d'une version logicielle et d'automatiser les étapes nécessaires à la publication continue des modifications logicielles.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, des AWS Lambda fonctions, des points de terminaison d'invocation HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS IAM Identity Centervous permet de gérer de manière centralisée l'accès par authentification unique (SSO) à toutes vos applications Comptes AWS et à celles du cloud.
- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée.
- AWS SDK pour Python (Boto3)est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python à Services AWS.

- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel aws-iam-identity-center-pipeline. Le dossier des modèles du référentiel contient des exemples de modèles pour les ensembles d'autorisations et les attributions. Il inclut également des AWS CloudFormation modèles pour déployer le pipeline CI/CD et les AWS ressources dans les comptes cibles.

Bonnes pratiques

- Avant de commencer à modifier le jeu d'autorisations et les modèles d'attribution, nous vous recommandons de planifier des ensembles d'autorisations pour votre organisation. Déterminez quelles devraient être les autorisations, à quels comptes ou OUs ensemble d'autorisations devraient s'appliquer, et quels principaux du centre d'identité IAM (utilisateurs ou groupes) devraient être concernés par l'ensemble d'autorisations. Les noms des ensembles d'autorisations, les associations IDs et les types principaux du centre d'identité IAM IDs ne peuvent pas être modifiés après le déploiement.
- Respectez le principe du moindre privilège et accordez les autorisations minimales requises pour effectuer une tâche. Pour plus d'informations, consultez les sections Accorder le moindre privilège et Bonnes pratiques en matière de sécurité dans la documentation AWS Identity and Access Management (IAM).

Épopées

Planifier les ensembles d'autorisations et les attributions

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Dans un shell bash, entrez la commande suivante. Cela clone le référentiel aws-iam-identity-center-pipeline à partir de. GitHub	DevOps ingénieur

Tâche	Description	Compétences requises
	`git clone https://github.com/aws-samples/aws-iam-identity-center-pipeline.git`	

Tâche	Description	Compétences requises
Définissez les ensembles d'autorisations.	1. Dans le référentiel cloné, accédez au `templates/permissionsets` dossier, puis ouvrez l'un des modèles disponibles. 2. Dans le `Name` paramètre, entrez le nom de l'ensemble d'autorisations. Cette valeur doit être unique et ne peut pas être modifiée après le déploiement. 3. Dans le `Description` paramètre, décrivez brièvement l'ensemble d'autorisations, par exemple son cas d'utilisation. 4. Dans le `SessionDuration` paramètre, spécifiez la durée pendant laquelle un utilisateur peut être connecté à un Compte AWS. Utilisez le format de durée ISO-8601 (Wikipedia), par exemple `PT4H` pendant 4 heures. Si aucune valeur n'est définie, la valeur par défaut dans IAM Identity Center est de 1 heure. 5. Dans le `RelayState` paramètre, spécifiez l'URL qui fournit un accès rapide à la console la mieux	DevOps ingénieur

Tâche	Description	Compétences requises
	adaptée au rôle de l'utilisateur. 6. Personnalisez les politiques de l'ensemble d'autorisations. Tous les paramètres suivants sont facultatifs et peuvent être modifiés après le déploiement. Vous devez utiliser au moins l'un des paramètres afin de définir les politiques du jeu d'autorisations : • Dans le `ManagedPolicies` paramètre, entrez toutes ARNs les politiques AWS gérées que vous souhaitez attribuer. • Dans le `CustomerManagedPolicies` paramètre, entrez le nom de toutes les politiques gérées par le client que vous souhaitez attribuer. N'utilisez pas l'ARN. • Dans le `PermissionBoundary` paramètre, procédez comme suit pour attribuer une limite d'autorisation : • Si vous utilisez une politique AWS gérée comme limite d'autorisation`PolicyType` ,	

Tâche	Description	Compétences requises
	entrezAWS, entrez et entrez l'ARN de la politique. `Policy` • Si vous utilisez une politique gérée par le client comme limite d'autoris ationsPolicyTyp e , entrez`Customer`, entrez et entrez le nom de la politique. `Policy` N'utilisez pas l'ARN. • Dans le `CustomPolicy` paramètre, définissez les politiques personnalisées au format JSON que vous souhaitez attribuer. Pour plus d'informations sur la structure des politique s JSON, consultez la section Présentation des politiques JSON. 7. Enregistrez et fermez le modèle d'ensemble d'autorisations. Nous vous recommandons d'enregis trer le fichier sous un nom correspondant au nom de l'ensemble d'autorisations. 8. Répétez ce processus pour créer autant d'ensembl es d'autorisations que nécessaire pour votre organisation et supprimez	

Tâche	Description	Compétences requises
	les exemples de modèles qui ne sont pas nécessaires.	

Tâche	Description	Compétences requises
Définissez les missions.	1. Dans le référentiel cloné, accédez au `templates/assignments` dossier, puis `iam-identitycenter-assigments.json` ouvrez-le. Ce fichier décrit la manière dont vous souhaitez attribuer les ensembles d'autorisations à Comptes AWS ou OUs. 2. Dans le `SID` paramètre, entrez un identifiant pour l'affectation. Cette valeur doit être unique et ne peut pas être modifiée après le déploiement. 3. Dans le `Target` paramètre , définissez les comptes ou les organisations auxquels vous souhaitez appliquer l'ensemble d'autorisations. Les valeurs valides sont IDs account OUs, ou`root`. `root`attribue l'ensembl e d'autorisations à tous les comptes membres de l'organisation, à l'excepti on du compte de gestion. Entrez les valeurs entre guillemets et séparez les valeurs multiples par des virgules. Compte IDs et OUs doit suivre le	DevOps ingénieur

Tâche	Description	Compétences requises
	schéma : `{{account_name}}:{{account_id}}` ou`{{ou_name}}:{{ou_id}}` . Si vous souhaitez attribuer des autorisations de manière récursive à Nested OUs, utilisez le modèle d'unité d'organisation avec un caractère générique à la fin. Exemple : `{{ou_name}}:{{ou_id}}:*` 4. Dans le `PrincipalType` paramètre, entrez le type de principal IAM Identity Center qui sera affecté par l'ensemble d'autorisations. Les valeurs valides sont `USER` ou `GROUP`. Cette valeur ne peut pas être modifiée après le déploiement. 5. Dans le `PrincipalID` paramètre, entrez le nom de l'utilisateur ou du groupe dans le magasin d'identités IAM Identity Center qui sera affecté par l'ensemble d'autorisations. Cette valeur ne peut pas être modifiée après le déploiement. 6. Dans le `PermissionSetName` paramètre, entrez le nom de l'ensembl	

Tâche	Description	Compétences requises
	e d'autorisations que vous souhaitez attribuer. 7. Répétez les étapes 2 à 6 pour créer autant d'assignations que nécessaire dans ce fichier. Il existe généralement une attribution pour chaque ensemble d'autorisations. Supprimez tous les exemples de devoirs qui ne sont pas obligatoires. 8. Enregistrez et fermez le fichier `iam-identitycenter-assignments.json` .	

Déployer les ensembles d'autorisations et les attributions

Tâche	Description	Compétences requises
Déployez des ressources dans le compte d'administrateur délégué d'IAM Identity Center.	1. Dans le compte d'administrateur délégué d'IAM Identity Center, ouvrez la AWS CloudFormation console. 2. Déployez le `iam-identitycenter-pipeline.yaml` modèle. Donnez un nom clair et descriptif à la pile et mettez à jour les paramètres comme indiqué. Pour obtenir des instructions, consultez la section	DevOps ingénieur

Tâche	Description	Compétences requises
	Création d'une pile dans la CloudFormation documentation.	
Déployez des ressources dans le compte AWS Organizations de gestion.	1. Connectez-vous au compte de gestion de l'organisation. 2. Ouvrez la AWS CloudFormation console. 3. Dans la barre de navigation, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la `us-east-1` région. Cette région est requise pour que la `MoveAccount` EventBridge règle puisse détecter les AWS CloudTrail événements associés aux changements d'organisation. 4. Déployez le `iam-identitycenter-organization` modèle. Donnez un nom clair et descriptif à la pile et mettez à jour les paramètres comme indiqué. Pour obtenir des instructions, consultez la section Création d'une pile dans la CloudFormation documentation.	DevOps ingénieur

Tâche	Description	Compétences requises
Terminez la configuration du référentiel distant.	Modifiez le statut de la AWS CodeConnections connexion de `PENDING` à`AVAILABLE` . Cette connexion a été créée lorsque vous avez déployé la CloudFormation pile. Pour obtenir des instructions, consultez la section Mettre à jour une connexion en attente dans la CodeConnections documentation.	DevOps ingénieur
Téléchargez des fichiers dans le référentiel distant.	Téléchargez tous les fichiers que vous avez téléchargés depuis le `aws-samples` référentiel et modifiés au cours des étapes précédent es vers le référentiel distant. Les modifications apportées à la `main` branche démarrent le pipeline, qui crée ou met à jour les ensembles d'autorisations et les attributions.	DevOps ingénieur

Mise à jour des ensembles d'autorisations et des attributions

Tâche	Description	Compétences requises
Mettez à jour les ensembles d'autorisations et les attributi ons.	Lorsque la EventBridge règle `MoveAccount` Amazon détecte des modifications apportées aux comptes de l'organisation, le CI/CD pipeline automatically starts	DevOps ingénieur

Tâche	Description	Compétences requises
	and updates the permission sets. For example, if you add an account to an OU specified in the assignments JSON file, then the CI/CD pipeline applique les autorisations définies au nouveau compte. Si vous souhaitez modifier les ensembles d'autorisations et les attributions déployés, mettez à jour les fichiers JSON, puis validez-les dans le référentiel distant. Notez les points suivants lorsque vous utilisez le pipeline CI/CD pour gérer des ensembles d'autorisations et des associations précédemm ent déployés : • Si vous modifiez le nom d'un ensemble d'autorisations, le pipeline CI/CD supprime le jeu d'autorisations d'origine et en crée un nouveau. • Ce pipeline gère uniquemen t les ensembles d'autoris ations dotés de cette `SSOPipeline:true` balise. • Vous pouvez avoir plusieurs ensembles d'autorisations et	

Tâche	Description	Compétences requises
	modèles d'attribution dans le même dossier du référentiel. • Si vous supprimez un modèle, le pipeline supprime l'attribution ou l'ensemble d'autorisations. • Si vous supprimez l'intégra lité d'un bloc JSON d'attribu tion, le pipeline supprime l'attribution d'IAM Identity Center. • Vous ne pouvez pas supprimer un ensemble d'autorisations attribué à un Compte AWS. Tout d'abord, vous devez annuler l'attribu tion de l'ensemble d'autoris ations.	

Résolution des problèmes

Problème	Solution
Erreurs d'accès refusé	Vérifiez que vous disposez des autorisations requises pour déployer les CloudFormation modèles et les ressources qui y sont définies. Pour plus d'informations, consultez la section Contrôle de l'accès dans la CloudFormation documentation.
Erreurs de pipeline lors de la phase de validatio n	Cette erreur apparaît en cas d'erreur dans l'ensemble d'autorisations ou les modèles d'attribution.

Problème	Solution
	1. Dans CodeBuild, consultez les détails de la version. 2. Dans le journal de génération, recherche z l'erreur de validation qui fournit plus d'informations sur la cause de l'échec de la génération. 3. Mettez à jour l'ensemble d'autorisations ou les modèles d'attribution, puis validez-les dans le référentiel. 4. Le pipeline CI/CD redémarre le projet. CodeBuild Surveillez l'état pour confirmer que l'erreur de validation est résolue.

Ressources connexes

- Ensembles d'autorisations (documentation IAM Identity Center)

Gérez les informations d'identification à l'aide d'AWS Secrets Manager

Créée par Durga Prasad Cheepuri (AWS)

Récapitulatif

Ce modèle vous explique comment utiliser AWS Secrets Manager pour récupérer dynamiquement les informations d'identification d'une base de données pour une application Java Spring.

Auparavant, lorsque vous créiez une application personnalisée récupérant les informations d'une base de données, vous deviez généralement intégrer les informations d'identification (le secret) nécessaires pour accéder à la base de données directement dans l'application. Au moment de changer les informations d'identification, vous avez dû investir du temps pour mettre à jour l'application afin d'utiliser les nouvelles informations d'identification, puis distribuer l'application mise à jour. Si plusieurs applications partageaient des informations d'identification et que vous ne mettiez pas à jour l'une d'entre elles, l'application échouerait. En raison de ce risque, de nombreux utilisateurs ont choisi de ne pas alterner régulièrement leurs informations d'identification, ce qui a effectivement substitué un risque à un autre.

Secrets Manager vous permet de remplacer les informations d'identification codées en dur dans votre code (y compris les mots de passe) par un appel d'API pour récupérer le secret par programmation. Cela permet de s'assurer que le secret ne peut pas être compromis par quelqu'un qui examine votre code, car le secret n'existe tout simplement pas. Vous pouvez également configurer Secrets Manager pour qu'il fasse automatiquement pivoter le secret selon un calendrier que vous spécifiez. Cela vous permet de remplacer les secrets à long terme par des secrets à court terme, ce qui contribue à réduire considérablement le risque de compromission. Pour plus d'informations, consultez la documentation d'AWS Secrets Manager.

Conditions préalables et limitations

Prérequis

- Un compte AWS avec accès à Secrets Manager
- Une application Java Spring

Architecture

Pile technologique source

- Une application Java Spring avec un code qui accède à une base de données, avec des informations d'identification de base de données gérées à partir du fichier application.properties.

Pile technologique cible

- Une application Java Spring avec un code qui accède à une base de données, avec des informations d'identification de base de données gérées dans Secrets Manager. Le fichier application.properties contient les secrets de Secrets Manager.

Intégration de Secrets Manager à une application

Outils

- Secrets Manager — AWS Secrets Manager est un service AWS qui facilite la gestion des secrets. Les secrets peuvent être des informations d'identification de base de données, des mots de passe, des clés d'API tierces et même un texte arbitraire. Vous pouvez stocker et contrôler l'accès à ces secrets de manière centralisée à l'aide de la console Secrets Manager, de l'interface de ligne de commande (CLI) de Secrets Manager ou de l'API Secrets Manager et. SDKs

Épopées

Enregistrer le secret dans Secrets Manager

Tâche	Description	Compétences requises
Stockez les informations d'identification de base de données sous forme de secret dans Secrets Manager.	Stockez les informations d'identification d'Amazon Relational Database Service (Amazon RDS) ou d'autres informations d'identification de base de données sous forme secrète dans Secrets Manager	Administrateur système

Tâche	Description	Compétences requises
	en suivant les étapes décrites dans la section Création d'un secret dans la documentation de Secrets Manager.	
Définissez les autorisations permettant à l'application Spring d'accéder à Secrets Manager.	Définissez les autorisations appropriées en fonction de la manière dont l'application Java Spring utilise Secrets Manager. Pour contrôler l'accès au secret, créez une politique basée sur les informations fournies dans la documentation de Secrets Manager, dans les sections Utilisation de politiques basées sur l'identité (politiques IAM) et ABAC pour Secrets Manager et Utilisation de politiques basées sur les ressources pour Secrets Manager. Suivez les étapes décrites dans la section Récupération de la valeur secrète de la documentation de Secrets Manager.	Administrateur système

Mettre à jour l'application Spring

Tâche	Description	Compétences requises
Ajoutez des dépendances JAR pour utiliser Secrets Manager.	Consultez la section Informations supplémentaires pour plus de détails.	Développeur Java

Tâche	Description	Compétences requises
Ajoutez les détails du secret à l'application Spring.	Mettez à jour le fichier application.properties avec le nom secret, les points de terminaison et la région AWS. Pour un exemple, consultez la section Informations supplémentaires.	Développeur Java
Mettez à jour le code de récupération des informations d'identification de la base de données en Java.	Dans l'application, mettez à jour le code Java qui récupère les informations d'identification de la base de données pour récupérer ces informations depuis Secrets Manager. Pour un exemple de code, consultez la section Informations supplémentaires.	Développeur Java

Ressources connexes

- Documentation d'AWS Secrets Manager
- Utilisation de politiques basées sur l'identité (politiques IAM) et d'ABAC pour Secrets Manager
- Utilisation de politiques basées sur les ressources pour Secrets Manager
- Exemple de code

Informations supplémentaires

Ajouter des dépendances JAR pour utiliser Secrets Manager

Maven :

```
<groupId>com.amazonaws</groupId>
    <artifactId>aws-java-sdk-secretsmanager</artifactId>
    <version>1.11. 355 </version>
```

Gradle :

```
compile group: 'com.amazonaws', name: 'aws-java-sdk-secretsmanager', version:
 '1.11.355'
```

Mise à jour du fichier application.properties avec les détails du secret

```
spring.aws.secretsmanager.secretName=postgres-local
spring.aws.secretsmanager.endpoint=secretsmanager.us-east-1.amazonaws.com
spring.aws.secretsmanager.region=us-east-1
```

Mise à jour du code de récupération des informations d'identification de la base de données en Java

```
String  secretName  =  env.getProperty("spring.aws.secretsmanager.secretName");
String  endpoints  =  env.getProperty("spring.aws.secretsmanager.endpoint");
String  AWS Region  =  env.getProperty("spring.aws.secretsmanager.region");
AwsClientBuilder.EndpointConfiguration  config  =  new
  AwsClientBuilder.EndpointConfiguration(endpoints, AWS Region);
AWSSecretsManagerClientBuilder  clientBuilder  =
  AWSSecretsManagerClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AWSSecretsManager  client  =  clientBuilder.build();

ObjectMapper  objectMapper  =  new  ObjectMapper();

JsonNode  secretsJson  =  null;

ByteBuffer  binarySecretData;

GetSecretValueRequest  getSecretValueRequest  =  new
  GetSecretValueRequest().withSecretId(secretName);

GetSecretValueResult  getSecretValueResponse  =  null;

try  {
     getSecretValueResponse  =  client.getSecretValue(getSecretValueRequest);
    }

catch  (ResourceNotFoundException  e)  {
     log.error("The requested secret "  +  secretName  +  " was not found");
    }
```

```
catch  (InvalidRequestException  e)  {
     log.error("The request was invalid due to: "  +  e.getMessage());
     }

catch  (InvalidParameterException  e)  {
     log.error("The request had invalid params: "  +  e.getMessage());
     }
if  (getSecretValueResponse  ==  null)  {
     return  null;
     }  // Decrypted secret using the associated KMS key // Depending on whether the
 secret was a string or binary, one of these fields will be populated


String secret = getSecretValueResponse.getSecretString();

if (secret != null) {
     try {
                secretsJson  =  objectMapper.readTree(secret);
          }

     catch  (IOException  e)  {
                log.error("Exception while retrieving secret values: "  +
  e.getMessage());
          }
}

else  {
     log.error("The Secret String returned is null");

     return null;

     }
     String  host  =  secretsJson.get("host").textValue();
     String  port  =  secretsJson.get("port").textValue();
     String  dbname  =  secretsJson.get("dbname").textValue();
     String  username  =  secretsJson.get("username").textValue();
     String  password  =  secretsJson.get("password").textValue();
}
```

Surveiller les ElastiCache clusters pour les groupes de sécurité

Créée par Susanne Kangnoh (AWS) et Archit Mathur (AWS)

Récapitulatif

Amazon ElastiCache est un service Amazon Web Services (AWS) qui fournit une solution de mise en cache performante, évolutive et rentable pour distribuer un stockage de données en mémoire ou un environnement de cache dans le cloud. Il extrait les données des magasins de données en mémoire à haut débit et à faible latence. Cette fonctionnalité en fait un choix populaire pour les cas d'utilisation en temps réel tels que la mise en cache, les magasins de sessions, les jeux, les services géo-spatiaux, les analyses en temps réel et les files d'attente. ElastiCache propose des magasins de données Redis et Memcached, qui fournissent tous deux des temps de réponse inférieurs à la milliseconde.

Un groupe de sécurité agit comme un pare-feu virtuel pour vos ElastiCache instances en contrôlant le trafic entrant et sortant. Les groupes de sécurité agissent au niveau de l'instance, et non au niveau du sous-réseau. Pour chaque groupe de sécurité, vous ajoutez un ensemble de règles qui contrôlent le trafic entrant vers les instances, et un ensemble distinct de règles qui contrôlent le trafic sortant. Vous pouvez définir des règles d'autorisation, mais pas de règles de refus.

Ce modèle fournit un contrôle de sécurité qui surveille les appels d'API et génère un événement dans Amazon CloudWatch Events sur les ModifyReplicationGroupopérations CreateReplicationGroupCreateCacheClusterModifyCacheCluster,, et. Cet événement appelle une AWS Lambda fonction qui exécute un script Python. La fonction obtient l'ID du groupe de réplication à partir de l'entrée JSON de l'événement et effectue les vérifications suivantes pour déterminer s'il existe une violation de sécurité :

- Vérifie si le groupe de sécurité du cluster correspond au groupe de sécurité configuré dans la fonction Lambda.
- Si le groupe de sécurité du cluster ne correspond pas, la fonction envoie un message de violation à l'adresse e-mail que vous fournissez, en utilisant une notification Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un AWS compte actif.
- Un bucket Amazon Simple Storage Service (Amazon S3) pour télécharger le code Lambda fourni.
- Adresse e-mail à laquelle vous souhaitez recevoir des notifications de violation.
- ElastiCache journalisation activée, pour accéder à tous les journaux de l'API.

Limites

- Ce contrôle de détection est régional et doit être déployé dans chacune des régions Région AWS que vous souhaitez surveiller.
- Le contrôle prend en charge les groupes de réplication qui s'exécutent dans un cloud privé virtuel (VPC).

Architecture

Architecture du flux de travail

Automatisation et mise à l'échelle

- Si vous l'utilisez AWS Organizations, vous pouvez l'utiliser AWS CloudFormation StackSetspour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

AWS services

- Amazon ElastiCache facilite la configuration, la gestion et le dimensionnement des environnements de cache en mémoire distribués dans le AWS Cloud. Il fournit un cache en mémoire performant, redimensionnable et économique, tout en éliminant la complexité associée au déploiement et à la gestion d'un environnement de cache distribué. ElastiCache fonctionne avec les moteurs Redis et Memcached.
- AWS CloudFormationvous aide à modéliser et à configurer vos AWS ressources, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs Comptes AWS et Régions AWS.

- Amazon CloudWatch Events fournit un flux en temps quasi réel d'événements système décrivant les modifications apportées aux AWS ressources. CloudWatch Events prend connaissance des changements opérationnels au fur et à mesure qu'ils se produisent et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état.
- AWS Lambdaest un service de calcul qui prend en charge l'exécution de code sans provisionnement ni gestion de serveurs. Lambda exécute votre code uniquement lorsque cela est nécessaire et passe automatiquement de quelques requêtes par jour à des milliers par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- Amazon Simple Notification Service (Amazon SNS) coordonne et gère l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Ce modèle inclut une pièce jointe contenant deux fichiers :

- `ElastiCacheAllowedSecurityGroup.zip`est un fichier compressé qui inclut le contrôle de sécurité (code Lambda).
- `ElastiCacheAllowedSecurityGroup.yml`est un CloudFormation modèle qui déploie le contrôle de sécurité.

Consultez la section Epics pour plus d'informations sur l'utilisation de ces fichiers.

Épopées

Déployez le contrôle de sécurité

Tâche	Description	Compétences requises
Téléchargez le code dans un compartiment S3.	Créez un nouveau compartiment S3 ou utilisez un compartiment S3 existant pour télécharger le `ElastiCac`	Architecte du cloud

Tâche	Description	Compétences requises
	`heAllowedSecurityGroup.zip` fichier joint (code Lambda). Ce compartiment doit se trouver dans le même compartiment Région AWS que les ressources que vous souhaitez évaluer.	
Déployez le CloudFormation modèle.	Ouvrez la CloudFormation console au même endroit Région AWS que le compartiment S3 et déployez le `ElastiCacheAllowedSecurityControl.yml` fichier fourni dans la pièce jointe. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou sélectionné dans le premier épisode épique. Ce compartiment S3 contient le fichier .zip pour le code Lambda et doit être Région AWS identique au modèle et à CloudFormation la ressource qui seront évalués.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda	Architecte du cloud

Tâche	Description	Compétences requises
	dans votre compartiment S3, sans barres obliques (par exemple, ou). `ElasticCacheAllowedSecurityGroup.zip controls/ElasticCacheAllowedSecurityGroup.zip`	
Indiquez une adresse e-mail.	Indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications de violation.	Architecte du cloud
Spécifiez un niveau de journalisation.	Spécifiez le niveau de journalisation et la verbosité. `Info`désigne des messages d'information détaillés sur la progression de l'application et ne doit être utilisé que pour le débogage. `Error`désigne les événements d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situations potentiellement dangereuses.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'abonnement par e-mail.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-	Architecte du cloud

Tâche	Description	Compétences requises
	mail que vous avez fournie. Pour recevoir des notificat ions, vous devez confirmer cet abonnement par e-mail.	

Ressources connexes

- Création d'une pile sur la AWS CloudFormation console (AWS CloudFormation documentation)
- Amazon VPCs et ElastiCache la sécurité (ElastiCache documentation Amazon)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Surveillez les clusters Amazon EMR pour le chiffrement en transit lors du lancement

Créée par Susanne Kangnoh (AWS)

Récapitulatif

Ce modèle fournit un contrôle de sécurité qui surveille les clusters Amazon EMR au lancement et envoie une alerte si le chiffrement en transit n'est pas activé.

Amazon EMR est un service Web qui vous permet d'exécuter facilement des frameworks de mégadonnées, tels qu'Apache Hadoop, pour traiter et analyser des données. Amazon EMR vous permet de traiter de grandes quantités de données de manière rentable en exécutant le mappage et en réduisant les étapes en parallèle.

Le chiffrement des données empêche les utilisateurs non autorisés d'accéder ou de lire des données au repos ou des données en transit. Les données au repos font référence aux données stockées sur des supports tels qu'un système de fichiers local sur chaque nœud, le système de fichiers distribué Hadoop (HDFS) ou le système de fichiers EMR (EMRFS) via Amazon Simple Storage Service (Amazon S3). Les données en transit font référence aux données qui circulent sur le réseau et qui circulent entre deux tâches. Le chiffrement en transit prend en charge les fonctionnalités de chiffrement open source pour Apache Spark, Apache TEZ, Apache Hadoop, Apache HBase et Presto. Vous activez le chiffrement en créant une configuration de sécurité à partir de l'interface de ligne de commande AWS (AWS CLI), de la console ou d' SDKsAWS, et en spécifiant les paramètres de chiffrement des données. Vous pouvez fournir les artefacts de chiffrement pour le chiffrement en transit de deux manières :

- En téléchargeant un fichier compressé de certificats sur Amazon S3.
- En faisant référence à une classe Java personnalisée qui fournit des artefacts de chiffrement.

Le contrôle de sécurité inclus dans ce modèle surveille les appels d'API et génère un événement Amazon CloudWatch Events sur l'RunJobFlowaction. L'événement appelle une fonction AWS Lambda, qui exécute un script Python. La fonction obtient l'ID du cluster EMR à partir de l'entrée JSON de l'événement et effectue les vérifications suivantes pour déterminer s'il existe une violation de sécurité :

- Vérifie si le cluster EMR possède une configuration de sécurité spécifique à Amazon EMR.

- Si le cluster possède une configuration de sécurité, vérifie si le chiffrement en transit est activé.
- Si le cluster n'a pas de configuration de sécurité, envoie une alerte à l'adresse e-mail que vous fournissez, en utilisant Amazon Simple Notification Service (Amazon SNS). La notification indique le nom du cluster EMR, les détails de la violation, les informations relatives à la région AWS et au compte, ainsi que l'ARN AWS Lambda (Amazon Resource Name) d'où provient la notification.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un compartiment S3 pour télécharger le code Lambda fourni avec ce modèle.
- Adresse e-mail à laquelle vous souhaitez recevoir des notifications de violation.
- La journalisation Amazon EMR est activée, pour accéder à tous les journaux d'API.

Limites

- Ce contrôle de détection est régional et doit être déployé dans chaque région AWS que vous souhaitez surveiller.

Versions du produit

- Amazon EMR version 4.8.0 ou ultérieure.

Architecture

Architecture du flux de travail

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer le modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- Amazon EMR — Amazon EMR est une plate-forme de cluster gérée qui simplifie l'exécution de frameworks de mégadonnées, tels qu'Apache Hadoop et Apache Spark, sur AWS afin de traiter et d'analyser de grandes quantités de données. Grâce à ces infrastructures et des projets open source connexes, vous pouvez traiter des données à des fins d'analytique et pour des charges de travail d'informatique décisionnelle. En outre, vous pouvez utiliser Amazon EMR pour transformer et déplacer de grandes quantités de données vers et depuis d'autres banques de données et bases de données AWS, tels qu'Amazon S3 et Amazon DynamoDB.
- AWS Cloudformation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.
- AWS Cloudwatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS. CloudWatch Events prend connaissance des changements opérationnels au fur et à mesure qu'ils se produisent et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute votre code uniquement lorsque cela est nécessaire et passe automatiquement de quelques requêtes par jour à des milliers par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.
- AWS SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Ce modèle inclut une pièce jointe contenant deux fichiers :

- `EMRInTransitEncryption.zip`est un fichier compressé qui inclut le contrôle de sécurité (code Lambda).
- `EMRInTransitEncryption.yml`est un CloudFormation modèle qui déploie le contrôle de sécurité.

Consultez la section Epics pour plus d'informations sur l'utilisation de ces fichiers.

Épopées

Déployez le contrôle de sécurité

Tâche	Description	Compétences requises
Téléchargez le code dans un compartiment S3.	Créez un nouveau compartiment S3 ou utilisez un compartiment S3 existant pour télécharger le `EMRInTransitEncryption.zip` fichier joint (code Lambda). Ce compartiment doit se trouver dans la même région AWS que le CloudFormation modèle et les ressources que vous souhaitez évaluer.	Architecte du cloud
Déployez le CloudFormation modèle.	Ouvrez la console Cloudformation dans la même région AWS que le compartiment S3 et déployez le `EMRInTransitEncryption.yml` fichier fourni dans la pièce jointe. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	Architecte du cloud,

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou sélectionné dans le premier épisode épique. Ce compartiment S3 contient le fichier .zip pour le code Lambda et doit se trouver dans la même région AWS que CloudFormation le modèle et la ressource qui seront évalués.	Architecte du cloud
Fournissez la clé S3.	Spécifiez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple, ou). `EMRInTransitEncryption.zip` `controls/EMRInTransitEncryption.zip`	Architecte du cloud
Indiquez une adresse e-mail.	Spécifiez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications de violation.	Architecte du cloud
Spécifiez un niveau de journalisation.	Spécifiez le niveau de journalisation et la verbosité des journaux Lambda. `Info`désigne des messages d'information détaillés sur la progression de l'application et ne doit être utilisé que pour le débogage. `Error`désigne les	Architecte du cloud

Tâche	Description	Compétences requises
	événements d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situations potentiellement dangereuses.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'abonnement par e-mail.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Pour recevoir des notifications, vous devez confirmer cet abonnement par e-mail.	Architecte du cloud

Ressources connexes

- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Options de chiffrement (documentation Amazon EMR)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Surveillez les ElastiCache clusters Amazon pour le chiffrement au repos

Créée par Susanne Kangnoh (AWS)

Récapitulatif

Amazon ElastiCache est un service Amazon Web Services (AWS) qui fournit une solution de mise en cache performante, évolutive et rentable pour distribuer un stockage de données en mémoire ou un environnement de cache dans le cloud. Il extrait les données des magasins de données en mémoire à haut débit et à faible latence. Cette fonctionnalité en fait un choix populaire pour les cas d'utilisation en temps réel tels que la mise en cache, les magasins de sessions, les jeux, les services géospatiaux, les analyses en temps réel et les files d'attente. ElastiCache propose des magasins de données Redis et Memcached, qui fournissent tous deux des temps de réponse inférieurs à la milliseconde.

Le chiffrement des données permet d'empêcher les utilisateurs non autorisés de lire les données sensibles disponibles sur vos clusters Redis et leurs systèmes de stockage en cache associés. Cela inclut les données enregistrées sur un support persistant, appelées données au repos, et les données susceptibles d'être interceptées lorsqu'elles transitent par le réseau entre les clients et les serveurs de cache, appelées données en transit.

Vous pouvez activer le chiffrement au repos ElastiCache pour Redis lorsque vous créez un groupe de réplication, en définissant le AtRestEncryptionEnabledparamètre sur true. Lorsque ce paramètre est activé, il chiffre le disque pendant les opérations de synchronisation, de sauvegarde et de swap, et chiffre les sauvegardes stockées dans Amazon Simple Storage Service (Amazon S3). Vous ne pouvez pas activer le chiffrement au repos sur un groupe de réplication existant. Lorsque vous créez un groupe de réplication, vous pouvez activer le chiffrement au repos de deux manières :

- En choisissant l'option Par défaut, qui utilise le chiffrement géré par le service au repos.
- En utilisant une clé gérée par le client et en fournissant l'ID de clé ou le nom de ressource Amazon (ARN) fourni par AWS Key Management Service (AWS KMS).

Ce modèle fournit un contrôle de sécurité qui surveille les appels d'API et génère un événement Amazon CloudWatch Events lors de l'CreateReplicationGroupopération. Cet événement appelle une fonction AWS Lambda, qui exécute un script Python. La fonction obtient l'ID du groupe de réplication

à partir de l'entrée JSON de l'événement et effectue les vérifications suivantes pour déterminer s'il existe une violation de sécurité :

- Vérifie si la AtRestEncryptionEnabledclé existe.
- S'AtRestEncryptionEnabledil existe, vérifie la valeur pour voir si elle est vraie.
- Si la AtRestEncryptionEnabledvaleur est définie sur false, définit une variable qui suit les violations et envoie un message de violation à l'adresse e-mail que vous fournissez, en utilisant une notification Amazon Simple Notification Service (Amazon SNS).

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Un compartiment S3 pour télécharger le code Lambda fourni.
- Adresse e-mail à laquelle vous souhaitez recevoir des notifications de violation.
- ElastiCache journalisation activée, pour accéder à tous les journaux de l'API.

Limites

- Ce contrôle de détection est régional et doit être déployé dans chaque région AWS que vous souhaitez surveiller.
- Le contrôle prend en charge les groupes de réplication qui s'exécutent dans un cloud privé virtuel (VPC).
- Le contrôle prend en charge les groupes de réplication qui exécutent les types de nœuds suivants :
  - R5, R4, R3
  - M5, M4, M3
  - T3, T2

Versions du produit

- ElastiCache pour Redis version 3.2.6 ou ultérieure

Architecture

Architecture du flux de travail

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- Amazon ElastiCache — Amazon ElastiCache facilite la configuration, la gestion et le dimensionnement d'environnements de cache en mémoire distribués dans le cloud AWS. Il fournit un cache en mémoire performant, redimensionnable et économique, tout en éliminant la complexité associée au déploiement et à la gestion d'un environnement de cache distribué. ElastiCache fonctionne avec les moteurs Redis et Memcached.
- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Vous pouvez gérer et approvisionner des piles sur plusieurs comptes AWS et régions AWS.
- AWS Cloudwatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS. CloudWatch Events prend connaissance des changements opérationnels au fur et à mesure qu'ils se produisent et prend les mesures correctives nécessaires, en envoyant des messages pour répondre à l'environnement, en activant des fonctions, en apportant des modifications et en capturant des informations d'état.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute votre code uniquement lorsque cela est nécessaire et passe automatiquement de quelques requêtes par jour à des milliers par seconde. Vous payez uniquement le temps de calcul que vous utilisez. Vous n'exposez aucuns frais quand votre code n'est pas exécuté.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Ce modèle inclut une pièce jointe contenant deux fichiers :

- `ElasticCache-EncryptionAtRest.zip`est un fichier compressé qui inclut le contrôle de sécurité (code Lambda).
- `elasticache_encryption_at_rest.yml`est un CloudFormation modèle qui déploie le contrôle de sécurité.

Consultez la section Epics pour plus d'informations sur l'utilisation de ces fichiers.

Épopées

Déployez le contrôle de sécurité

Tâche	Description	Compétences requises
Téléchargez le code dans un compartiment S3.	Créez un nouveau compartiment S3 ou utilisez un compartiment S3 existant pour télécharger le `ElastiCache-EncryptionAtRest.zip` fichier joint (code Lambda). Ce compartiment doit se trouver dans la même région AWS que les ressources que vous souhaitez évaluer.	Architecte du cloud
Déployez le CloudFormation modèle.	Ouvrez la console Cloudformation dans la même région AWS que le compartiment S3 et déployez le `elasticac`	Architecte du cloud

Tâche	Description	Compétences requises
	`he_encryption_at_rest.yml` fichier fourni dans la pièce jointe. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou sélectionné dans le premier épisode épique. Ce compartiment S3 contient le fichier .zip pour le code Lambda et doit se trouver dans la même région AWS que CloudFormation le modèle et la ressource qui seront évalués.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple, ou). `ElasticCache-EncryptionAtRest.zip` `controls/ElasticCache-EncryptionAtRest.zip`	Architecte du cloud
Indiquez une adresse e-mail.	Indiquez une adresse e-mail active à laquelle vous	Architecte du cloud

Tâche	Description	Compétences requises
	souhaitez recevoir des notifications de violation.	
Spécifiez un niveau de journalisation.	Spécifiez le niveau de journalisation et la verbosité. `Info`désigne des messages d'information détaillés sur la progression de l'application et ne doit être utilisé que pour le débogage. `Error`désigne les événements d'erreur susceptib les de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez l'abonnement par e-mail.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Pour recevoir des notificat ions, vous devez confirmer cet abonnement par e-mail.	Architecte du cloud

Ressources connexes

- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Chiffrement au repos dans ElastiCache Redis (documentation Amazon ElastiCache)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Surveillez les paires de clés d' EC2 instance à l'aide d'AWS Config

Créée par Wassim Benhallam (AWS), Sergio Bilbao Lopez (AWS) et Vikrant Telkar (AWS)

Récapitulatif

Lors du lancement d'une instance Amazon Elastic Compute Cloud (Amazon EC2) sur le cloud Amazon Web Services (AWS), il est recommandé de créer ou d'utiliser une paire de clés existante pour se connecter à l'instance. La paire de clés, composée d'une clé publique stockée dans l'instance et d'une clé privée fournie à l'utilisateur, permet un accès sécurisé via Secure Shell (SSH) à l'instance et évite l'utilisation de mots de passe. Cependant, les utilisateurs peuvent parfois lancer des instances par inadvertance sans attacher de paire de clés. Les paires de clés ne pouvant être attribuées que lors du lancement d'une instance, il est important d'identifier rapidement et de signaler comme non conforme les instances lancées sans paires de clés. Cela est particulièrement utile lorsque vous travaillez dans des comptes ou des environnements qui nécessitent l'utilisation de paires de clés, par exemple l'accès.

Ce modèle décrit comment créer une règle personnalisée dans AWS Config pour surveiller les paires de clés d' EC2 instance. Lorsque des instances sont identifiées comme non conformes, une alerte est envoyée à l'aide des notifications Amazon Simple Notification Service (Amazon SNS) initiées par le biais d'un événement Amazon. EventBridge

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- AWS Config est activé pour la région AWS que vous souhaitez surveiller et configuré pour enregistrer toutes les ressources AWS

Limites

- Cette solution est spécifique à chaque région. Toutes les ressources doivent être créées dans la même région AWS.

Architecture

Pile technologique cible

- AWS Config
- Amazon EventBridge
- AWS Lambda
- Amazon SNS

Architecture cible

1. AWS Config initie la règle.
2. La règle invoque la fonction Lambda pour évaluer la conformité EC2 des instances.
3. La fonction Lambda envoie l'état de conformité mis à jour à AWS Config.
4. AWS Config envoie un événement à EventBridge.
5. EventBridge publie des notifications de modification de conformité dans une rubrique SNS.
6. Amazon SNS envoie une alerte par e-mail.

Automatisation et évolutivité

La solution peut surveiller un nombre illimité d' EC2 instances au sein d'une région.

Outils

Outils

- AWS Config — AWS Config est un service qui vous permet d'évaluer, d'auditer et d'évaluer les configurations de vos ressources AWS. AWS Config surveille et enregistre en permanence les configurations de vos ressources AWS et vous permet d'automatiser l'évaluation des configurations enregistrées par rapport aux configurations souhaitées.
- Amazon EventBridge — Amazon EventBridge est un service de bus d'événements sans serveur permettant de connecter vos applications à des données provenant de diverses sources.
- AWS Lambda — AWS Lambda est un service de calcul sans serveur qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs, créer une logique de dimensionnement des clusters adaptée à la charge de travail, gérer les intégrations d'événements ou gérer les temps d'exécution.

- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service de messagerie entièrement géré pour les communications (A2A) application-to-application et (A2P). application-to-person

Code

Le code de la fonction Lambda est joint.

Épopées

Créez une fonction Lambda pour évaluer la conformité d'Amazon EC2

Tâche	Description	Compétences requises
Créez un rôle AWS Identity and Access Management (IAM) pour Lambda.	Sur la console de gestion AWS, choisissez IAM, puis créez le rôle en utilisant Lambda comme entité de confiance et en ajoutant `AmazonEventBridgeFullAccess` les `AWSConfigRulesExecutionRole` autorisations et. Pour plus d'informations, consultez la documentation AWS.	DevOps
Créez et déployez la fonction Lambda.	1. Sur la console Lambda, créez une fonction en utilisant Author from scratch, avec Python 3.6 comme moteur d'exécution et le rôle IAM créé précédemment. Notez l'Amazon Resource Name (ARN).	DevOps

Tâche	Description	Compétences requises
	2. Dans l'onglet Code`lambda_function.py`, choisissez et collez le code associé à ce modèle. 3. Pour enregistrer vos modifications, choisissez Déployer.	

Création d'une règle AWS Config personnalisée

Tâche	Description	Compétences requises
Ajoutez une règle AWS Config personnalisée.	Sur la console AWS Config, ajoutez une règle personnalisée à l'aide des paramètres suivants : • ARN — L'ARN de la fonction Lambda créée précédemment • Type de déclencheur : modifications de configuration • Portée des modifications — Ressources • Type de ressource : EC2 instance Amazon Pour plus d'informations, consultez la documentation AWS.	DevOps

Configurer les notifications par e-mail lorsqu'un événement de changement de conformité est détecté

Tâche	Description	Compétences requises
Créez le sujet et l'abonnement SNS.	Sur la console Amazon SNS, créez un sujet en utilisant le type Standard, puis créez un abonnement en utilisant le protocole Email comme protocole. Lorsque vous recevez le message électronique de confirmation, cliquez sur le lien pour confirmer l'abonnement. Pour plus d'informations, consultez la documentation AWS.	DevOps
Créez une EventBridge règle pour lancer les notifications Amazon SNS.	Sur la EventBridge console, créez une règle à l'aide des paramètres suivants : • Nom du service — AWS Config • Type d'événement : modification de la conformité aux règles de configuration • Type de message : types de messages spécifiques, ComplianceChangeNotification • Nom de règle spécifique : nom de votre règle AWS Config créée précédemment	DevOps

Tâche	Description	Compétences requises
	• Cible : sujet SNS, sujet que vous avez créé précédemment Pour plus d'informations, consultez la documentation AWS.	

Vérifiez la règle et les notifications

Tâche	Description	Compétences requises
Créez des EC2 instances.	Créez deux EC2 instances de n'importe quel type et attachez une paire de clés, puis créez une EC2 instance sans paire de clés.	DevOps
Vérifiez la règle.	1. Sur la console AWS Config, sur la page Règles, sélectionnez votre règle. 2. Pour voir les EC2 instances conformes et non conformes, remplacez Resources in scope par All. Vérifiez que deux instances sont répertoriées comme conformes et qu'une instance est répertoriée comme non conforme. 3. Attendez de recevoir la notification par e-mail d'Amazon SNS concernan	DevOps

Tâche	Description	Compétences requises
	t l'état de conformité des EC2 instances.	

Ressources connexes

- Création d'un rôle pour la délégation d'autorisations à un service AWS
- Création d'une règle personnalisée dans AWS Config
- Création d'une rubrique Amazon SNS
- Abonnement à une rubrique Amazon SNS
- Création d'une règle dans Amazon EventBridge

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Surveiller l'activité de l'utilisateur root IAM

Créée par Mostefa Brougui (AWS)

Récapitulatif

Chaque compte Amazon Web Services (AWS) possède un utilisateur root. En tant que bonne pratique de sécurité pour AWS Identity and Access Management (IAM), nous vous recommandons d'utiliser l'utilisateur root pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète, consultez la section Tâches nécessitant des informations d'identification de l'utilisateur root dans le guide de référence de gestion des comptes AWS. Étant donné que l'utilisateur root dispose d'un accès complet à toutes vos ressources AWS et à vos informations de facturation, nous vous recommandons de ne pas utiliser ce compte et de le surveiller pour détecter toute activité susceptible d'indiquer que les informations d'identification de l'utilisateur root ont été compromises.

À l'aide de ce modèle, vous configurez une architecture axée sur les événements qui surveille l'utilisateur root IAM. Ce modèle met en place une hub-and-spoke solution qui surveille plusieurs comptes AWS, les comptes Spoke, et centralise la gestion et les rapports dans un seul compte, le compte hub.

Lorsque les informations d'identification de l'utilisateur root IAM sont utilisées, Amazon CloudWatch et AWS CloudTrail enregistrent l'activité dans le journal et dans le journal, respectivement. Dans le compte Spoke, une EventBridge règle Amazon envoie l'événement au bus d'événements central du compte hub. Dans le compte du hub, une EventBridge règle envoie l'événement à une fonction AWS Lambda. La fonction utilise une rubrique Amazon Simple Notification Service (Amazon SNS) qui vous informe de l'activité de l'utilisateur root.

Dans ce modèle, vous utilisez un CloudFormation modèle AWS pour déployer les services de surveillance et de gestion des événements dans les comptes Spoke. Vous utilisez un modèle HashiCorp Terraform pour déployer les services de gestion des événements et de notification dans le compte du hub.

Conditions préalables et limitations

Prérequis

1. Autorisations pour déployer des ressources AWS dans votre environnement AWS.

2. Autorisations pour déployer des ensembles de CloudFormation piles. Pour plus d'informations, consultez la section Conditions requises pour les opérations relatives aux ensembles de piles (CloudFormation documentation).
3. Terraform installé et prêt à l'emploi. Pour plus d'informations, consultez Get Started — AWS (documentation Terraform).
4. Une trace existante dans chaque compte Spoke. Pour plus d'informations, consultez Getting started with AWS CloudTrail (CloudTrail documentation).
5. Le journal est configuré pour envoyer des événements à CloudWatch Logs. Pour plus d'informations, consultez la section Envoi d'événements aux CloudWatch journaux (CloudTrail documentation).
6. Vos comptes hub et spoke doivent être gérés par AWS Organizations.

Architecture

Le schéma suivant illustre les éléments de base de la mise en œuvre.

1. Lorsque les informations d'identification de l'utilisateur root IAM sont utilisées, CloudWatch CloudTrail enregistrez l'activité dans le journal et dans le journal, respectivement.
2. Dans le compte Spoke, une EventBridge règle envoie l'événement au bus d'événements central du compte hub.
3. Dans le compte du hub, une EventBridge règle envoie l'événement à une fonction Lambda.
4. La fonction Lambda utilise une rubrique Amazon SNS qui vous informe de l'activité de l'utilisateur root.

Outils

Services AWS

- AWS vous CloudFormation aide à configurer les ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie sur l'ensemble des comptes et des régions AWS.
- AWS vous CloudTrail aide à auditer la gouvernance, la conformité et le risque opérationnel de votre compte AWS.

- Amazon CloudWatch Logs vous aide à centraliser les journaux de tous vos systèmes, applications et services AWS afin que vous puissiez les surveiller et les archiver en toute sécurité.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, les fonctions AWS Lambda, les points de terminaison d'appel HTTP utilisant des destinations d'API ou les bus d'événements dans d'autres comptes AWS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à approvisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- Amazon Simple Notification Service (Amazon SNS) vous aide à coordonner et à gérer l'échange de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Autres outils et services

- Terraform est une application CLI permettant de provisionner et de gérer l'infrastructure et les ressources cloud à l'aide de code, sous forme de fichiers de configuration.

Référentiel de code

Le code source et les modèles de ce modèle sont disponibles dans un GitHub référentiel. Ce modèle fournit deux modèles :

- Un modèle Terraform contenant les ressources que vous déployez dans le compte du hub
- Un CloudFormation modèle que vous déployez en tant qu'instance stack set dans les comptes Spoke

La structure globale du référentiel est la suivante.

```
.
 |__README.md
 |__spoke-stackset.yaml
 |__hub.tf
 |__root-activity-monitor-module
```

```
    |__main.tf  # contains Terraform code to deploy resources in the Hub account
    |__iam      # contains IAM policies JSON files
        |__ lambda-assume-policy.json          # contains trust policy of the IAM role
used by the Lambda function
        |__ lambda-policy.json                 # contains the IAM policy attached to
the IAM role used by the Lambda function
    |__outputs  # contains Lambda function zip code
```

La section Epics fournit des step-by-step instructions pour déployer les modèles.

Épopées

Déployer des ressources sur le compte du hub

Tâche	Description	Compétences requises
Clonez le référentiel d'exemples de code.	1. Ouvrez le référentiel AWS IAM Root User Activity Monitor. 2. Dans l'onglet Code, au-dessus de la liste des fichiers, choisissez Code, puis copiez l'URL HTTPS. 3. Dans une interface de ligne de commande, remplacez votre répertoire de travail par l'emplacement où vous souhaitez stocker les fichiers d'exemple. 4. Entrez la commande suivante : `git clone <repoURL>`	AWS général
Mettez à jour le modèle Terraform.	1. Récupérez l'identifiant de votre organisation. Pour obtenir des instructions, consultez la section	AWS général

Tâche	Description	Compétences requises
	Affichage des informations relatives à une organisation depuis le compte de gestion (documentation AWS Organizations). 2. Dans le référentiel cloné, ouvrez `hub.tf`. 3. Mettez à jour les éléments suivants avec les valeurs appropriées pour votre environnement : • `OrganizationId` — Ajoutez l'identifiant de votre organisation. • `SNSTopicName` — Ajoutez un nom à la rubrique Amazon SNS. • `SNSSubscriptions` — Ajoutez l'adresse e-mail à laquelle les notifications Amazon SNS doivent être envoyées. • `Region`— Ajoutez le code de région AWS dans lequel vous déployez les ressources. Par exemple, `eu-west-1` . • `Tags`— Ajoutez vos tags. Pour plus d'informations, consultez la section Balisage des ressources	

Tâche	Description	Compétences requises
	AWS (référence générale AWS). 4. Enregistrez et fermez le fichier `hub.tf`.	

Déployez les ressources sur le compte du hub AWS.	1. Dans l'interface de ligne de commande Terraform , accédez au dossier racine du référentiel cloné, puis entrez la commande suivante.
	`terraform init && terraform plan`
	2. Passez en revue le résultat et confirmez que vous souhaitez créer les ressources décrites.
	3. Entrez la commande suivante.
	`terraform apply`
	4. Lorsque vous y êtes invité, confirmez le déploiement en entrant `yes`.
		AWS général

Déployez des ressources sur vos comptes Spoke

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	1. Connectez-vous à l'AWS Management Console	AWS général

Tâche	Description	Compétences requises
	et ouvrez la console CloudFormation . 2. Dans le volet de navigation, choisissez StackSets. 3. En haut de la StackSets page, choisissez Create StackSet. 4. Sous Autorisations, choisissez Autorisations gérées par le service. CloudFormation configure automatiquement les autorisations requises pour le déploiement sur les comptes cibles gérés par AWS Organizations. 5. Sous Prérequis - Préparer le modèle, sélectionnez Le modèle est prêt. 6. Sous Spécifier le modèle, choisissez Télécharger un fichier modèle. 7. Choisissez Choisir un fichier, puis dans le référentiel cloné, sélectionnez`spoke-stackset.yaml` . 8. Choisissez Suivant. 9. Sur la page Spécifier StackSet les détails, entrez le nom de l'ensemble de piles.	

Tâche	Description	Compétences requises
	10. Sous Paramètres, entrez l'ID du compte du hub, puis choisissez Next. 11. Sur la page Configurer StackSet les options, sous Balises, ajoutez vos balises. 12. Sous Configuration de l'exécution, choisissez Inactif, puis Next. 13. Sur la page Définir les options de déploiement, spécifiez les unités organisationnelles et les régions dans lesquelles vous souhaitez déployer le stack set, puis choisissez Next. 14. Sur la page de révision, sélectionnez Je reconnais qu'AWS est CloudFormation susceptible de créer des ressources IAM, puis choisissez Soumettre. CloudFormation commence à déployer votre stack set. Pour plus d'informations et d'instructions, voir Création d'un ensemble de piles (CloudFormation documentation).	

(Facultatif) Testez les notifications

Tâche	Description	Compétences requises
Utilisez les informations d'identification de l'utilisateur root.	1. Connectez-vous à un compte Spoke ou au compte Hub à l'aide des informations d'identification de l'utilisateur root. 2. Vérifiez que le compte e-mail que vous avez spécifié reçoit la notification Amazon SNS.	AWS général

Ressources connexes

- Bonnes pratiques en matière de sécurité (documentation IAM)
- Travailler avec StackSets (CloudFormation documentation)
- Commencer (documentation Terraform)

Informations supplémentaires

Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les journaux afin d'identifier les activités inattendues et potentiellement non autorisées dans votre environnement AWS. Comme alternative à cette solution, si vous l'avez activée GuardDuty, elle peut vous avertir lorsque les informations d'identification de l'utilisateur root ont été utilisées. Le GuardDuty résultat est`Policy:IAMUser/RootCredentialUsage`, et la gravité par défaut est faible. Pour plus d'informations, consultez Gérer les GuardDuty résultats d'Amazon.

Envoyer une notification lorsqu'un utilisateur IAM est créé

Créée par Mansi Suratwala (AWS) et Sergiy Shevchenko (AWS)

Récapitulatif

Sur Amazon Web Services (AWS), vous pouvez utiliser ce modèle pour déployer un CloudFormation modèle AWS afin de recevoir automatiquement des notifications lorsque des utilisateurs AWS Identity and Access Management (IAM) sont créés.

Grâce à IAM, vous pouvez gérer l'accès aux services et aux ressources AWS en toute sécurité. Vous pouvez créer et gérer des utilisateurs et des groupes AWS, et utiliser des autorisations pour autoriser ou refuser à ces utilisateurs et groupes l'accès aux ressources AWS.

Le CloudFormation modèle crée un événement Amazon CloudWatch Events et une fonction AWS Lambda. L'événement utilise AWS CloudTrail pour surveiller la présence de tout utilisateur IAM créé dans le compte AWS. Si un utilisateur est créé, l'événement CloudWatch Events lance une fonction Lambda, qui vous envoie une notification Amazon Simple Notification Service (Amazon SNS) vous informant de l'événement de création du nouvel utilisateur.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif
- Création et déploiement d'une CloudTrail piste AWS

Limites

- Le CloudFormation modèle AWS doit être déployé `CreateUser` uniquement pour.

Architecture

Pile technologique cible

- IAM
- AWS CloudTrail

- CloudWatch Événements Amazon
- AWS Lambda
- Amazon Simple Storage Service (Amazon S3)
- Amazon SNS

Architecture cible

Automatisation et mise à l'échelle

Vous pouvez utiliser le CloudFormation modèle AWS à plusieurs reprises pour différents comptes et régions AWS. Vous ne devez l'exécuter qu'une seule fois dans chaque région ou compte. Pour automatiser le déploiement sur plusieurs comptes, utilisez AWS CloudFormation StackSets. Le CloudFormation modèle sera en mesure de déployer toutes les ressources requises dans chaque compte.

Outils

Outils

- IAM — AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux ressources AWS. Vous pouvez utiliser IAM pour contrôler les personnes qui s’authentifient (sont connectées) et sont autorisées (disposent d’autorisations) à utiliser des ressources.
- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources Amazon Web Services afin que vous puissiez passer moins de temps à gérer ces ressources et plus de temps à vous concentrer sur vos applications exécutées sur AWS. Vous créez un modèle qui décrit toutes les ressources AWS que vous souhaitez, et vous vous CloudFormation occupez du provisionnement et de la configuration de ces ressources pour vous.
- AWS CloudTrail — AWS vous CloudTrail aide à gérer la gouvernance, la conformité, ainsi que l'audit opérationnel et des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail. Les événements incluent les actions entreprises dans la console de gestion AWS, l'interface de ligne de commande AWS et AWS SDKs et APIs.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un near-real-time flux d'événements système décrivant les modifications apportées aux ressources AWS.

- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage pour Internet. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service géré qui fournit des messages via Lambda, HTTP, e-mail, notifications push mobiles et messages texte (SMS) mobiles.

Code

Un fichier .zip du projet est disponible en pièce jointe.

Épopées

Créez le compartiment S3 pour le script Lambda

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Ouvrez la console Amazon S3 et choisissez ou créez un compartiment S3. Ce compartiment S3 hébergera le fichier .zip du code Lambda. Le nom du compartiment S3 ne peut pas contenir de barres obliques en tête.	Architecte du cloud

Téléchargez le code Lambda dans le compartiment S3

Tâche	Description	Compétences requises
Téléchargez le code Lambda.	Téléchargez le fichier .zip de code Lambda fourni dans la	Architecte du cloud

Tâche	Description	Compétences requises
	section Pièces jointes dans le compartiment S3 que vous avez défini.	

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle.	Sur la CloudFormation console, déployez le CloudFormation `createIAMuser.yaml` modèle fourni en pièce jointe à ce modèle. Dans l'épopée suivante, fournissez des valeurs pour les paramètres du modèle.	Architecte du cloud

Complétez les paramètres dans le CloudFormation modèle

Tâche	Description	Compétences requises
Indiquez le nom du compartiment S3.	Entrez le nom du compartiment S3 que vous avez créé ou choisi dans le premier épisode épique.	Architecte du cloud
Fournissez la clé S3.	Indiquez l'emplacement du fichier .zip de code Lambda dans votre compartiment S3, sans barres obliques (par exemple,). `<directory>/<file-name>.zip`	Architecte du cloud

Tâche	Description	Compétences requises
Indiquez une adresse e-mail.	Fournissez une adresse e-mail active pour recevoir les notifications Amazon SNS.	Architecte du cloud
Définissez le niveau de journalisation.	Définissez le niveau et la fréquence de journalisation pour votre fonction Lambda. `Info`désigne des messages d'information détaillés sur l'état d'avancement de l'application. `Error`désigne les événement s d'erreur susceptibles de permettre à l'application de continuer à fonctionner. `Warning`désigne les situation s potentiellement dangereus es.	Architecte du cloud

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail fournie. Pour recevoir des notifications, vous devez confirmer cet abonnement par e-mail.	Architecte du cloud

Ressources connexes

- Création d’un journal de suivi

- Création d'un compartiment S3
- Téléchargement de fichiers dans un compartiment S3
- Déploiement d'un CloudFormation modèle
- Création d'un utilisateur IAM
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Empêchez l'accès à Internet au niveau du compte en utilisant une politique de contrôle des services

Créée par Sergiy Shevchenko (AWS), Sean O'Sullivan (AWS) et Victor Mazeo Whitaker (AWS)

Récapitulatif

Organisations souhaitent souvent limiter l'accès à Internet pour les ressources du compte qui doivent rester privées. Dans ces comptes, les ressources des clouds privés virtuels (VPCs) ne doivent en aucun cas accéder à Internet. De nombreuses organisations optent pour une architecture d'inspection centralisée. Pour le trafic est-ouest (VPC à VPC) dans une architecture d'inspection centralisée, vous devez vous assurer que les comptes parlés et leurs ressources n'ont pas accès à Internet. Pour le trafic nord-sud (sortie Internet et sur site), vous souhaitez autoriser l'accès à Internet uniquement via le VPC d'inspection.

Ce modèle utilise une politique de contrôle des services (SCP) pour empêcher l'accès à Internet. Vous pouvez appliquer ce SCP au niveau du compte ou de l'unité organisationnelle (UO). Le SCP limite la connectivité Internet en empêchant ce qui suit :

- Création ou connexion d'une IPv4 passerelle IPv6 Internet permettant un accès Internet direct au VPC
- Création ou acceptation d'une connexion d'appairage VPC susceptible de permettre un accès indirect à Internet via un autre VPC
- Création ou mise à jour d'une AWS Global Acceleratorconfiguration susceptible d'autoriser un accès Internet direct aux ressources VPC

Conditions préalables et limitations

Prérequis

- Une ou plusieurs Comptes AWS sont gérées en tant qu'organisation dans AWS Organizations.
- Toutes les fonctionnalités sont activées dans AWS Organizations.
- SCPs sont activés dans l'organisation.
- Autorisations pour :
  - Accédez au compte de gestion de l'organisation.

- Créez SCPs. Pour plus d'informations sur les autorisations minimales, voir Création d'un SCP.
- Associez le SCP aux comptes ou unités organisationnelles cibles (OUs). Pour plus d'informations sur les autorisations minimales, consultez la section Attacher et détacher des politiques de contrôle des services.

Limites

- SCPs n'affectent pas les utilisateurs ni les rôles dans le compte de gestion. Elles affectent uniquement les comptes membres de votre organisation.
- SCPs concernent uniquement les utilisateurs AWS Identity and Access Management (IAM) et les rôles gérés par des comptes faisant partie de l'organisation. Pour de plus amples informations, veuillez consulter Effets des SCP sur les autorisations.

Outils

Services AWS

- AWS Organizationsest un service de gestion de comptes qui vous aide à Comptes AWS en regrouper plusieurs au sein d'une organisation que vous créez et gérez de manière centralisée. Dans ce modèle, vous utilisez les politiques de contrôle des services (SCPs) dans AWS Organizations.
- Amazon Virtual Private Cloud (Amazon VPC) vous aide à lancer AWS des ressources dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d' AWS.

Bonnes pratiques

Après avoir mis en place ce SCP dans votre organisation, assurez-vous de le mettre à jour fréquemment pour tenir compte de toute nouvelle Services AWS fonctionnalité susceptible d'affecter l'accès à Internet.

Épopées

Créez et attachez le SCP

Tâche	Description	Compétences requises
Créez le SCP.	1. Connectez-vous à la console AWS Organizations. Vous devez vous connecter au compte de gestion de l'organisation. 2. Dans le volet de gauche, choisissez Policies. 3. Sur la page des politiques, choisissez Politiques de contrôle des services. 4. Sur la page Politiques de contrôle des services, choisissez Créer une politique. 5. Sur la page Créer une nouvelle politique de contrôle des services, entrez le nom de la politique et une description de la politique facultative. 6. (Facultatif) Ajoutez des AWS balises à votre politique. 7. Dans l'éditeur JSON, supprimez la politique d'espace réservé. 8. Collez le politique suivante dans l'éditeur JSON. `{`	Administrateur AWS

Tâche	Description	Compétences requises

	<pre>{
	  "Version":
	 "2012-10-17",
	  "Statement": [
	  {
	  "Action": [
	  "ec2:Atta
	chInternetGateway",
	  "ec2:Crea
	teInternetGateway",
	
	  "ec2:Crea
	teVpcPeeringConnec
	tion",
	  "ec2:Acce
	ptVpcPeeringConnec
	tion",
	  "ec2:Crea
	teEgressOnlyIntern
	etGateway"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  },
	  {
	  "Action": [
	  "globalac
	celerator:Create*",
	  "globalac
	celerator:Update*"
	  ],
	  "Resource":
	 "*",
	  "Effect": "Deny"
	  }
	  ]
	}</pre>
	9. Choisissez Create Policy (Créer une politique).	

Tâche	Description	Compétences requises
Fixez le SCP.	1. Sur la page Politiques de contrôle des services, choisissez la politique que vous avez créée. 2. Dans l'onglet Cibles, choisissez Attacher. 3. Sélectionnez l'unité d'organisation ou le compte auquel vous souhaitez associer la politique. Vous devrez peut-être développe r le pour OUs trouver l'unité d'organisation ou le compte que vous souhaitez. 4. Choisissez Attach policy (Attacher la politique).	Administrateur AWS

Ressources connexes

- AWS Organizations documentation
- Politiques de contrôle des services (SCPs)
- Architecture d'inspection centralisée avec AWS Gateway Load Balancer et AWS Transit Gateway (AWS article de blog)

Limitez l'accès en fonction de l'adresse IP ou de la géolocalisation en utilisant AWS WAF

Créée par Louis Hourcade (AWS)

Récapitulatif

AWS WAFest un pare-feu pour applications Web qui aide à protéger les applications Web APIs contre les exploits Web courants et les robots susceptibles d'affecter la disponibilité, de compromettre la sécurité ou de consommer des ressources excessives. Les listes de contrôle d'accès Web (Web ACLs) vous AWS WAF permettent de contrôler la manière dont le trafic atteint vos applications. Dans une ACL Web, vous ajoutez des règles ou des groupes de règles conçus pour autoriser le trafic légitime, contrôler le trafic des robots et bloquer les modèles d'attaque courants. Pour plus d'informations, consultez la section AWS WAF Fonctionnement.

Vous pouvez associer les types de règles suivants à votre AWS WAF site Web ACLs :

- Groupes de règles AWS gérés : les équipes chargées des règles gérées et AWS Marketplace les vendeurs proposent des ensembles de règles préconfigurés. Certains groupes de règles gérés sont conçus pour protéger des types spécifiques d'applications Web. D'autres offrent une protection étendue contre les menaces connues ou les vulnérabilités courantes.
- Règles personnalisées et groupes de règles personnalisés — Vous pouvez également créer des règles et des groupes de règles qui personnalisent l'accès à vos applications Web et APIs. Par exemple, vous pouvez restreindre le trafic en fonction d'une liste spécifique d'adresses IP ou d'une liste de pays.

En utilisant ce modèle et le référentiel de code associé, vous pouvez utiliser le AWS Cloud Development Kit (AWS CDK)pour déployer le AWS WAF Web ACLs avec des règles personnalisées. Ces règles limitent l'accès aux ressources des applications Web en fonction de l'adresse IP ou de la géolocalisation de l'utilisateur final. Vous pouvez également éventuellement associer plusieurs groupes de règles gérés.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS

- Autorisations pour déployer AWS WAF des ressources
- AWS CDK, installé et configuré dans votre compte
- Git, installé

Limites

- Vous ne pouvez utiliser ce modèle que Régions AWS là où il AWS WAF est disponible. Pour connaître la disponibilité par région, voir Services AWS par région.

Outils

Services AWS

- AWS Cloud Development Kit (AWS CDK)est un framework de développement logiciel qui vous aide à définir et à provisionner AWS Cloud l'infrastructure dans le code.
- AWS WAFest un pare-feu d'applications Web qui vous aide à surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources protégées de votre application Web.

Référentiel de code

Le code de ce modèle est disponible dans la restriction d' GitHub adresse IP et de géolocalisation avec AWS WAF référentiel. Le code déploie deux AWS WAF sites Web. ACLs La première est une ACL Web régionale destinée aux ressources Amazon API Gateway. Le second est l'ACL Web mondial pour les CloudFront ressources Amazon. Les deux sites Web ACLs contiennent les règles personnalisées suivantes :

- `IPMatch`bloque les demandes provenant d'adresses IP non autorisées.
- `GeoMatch`bloque les demandes provenant de pays non autorisés.

Au cours du déploiement, vous pouvez éventuellement associer tous les groupes de règles gérés suivants à votre site Web ACLs :

- Ensemble de règles de base (CRS) : ce groupe de règles contient des règles généralement applicables aux applications Web. Il permet de se protéger contre l'exploitation d'un large éventail de vulnérabilités, y compris certaines des vulnérabilités à haut risque et fréquentes décrites dans les publications de l'OWASP, telles que le Top 10 de l'OWASP.

- Protection de l'administrateur : ce groupe de règles contient des règles qui vous aident à bloquer l'accès externe aux pages administratives exposées.
- Entrées erronées connues — Ce groupe de règles permet de bloquer les modèles de demandes dont on sait qu'ils ne sont pas valides et qui sont associés à l'exploitation ou à la découverte de vulnérabilités.
- Liste de réputation IP d'Amazon : ce groupe de règles contient des règles basées sur les renseignements internes d'Amazon sur les menaces. Il vous aide à bloquer les adresses IP généralement associées à des robots ou à d'autres menaces.
- Groupe de règles géré par le système d'exploitation Linux : ce groupe de règles permet de bloquer les modèles de demandes associés à l'exploitation de vulnérabilités Linux, notamment les attaques d'inclusion de fichiers locaux (LFI) spécifiques à Linux.
- Groupe de règles géré par base de données SQL : ce groupe de règles permet de bloquer les modèles de demandes associés à l'exploitation de bases de données SQL, tels que les attaques par injection SQL.

Épopées

Configuration du AWS WAF Web ACLs

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Entrez la commande suivante pour cloner l'adresse IP et la restriction de géolocalisation avec le AWS WAF référentiel sur votre poste de travail local : `git clone https://github.com/aws-samples/ip-and-geolocation-restriction-with-waf-cdk.git`	Git
Configurez les règles.	1. Dans le référentiel cloné, ouvrez le fichier app.py.	AWS, Python en général

Tâche	Description	Compétences requises

	2. Modifiez les valeurs des variables suivantes pour personnaliser les règles :
	
	`aws_acccount = "AWS_ACCOUNT"`
	`region = "AWS_REGION"`
	`ip_list = ["CIDR_RANGE_1", "CIDR_RANGE_2"]`
	`geo_list = ["COUNTRY_CODE_1", "COUNTRY_CODE_2"]`
	`aws_managed_rules = True`
	
	Où :
	• `aws_account` est l'ID de la cible Compte AWS.
	• `region`est la cible Région AWS de l'ACL Web pour les ressources API Gateway.
	
	Note
	L'ACL Web pour les CloudFront ressources est mondial et sera déployé dans la `us-east-1` région.	

Tâche	Description	Compétences requises
	• `ip_list`est la liste des plages d'adresses CIDR dont l'accès est autorisé. • `geo_list`est la liste des pays autorisés à y accéder. Pour connaître les valeurs valides, consultez la AWS WAF documentation. • `aws_managed_rules` contrôle si les groupes de règles gérés sont ajoutés à l'ACL Web. Si cette valeur l'est`True`, ils sont ajoutés. Si cette valeur l'est`False`, ils sont exclus. 3. Enregistrez et fermez le fichier app.py.	

Démarrez et déployez le code

Tâche	Description	Compétences requises
Bootstrap votre AWS environnement.	Si ce n'est pas déjà fait, vous devez démarrer votre AWS environnement avant de pouvoir déployer l' AWS CDK application. 1. Dans la AWS CDK CLI, entrez la commande	AWS général

Tâche	Description	Compétences requises

	suivante pour démarrer la `us-east-1` région :
	`cdk bootstrap aws://<account-id>/us-east-1`
	2. Si vous déployez l'ACL Web pour API Gateway dans une région autre que`us-east-1` , entrez la commande suivante pour démarrer la région cible :
	`cdk bootstrap aws://<account-id>/<region>`	

Déployez AWS CDK l'application.	1. Entrez la commande suivante pour déployer l' AWS CDK application : `cdk deploy --all` 2. Attendez que le déploiement de la AWS CloudFormation pile soit terminé.	AWS général

Valider le déploiement

Tâche	Description	Compétences requises
Vérifiez que le Web ACLs a été correctement déployé.	1. Connectez-vous à la AWS WAF console AWS Management Console, puis ouvrez-la.	AWS général

Tâche	Description	Compétences requises
	2. Dans le volet de navigation, sélectionnez Web ACLs. 3. Dans la liste de Régions AWS, choisissez Global (CloudFront). 4. Vérifiez que la nouvelle ACL CloudFront Web a été déployée et qu'elle possède l'adresse IP et les règles de géolocalisation que vous avez définies. Le nom par défaut de cette ACL Web est`WebACLCloudfront-<ID>` . 5. Dans la liste des Régions AWS, choisissez la région dans laquelle vous avez déployé la pile. 6. Vérifiez qu'une nouvelle ACL Web pour les ressources API Gateway a été déployée. Vérifiez qu'il possède l'adresse IP et les règles de géolocalisation que vous avez définies. Le nom par défaut de cette ACL Web est`WebACLApiGW-<ID>` .	

Tâche	Description	Compétences requises
(Facultatif) Associez le Web ACLs à vos ressources.	Associez le AWS WAF Web ACLs à vos AWS ressources, telles qu'un Application Load Balancer, une API Gateway ou CloudFront une distribut ion. Pour obtenir des instructi ons, voir Associer ou dissocier une ACL Web à une AWS ressource. Pour un exemple, voir class CfnWeb ACLAssoci ation (construct) dans la AWS CDK documentation.	AWS général

Nettoyage des ressources

Tâche	Description	Compétences requises
Supprimez les piles.	1. Dissociez l'ACL Web de toutes les AWS ressource s. Pour obtenir des instructi ons, consultez la AWS WAF documentation. 2. Dans la AWS CDK CLI, entrez la commande suivante pour supprimer l' AWS CDK application. `cdk destroy --all`	AWS général

Ressources connexes

- Référence d'API (AWS CDK documentation)
- aws-cdk-libmodule .aws_wafv2 (documentation)AWS CDK

- Utilisation du Web ACLs (AWS WAF documentation)
- Gestion de vos propres groupes de règles (AWS WAF documentation)
- Règles (AWS WAF documentation)

Analysez les référentiels Git pour détecter les informations sensibles et les problèmes de sécurité à l'aide de git-secrets

Créée par Saurabh Singh (AWS)

Récapitulatif

Ce modèle décrit comment utiliser l'outil open source git-secrets de AWS Labs pour analyser les référentiels sources Git et trouver du code susceptible de contenir des informations sensibles, telles que des mots de passe utilisateur ou des clés d' AWS accès, ou présentant d'autres problèmes de sécurité.

`git-secrets`analyse les validations, les messages de validation et les fusions pour empêcher l'ajout d'informations sensibles telles que des secrets à vos référentiels Git. Par exemple, si un commit, un message de validation ou tout autre commit d'un historique de fusion correspond à l'un de vos modèles d'expression régulière interdits et configurés, le commit est rejeté.

Conditions préalables et limitations

Prérequis

- Un actif Compte AWS
- Un dépôt Git qui nécessite une analyse de sécurité
- Un client Git (version 2.37.1 et ultérieure) installé

Architecture

Architecture cible

- Git
- `git-secrets`

Outils

- git-secrets est un outil qui vous empêche de saisir des informations sensibles dans les référentiels Git.
- Git est un système de contrôle de version distribué open source.

Bonnes pratiques

- Scannez toujours un dépôt Git en incluant toutes les révisions :

```
git secrets --scan-history
```

Épopées

Se connecter à une EC2 instance

Tâche	Description	Compétences requises
Connectez-vous à une EC2 instance à l'aide de SSH.	Connectez-vous à une instance Amazon Elastic Compute Cloud (Amazon EC2) à l'aide de SSH et d'un fichier de paires de clés. Vous pouvez ignorer cette étape si vous scannez un dépôt sur votre ordinateur local.	AWS général

Installez Git

Tâche	Description	Compétences requises
Installez Git.	Installez Git à l'aide de la commande :	AWS général

Tâche	Description	Compétences requises
	`yum install git -y` Si vous utilisez votre machine locale, vous pouvez installer un client Git pour une version spécifique du système d'exploitation. Pour plus d'informations, consultez le site Web de Git.	

Clonez le dépôt source et installez git-secrets

Tâche	Description	Compétences requises
Clonez le référentiel source Git.	Pour cloner le dépôt Git que vous souhaitez analyser, choisissez la commande Git clone dans votre répertoire personnel.	AWS général
Clonez des secrets virtuels.	Clonez le dépôt `git-secrets` Git. `git clone https://github.com/awslabs/git-secrets.git` Placez-le `git-secrets` quelque part dans le vôtre `PATH` pour que Git le récupère lorsque vous l'exécutez`git-secrets` .	AWS général
Installez git-secrets.	Pour Unix et ses variantes (Linux/macOS) :	AWS général

Tâche	Description	Compétences requises

	Vous pouvez utiliser la `install` cible du `Makefile` (fournie dans le `git-secrets` référentiel) pour installer l'outil. Vous pouvez personnaliser le chemin d'installation à l'aide des `MANPREFIX` variables `PREFIX` et.
	`make install`
	Pour Windows:
	Exécutez le PowerShell `install.ps1` script fourni dans le `git-secrets` référentiel. Ce script copie les fichiers d'installation dans un répertoire d'installation (`%USERPROFILE%/.git-secrets` par défaut) et ajoute le répertoire à l'utilisateur actuel`PATH`.
	`PS > ./install.ps1`
	Pour Homebrew (utilisateurs de macOS) :
	Exécuter :
	`brew install git-secrets`	

Scannez le référentiel de code Git

Tâche	Description	Compétences requises
Accédez au référentiel source.	Accédez au répertoire du dépôt Git que vous souhaitez scanner : `cd my-git-repository`	AWS général
Enregistrez l'ensemble de règles AWS (Git hooks).	`git-secrets` Pour configurer l'analyse de votre dépôt Git à chaque validation, exécutez la commande suivante : `git secrets --register-aws`	AWS général
Scannez le référentiel.	Exécutez la commande suivante pour lancer l'analyse de votre dépôt : `git secrets --scan`	AWS général

Passez en revue le fichier de sortie.	L'outil génère un fichier de sortie s'il détecte une vulnérabilité dans votre dépôt Git. Par exemple :
	`example.sh:4:AWS_SECRET_ACCESS_KEY = *********`
	
	`[ERROR] Matched one or more prohibited patterns`
	
	`Possible mitigations:`
		AWS général

Tâche	Description	Compétences requises
	- Mark false positives as allowed using: git config --add secrets.allowed ... - Mark false positives as allowed by adding regular expressions to .gitallowed at repository's root directory - List your configured patterns: git config --get-all secrets.patterns - List your configured allowed patterns: git config --get-all secrets.allowed - List your configured allowed patterns in .gitallowed at repository's root directory - Use --no-verify if this is a one-time false positive	

Ressources connexes

- outil git-secrets

Envoyer des alertes depuis AWS Network Firewall vers un canal Slack

Créée par Venki Srivatsav (AWS) et Aromal Raj Jayarajan (AWS)

Récapitulatif

Ce modèle décrit comment déployer un pare-feu en utilisant le pare-feu réseau Amazon Web Services (AWS) avec le modèle de déploiement distribué et comment propager les alertes générées par AWS Network Firewall vers un canal Slack configurable.

Les normes de conformité telles que la norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) exigent que vous installiez et mainteniez un pare-feu pour protéger les données des clients. Dans le cloud AWS, un cloud privé virtuel (VPC) est considéré comme un réseau physique dans le contexte de ces exigences de conformité. Vous pouvez utiliser Network Firewall pour surveiller le trafic réseau entre VPCs et pour protéger vos charges de travail exécutées conformément à VPCs une norme de conformité. Network Firewall bloque l'accès ou génère des alertes lorsqu'il détecte un accès non autorisé provenant VPCs d'autres utilisateurs du même compte. Toutefois, Network Firewall prend en charge un nombre limité de destinations pour envoyer les alertes. Ces destinations incluent les buckets Amazon Simple Storage Service (Amazon S3), les groupes de log CloudWatch Amazon et les flux de livraison Amazon Data Firehose. Toute action ultérieure concernant ces notifications nécessite une analyse hors ligne à l'aide d'Amazon Athena ou d'Amazon Kinesis.

Ce modèle fournit une méthode pour propager les alertes générées par Network Firewall vers un canal Slack configurable pour une action ultérieure en temps quasi réel. Vous pouvez également étendre cette fonctionnalité à d'autres mécanismes d'alerte tels que PagerDuty Jira et le courrier électronique. (Ces personnalisations n'entrent pas dans le cadre de ce modèle.)

Conditions préalables et limitations

Prérequis

- Chaîne Slack (voir Commencer dans le centre d'aide Slack)
- Privilèges requis pour envoyer un message à la chaîne
- L'URL du point de terminaison Slack avec un jeton d'API (sélectionnez votre application et choisissez un webhook entrant pour voir son URL ; pour plus d'informations, consultez la section Création d'un webhook entrant dans la documentation de l'API Slack)

- Une instance de test Amazon Elastic Compute Cloud (Amazon EC2) dans les sous-réseaux de charge de travail
- Règles de test dans Network Firewall
- Trafic réel ou simulé pour déclencher les règles de test
- Un compartiment S3 pour contenir les fichiers source à déployer

Limites

- Actuellement, cette solution ne prend en charge qu'une seule plage de routage interdomaines sans classe (CIDR) en tant que filtre pour la source et la destination. IPs

Architecture

Pile technologique cible

- Un VPC
- Quatre sous-réseaux (deux pour le pare-feu et deux pour les charges de travail)
- Passerelle Internet
- Quatre tables de routage avec règles
- Compartiment S3 utilisé comme destination d'alerte, configuré avec une politique de compartiment et des paramètres d'événements pour exécuter une fonction Lambda
- Fonction Lambda avec rôle d'exécution, pour envoyer des notifications Slack
- Secret d'AWS Secrets Manager pour le stockage de l'URL Slack
- Pare-feu réseau avec configuration d'alertes
- Canal Slack

Tous les composants, à l'exception du canal Slack, sont fournis par les CloudFormation modèles et la fonction Lambda fournis avec ce modèle (voir la section Code).

Architecture cible

Ce modèle met en place un pare-feu réseau décentralisé avec intégration à Slack. Cette architecture consiste en un VPC avec deux zones de disponibilité. Le VPC comprend deux sous-réseaux protégés et deux sous-réseaux de pare-feu dotés de points de terminaison de pare-feu réseau. Tout le trafic entrant et sortant des sous-réseaux protégés peut être surveillé en créant des politiques

et des règles de pare-feu. Le pare-feu réseau est configuré pour placer toutes les alertes dans un compartiment S3. Ce compartiment S3 est configuré pour appeler une fonction Lambda lorsqu'il reçoit un `put` événement. La fonction Lambda extrait l'URL Slack configurée depuis Secrets Manager et envoie le message de notification à l'espace de travail Slack.

Pour plus d'informations sur cette architecture, consultez le billet de blog AWS Deployment models for AWS Network Firewall.

Outils

Services AWS

- AWS Network Firewall est un pare-feu réseau dynamique et géré, ainsi qu'un service de détection et de prévention des intrusions VPCs destiné au cloud AWS. Vous pouvez utiliser Network Firewall pour filtrer le trafic sur le périmètre de votre VPC et protéger vos charges de travail sur AWS.
- AWS Secrets Manager est un service de stockage et de récupération des informations d'identification. À l'aide de Secrets Manager, vous pouvez remplacer les informations d'identification codées en dur dans votre code, y compris les mots de passe, par un appel d'API à Secrets Manager pour récupérer le secret par programmation. Ce modèle utilise Secrets Manager pour stocker l'URL de Slack.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web. Ce modèle utilise Amazon S3 pour stocker les CloudFormation modèles et le script Python de la fonction Lambda. Il utilise également un compartiment S3 comme destination des alertes de pare-feu réseau.
- AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Ce modèle utilise AWS CloudFormation pour déployer automatiquement une architecture distribuée pour Firewall Manager.

Code

Le code de ce modèle est disponible sur GitHub le référentiel Network Firewall Slack Integration. Dans le `src` dossier du dépôt, vous trouverez :

- Ensemble de CloudFormation fichiers au format YAML. Vous utilisez ces modèles pour configurer les composants de ce modèle.
- Un fichier source Python (`slack-lambda.py`) pour créer la fonction Lambda.
- Un package de déploiement d'archive .zip (`slack-lambda.py.zip`) pour télécharger le code de votre fonction Lambda.

Pour utiliser ces fichiers, suivez les instructions de la section suivante.

Épopées

Configuration du compartiment S3

Tâche	Description	Compétences requises
Créez un compartiment S3.	1. Connectez-vous à la console de gestion AWS et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/. 2. Choisissez ou créez un compartiment S3 pour héberger le code. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Le nom du compartiment S3 ne peut pas inclure de barres obliques en tête. Nous vous recommandons d'utiliser un préfixe pour organiser le code de ce modèle.	Développeur d'applications, propriétaire de l'application, administrateur du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Création d'un compartiment dans la documentation Amazon S3.	
Téléchargez les CloudFormation modèles et le code Lambda.	1. Téléchargez les fichiers suivants depuis le GitHub référentiel pour ce modèle : • `base.yml` • `igw-ingress-route.yml` • `slack-lambda.py` • `slackLambda.yml` • `decentralized-deployment.yml` • `protected-subnet-route.yml` • `slack-lambda.py.zip` 2. Téléchargez les fichiers dans le compartiment S3 que vous avez créé.	Développeur d'applications, propriétaire de l'application, administrateur du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle.	Ouvrez la CloudFormation console AWS dans la même région AWS que votre compartiment S3 et déployez le modèle`base.yml`. Ce modèle crée les ressources	Développeur d'applications, propriétaire de l'application, administrateur du cloud

Tâche	Description	Compétences requises
	AWS et les fonctions Lambda requises pour les alertes à transmettre au canal Slack. Pour plus d'informations sur le déploiement CloudFormation de modèles, consultez la section Création d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation.	
Complétez les paramètres du modèle.	Spécifiez le nom de la pile et configurez les valeurs des paramètres. Pour obtenir la liste des paramètres, leurs descriptions et leurs valeurs par défaut, voir CloudFormation les paramètres dans la section Informations supplémentaires.	Développeur d'applications, propriétaire de l'application, administrateur du cloud
Créez la pile.	1. Passez en revue les détails de la pile et mettez à jour les valeurs en fonction des exigences de votre environnement. 2. Choisissez Create stack pour déployer le modèle.	Développeur d'applications, propriétaire de l'application, administrateur du cloud

Vérifiez la solution

Tâche	Description	Compétences requises
Testez le déploiement.	Utilisez la CloudFormation console AWS ou l'interface de ligne de commande AWS (AWS CLI) pour vérifier que les ressources répertoriées dans la section Target technology stack ont été créées. Si le déploiement du CloudFormation modèle échoue, vérifiez les valeurs que vous avez fournies pour les `pAvailabilityZone2` paramètres `pAvailabilityZone1` et. Ils doivent être adaptés à la région AWS dans laquelle vous déployez la solution. Pour obtenir la liste des zones de disponibilité pour chaque région, consultez Régions et zones dans la EC2 documentation Amazon.	Développeur d'applications, propriétaire de l'application, administrateur du cloud
Fonctionnalité de test.	1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/. 2. Créez une EC2 instance dans l'un des sous-réseaux protégés. Choisissez une AMI Amazon Linux 2 (HVM) à utiliser comme serveur	Développeur d'applications, propriétaire de l'application, administrateur du cloud

Tâche	Description	Compétences requises

	HTTPS. Pour obtenir des instructions, consultez la section Lancer une instance dans la EC2 documentation Amazon.
	
	Note
	Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.
	
	3. Utilisez les données utilisateur suivantes pour installer un serveur Web sur l' EC2 instance :
	
	`#!/bin/bash`
	`yum install httpd -y`
	`systemctl start httpd`
	`systemctl stop firewalld`
	`cd /var/www/html`
	`echo "Hello!! this is a NFW alert test page, 200 OK" > index.html`
	
	4. Créez les règles de pare-feu réseau suivantes :
	
	Règle d'apatridie :
	
	`Source: 0.0.0.0/0`	

Tâche	Description	Compétences requises
	Destination 10.0.3.65 /32 (private IP of the EC2 instance) Action: Forward Règle dynamique : Protocol: HTTP Source ip/port: Any / Any Destination ip/port: Any /Any 5. Obtenez l'adresse IP publique du serveur Web que vous avez créé à l'étape 3. 6. Accédez à l'adresse IP publique dans un navigateur. Le message suivant devrait s'afficher dans le navigateur : Hello!! this is a NFW alert test page, 200 OK Vous recevrez également une notification sur le canal Slack. La notification peut être différée en fonction de la taille du message. À des fins de test, envisagez de fournir un filtre CIDR qui n'est pas trop étroit (par exemple, une valeur CIDR avec /32 serait considérée comme trop étroite et /8 serait trop large). Pour	

Tâche	Description	Compétences requises
	plus d'informations, consultez la section Comportement du filtre dans Informations supplémentaires.	

Ressources connexes

- Modèles de déploiement pour AWS Network Firewall (article de blog AWS)
- Politiques d'AWS Network Firewall (documentation AWS)
- Network Firewall Slack Integration (GitHub référentiel)
- Création d'un espace de travail Slack (centre d'aide Slack)

Informations supplémentaires

CloudFormation parameters

Paramètre	Description	Valeur par défaut ou valeur d'échantillon
`pVpcName`	Nom du VPC à créer.	Inspection
`pVpcCidr`	La plage CIDR que le VPC doit créer.	10.0.0.0/16
`pVpcInstanceTenancy`	Comment EC2 les instances sont distribuées sur le matériel physique. Les options sont `default` (location partagée) ou `dedicated` (location unique).	default
`pAvailabilityZone1`	La première zone de disponibilité de l'infrastructure.	us-east-2a

pAvailabilityZone2	La deuxième zone de disponibilité de l'infrastructure.	us-east-2b
pNetworkFirewallSubnet1Cidr	La plage CIDR pour le premier sous-réseau de pare-feu (minimum /28).	10.0.1.0/24
pNetworkFirewallSubnet2Cidr	La plage CIDR pour le deuxième sous-réseau de pare-feu (minimum /28).	10.0.2.0/24
pProtectedSubnet1Cidr	La plage CIDR pour le premier sous-réseau protégé (charge de travail).	10.0.3.0/24
pProtectedSubnet2Cidr	La plage CIDR pour le deuxième sous-réseau protégé (charge de travail).	10.0.4.0/24
pS3BucketName	Le nom du compartiment S3 existant dans lequel vous avez chargé le code source Lambda.	us-w2- yourname-lambda-functions
pS3KeyPrefix	Le préfixe du compartiment S3 dans lequel vous avez chargé le code source Lambda.	test AOD
pAWSSecretName4Slack	Le nom du secret contenant l'URL de Slack.	SlackEnpoint-Cfn
pSlackChannelName	Le nom de la chaîne Slack que vous avez créée.	quelques notifications de nom
pSlackUserName	Nom d'utilisateur Slack.	Utilisateur de Slack

`pSecretKey`	Il peut s'agir de n'importe quelle clé. Nous vous recommandons d'utiliser la valeur par défaut.	URL du webhook
`pWebHookUrl`	La valeur de l'URL Slack.	https://hooks.slack.com/services/T ? ? ? 9E ? /A031885 JRM7 /9D4Y ? ? ? ? ?
`pAlertS3Bucket`	Nom du compartiment S3 à utiliser comme destination des alertes de pare-feu réseau. Ce bucket sera créé pour vous.	us-w2- yourname-security-aod-alerts
`pSecretTagName`	Le nom du tag pour le secret.	AppName
`pSecretTagValue`	La valeur de balise pour le nom de balise spécifié.	LambdaSlackIntegration
`pdestCidr`	Le filtre pour la plage d'adresses CIDR de destination. Pour plus d'informations, consultez la section suivante, Comportement du filtre.	10.0.0.0/16
`pdestCondition`	Un drapeau pour indiquer s'il faut exclure ou inclure la correspondance de destination. Pour plus d'informations, consultez la section suivante, . Les valeurs valides sont `include` et `exclude`.	inclure
`psrcCidr`	Le filtre correspondant à la plage d'adresses CIDR source à alerter. Pour plus d'informations, consultez la section suivante, .	118,2,0,0/16

`psrcCondition`	L'indicateur permettant d'exclure ou d'inclure la correspondance source. Pour plus d'informations, consultez la section suivante, .	inclure

Comportement du filtre

Si vous n'avez configuré aucun filtre dans AWS Lambda, toutes les alertes générées sont envoyées à votre chaîne Slack. La source et la destination IPs des alertes générées sont comparées aux plages CIDR que vous avez configurées lors du déploiement du CloudFormation modèle. Si une correspondance est trouvée, la condition est appliquée. Si la source ou la destination se situent dans la plage CIDR configurée et qu'au moins l'une d'entre elles est configurée avec la condition`include`, une alerte est générée. Les tableaux suivants fournissent des exemples de valeurs, de conditions et de résultats CIDR.

	CIDR configuré	IP d'alerte	Configured	Alerte
Source	10.0.0.0/16	10,0.0.25	inclure	Oui
Destination (Destination)	100,0,0/16	202,0.0.13	inclure	

	CIDR configuré	IP d'alerte	Configured	Alerte
Source	10.0.0.0/16	10,0.0.25	exclure	Non
Destination (Destination)	100,0,0/16	202,0.0.13	inclure	

	CIDR configuré	IP d'alerte	Configured	Alerte
Source	10.0.0.0/16	10,0.0.25	inclure	Oui

Destination (Destination)	100,0,0/16	100,0,13	inclure	

	CIDR configuré	IP d'alerte	Configured	Alerte
Source	10.0.0.0/16	90,0.0.25	inclure	Oui
Destination (Destination)	Null	202,0.0.13	inclure	

	CIDR configuré	IP d'alerte	Configured	Alerte
Source	10.0.0.0/16	90,0.0.25	inclure	Non
Destination (Destination)	100,0,0/16	202,0.0.13	inclure	

Simplifiez la gestion des certificats privés en utilisant AWS Private CA et AWS RAM

Créée par Everett Hinckley (AWS) et Vivek Goyal (AWS)

Récapitulatif

Vous pouvez utiliser l'autorité de certification privée AWS (AWS Private CA) pour émettre des certificats privés afin d'authentifier les ressources internes et de signer le code informatique. Ce modèle fournit un CloudFormation modèle AWS pour le déploiement rapide d'une hiérarchie d'autorités de certification à plusieurs niveaux et une expérience de provisionnement cohérente. Vous pouvez éventuellement utiliser AWS Resource Access Manager (AWS RAM) pour partager en toute sécurité l'autorité de certification au sein de vos organisations ou unités organisationnelles (OUs) dans AWS Organizations, et centraliser l'autorité de certification tout en utilisant la RAM AWS pour gérer les autorisations. Comme il n'est pas nécessaire d'avoir une autorité de certification privée pour chaque compte, cette approche vous permet d'économiser de l'argent. En outre, vous pouvez utiliser Amazon Simple Storage Service (Amazon S3) pour stocker la liste de révocation des certificats (CRL) et les journaux d'accès.

Cette implémentation fournit les fonctionnalités et avantages suivants :

- Centralise et simplifie la gestion de la hiérarchie des autorités de certification privées à l'aide d'AWS Private CA.
- Exporte les certificats et les clés vers des appareils gérés par le client sur AWS et sur site.
- Utilise un CloudFormation modèle AWS pour un déploiement rapide et une expérience de provisionnement cohérente.
- Crée une autorité de certification racine privée avec une hiérarchie de 1, 2, 3 ou 4 autorités de certification subordonnées.
- Utilise éventuellement la RAM AWS pour partager l'autorité de certification subordonnée de l'entité finale avec d'autres comptes au niveau de l'organisation ou de l'unité d'organisation.
- Permet d'économiser de l'argent en supprimant le besoin d'une autorité de certification privée pour chaque compte grâce à la RAM AWS.
- Crée un compartiment S3 facultatif pour la CRL.
- Crée un compartiment S3 facultatif pour les journaux d'accès CRL.

Conditions préalables et limitations

Prérequis

Si vous souhaitez partager l'autorité de certification au sein d'une structure AWS Organizations, identifiez ou configurez les éléments suivants :

- Un compte de sécurité pour créer la hiérarchie et le partage de l'autorité de certification.
- Une unité d'organisation ou un compte distinct pour les tests.
- Le partage est activé dans le compte de gestion AWS Organizations. Pour plus d'informations, consultez la section Activer le partage de ressources au sein d'AWS Organizations dans la documentation AWS RAM.

Limites

- CAs sont des ressources régionales. Tous CAs résident dans un seul compte AWS et dans une seule région AWS.
- Les certificats et clés générés par l'utilisateur ne sont pas pris en charge. Dans ce cas d'utilisation, nous vous recommandons de personnaliser cette solution pour utiliser une autorité de certification racine externe.
- Un bucket CRL public n'est pas pris en charge. Nous vous recommandons de garder la CRL privée. Si un accès Internet à la CRL est requis, consultez la section sur l'utilisation d'Amazon CloudFront pour servir CRLs dans la section Activation de la fonctionnalité S3 Block Public Access (BPA) dans la documentation d'AWS Private CA.
- Ce modèle met en œuvre une approche à région unique. Si vous avez besoin d'une autorité de certification multirégionale, vous pouvez implémenter des subordonnés dans une deuxième région AWS ou sur site. Cette complexité n'entre pas dans le cadre de ce modèle, car la mise en œuvre dépend de votre cas d'utilisation spécifique, du volume de charge de travail, des dépendances et des exigences.

Architecture

Pile technologique cible

- CA privée AWS
- AWS RAM

- Amazon S3
- AWS Organizations
- AWS CloudFormation

Architecture cible

Ce modèle propose deux options de partage avec AWS Organizations :

Option 1 – Créez le partage au niveau de l'organisation. Tous les comptes de l'organisation peuvent émettre les certificats privés en utilisant l'autorité de certification partagée, comme indiqué dans le schéma suivant.

Option 2 – Créez le partage au niveau de l'unité organisationnelle (UO). Seuls les comptes de l'unité d'organisation spécifiée peuvent émettre les certificats privés à l'aide de l'autorité de certification partagée. Par exemple, dans le schéma suivant, si le partage est créé au niveau de l'unité d'organisation Sandbox, le développeur 1 et le développeur 2 peuvent émettre des certificats privés en utilisant l'autorité de certification partagée.

Outils

Services AWS

- AWS Private CA — AWS Private Certificate Authority (AWS Private CA) est un service d'autorité de certification privée hébergé permettant d'émettre et de révoquer des certificats numériques privés. Il vous permet de créer des hiérarchies d'autorité de certification privées, y compris racine et subordonnée CAs, sans les coûts d'investissement et de maintenance liés à l'exploitation d'une autorité de certification sur site.
- AWS RAM — AWS Resource Access Manager (AWS RAM) vous permet de partager en toute sécurité vos ressources entre les comptes AWS et au sein de votre organisation ou OUs dans AWS Organizations. Pour réduire les frais opérationnels dans un environnement multi-comptes, vous pouvez créer une ressource et utiliser la RAM AWS pour partager cette ressource entre les comptes.
- AWS Organizations — AWS Organizations est un service de gestion de comptes qui vous permet de consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web. Ce modèle utilise Amazon S3 pour stocker la liste de révocation des certificats (CRL) et les journaux d'accès.
- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement. Ce modèle utilise AWS CloudFormation pour déployer automatiquement une hiérarchie de CA à plusieurs niveaux.

Code

Le code source de ce modèle est disponible sur GitHub, dans le référentiel hiérarchique AWS Private CA. Le référentiel inclut :

- Le CloudFormation modèle AWSACMPCA-RootCASubCA.yaml. Vous pouvez utiliser ce modèle pour déployer la hiérarchie de l'autorité de certification pour cette implémentation.
- Testez les fichiers pour des cas d'utilisation tels que la demande, l'exportation, la description et la suppression d'un certificat.

Pour utiliser ces fichiers, suivez les instructions de la section Epics.

Épopées

Architecte la hiérarchie de l'autorité de certification

Tâche	Description	Compétences requises
Collectez les informations relatives au sujet du certificat.	Rassemblez les informations relatives au sujet du certificat concernant le propriétaire du certificat : nom de l'organisation, unité organisationnelle, pays, État, localité et nom commun.	Architecte cloud, architecte de sécurité, ingénieur PKI

Tâche	Description	Compétences requises
Collectez des informations facultatives sur AWS Organizations.	Si l'autorité de certification doit faire partie d'une structure AWS Organizations et que vous souhaitez partager la hiérarchie de l'autorité de certification au sein de cette structure, collectez le numéro de compte de gestion, l'identifiant de l'organisation et éventuellement l'ID de l'unité d'organisation (si vous souhaitez partager la hiérarchie de l'autorité de certification uniquement avec une unité d'organisation spécifique). Déterminez également les comptes AWS Organizations ou OUs, le cas échéant, avec lesquels vous souhaitez partager l'autorité de certification.	Architecte cloud, architecte de sécurité, ingénieur PKI

Tâche	Description	Compétences requises
Concevez la hiérarchie de l'autorité de certification.	Déterminez quel compte hébergera le root et le subordonné. CAs Déterminez le nombre de niveaux subordonnés requis par la hiérarchie entre les certificats d'entité racine et d'entité finale. Pour plus d'informations, consultez la section Conception d'une hiérarchie d'autorités de certification dans la documentation AWS Private CA.	Architecte cloud, architecte de sécurité, ingénieur PKI
Déterminez les conventions de dénomination et de balisage pour la hiérarchie de l'autorité de certification.	Déterminez les noms des ressources AWS : l'autorité de certification racine et chaque autorité de certification subordonnée. Déterminez les balises qui doivent être attribuées à chaque autorité de certification.	Architecte cloud, architecte de sécurité, ingénieur PKI

Tâche	Description	Compétences requises
Déterminez les algorithmes de chiffrement et de signature requis.	Déterminez les éléments suivants : • L'algorithme de chiffrement de votre entreprise est requis pour les clés publiques utilisées par votre autorité de certification lorsqu'elle émet un certificat. La valeur par défaut est RSA_2048. • Algorithme clé utilisé par votre autorité de certification pour signer les certificats. La valeur par défaut est SHA256 WITHRSA.	Architecte cloud, architecte de sécurité, ingénieur PKI
Déterminez les exigences de révocation des certificats pour la hiérarchie de l'autorité de certification.	Si des fonctionnalités de révocation de certificats sont requises, établissez une convention de dénomination pour le compartiment S3 qui contient la liste de révocation de certificats (CRL).	Architecte cloud, architecte de sécurité, ingénieur PKI
Déterminez les exigences de journalisation pour la hiérarchie de l'autorité de certification.	Si des fonctionnalités de journalisation des accès sont requises, établissez une convention de dénomination pour le compartiment S3 qui contient les journaux d'accès.	Architecte cloud, architecte de sécurité, ingénieur PKI

Tâche	Description	Compétences requises
Déterminez les périodes d'expiration des certificats.	Déterminez la date d'expiration du certificat racine (la valeur par défaut est de 10 ans), des certificats d'entité finale (la valeur par défaut est de 13 mois) et des certificats CA subordonnés (la valeur par défaut est de 3 ans). Les certificats d'autorité de certification subordonnés doivent expirer plus tôt que les certificats d'autorité de certification situés aux niveaux supérieurs de la hiérarchie. Pour plus d'informations, consultez la section Gestion du cycle de vie de l'autorité de certification privée dans la documentation de l'autorité de certification privée AWS.	Architecte cloud, architecte de sécurité, ingénieur PKI

Déployer la hiérarchie CA

Tâche	Description	Compétences requises
Prérequis pour	Suivez les étapes décrites dans la section Prérequis de ce modèle.	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI
Créez des rôles CA pour différents personnages.	1. Déterminez les types de rôles ou d'utilisateurs AWS Identity and Access Management (IAM) dans AWS IAM Identity Center	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI

Tâche	Description	Compétences requises
	(successeur d'AWS Single Sign-On) nécessaires pour administrer les différent s niveaux de la hiérarchi e de l'autorité de certifica tion, tels que CAAdmin root, CAAdmin subordonné et. CertificateConsumer 2. Déterminez la granularité des politiques nécessaires pour séparer les tâches. 3. Créez les rôles ou utilisate urs IAM requis dans IAM Identity Center dans le compte sur lequel réside la hiérarchie de l'autorité de certification.	

Tâche	Description	Compétences requises
Déployez la CloudFormation pile.	1. À partir du GitHub dépôt de ce modèle, téléchargez le modèle AWSPCA-RootCASubCA .yaml. 2. Déployez le modèle depuis la CloudFormation console AWS ou depuis l'interface de ligne de commande AWS (AWS CLI). Pour plus d'informations, consultez la section Utilisation des piles dans la CloudFormation documentation. 3. Complétez les paramètres du modèle, notamment le nom de l'organisation, le nom de l'UO, l'algorithme clé, l'algorithme de signature et les autres options.	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI

Tâche	Description	Compétences requises
Concevez une solution pour mettre à jour les certificats utilisés par les ressources gérées par les utilisateurs.	Les ressources des services AWS intégrés, tels que Elastic Load Balancing, mettent à jour les certifica ts automatiquement avant leur expiration. Toutefois, les ressources gérées par les utilisateurs, telles que les serveurs Web exécutés sur des instances Amazon Elastic Compute Cloud (Amazon EC2), nécessitent un autre mécanisme. 1. Déterminez quelles ressources gérées par l'utilisateur nécessitent des certificats d'entité finale de la part de l'autorité de certification privée. 2. Planifiez un processus pour être informé de l'expirat ion des ressources et des certificats gérés par les utilisateurs. Pour obtenir des exemples relatifs à , consultez les rubriques suivantes : • Utilisation d'une règle gérée par AWS Config • Utilisation d'Amazon CloudWatch et d'Amazon EventBridge	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI

Tâche	Description	Compétences requises
	3. Rédigez des scripts personnalisés pour mettre à jour les certificats sur les ressources gérées par les utilisateurs et intégrez-les aux services AWS pour automatiser les mises à jour. Pour plus d'informations sur les services AWS intégrés, consultez la section Services intégrés à AWS Certificate Manager dans la documentation ACM.	

Valider et documenter la hiérarchie de l'autorité de certification

Tâche	Description	Compétences requises
Validez le partage facultatif de RAM AWS.	Si la hiérarchie de l'autorité de certification est partagée avec d'autres comptes dans AWS Organizations, connectez-vous à l'un de ces comptes depuis l'AWS Management Console, accédez à la console AWS Private CA et vérifiez que l'autorité de certification nouvellement créée est partagée avec ce compte. Seule l'autorité de certification de niveau inférieur de la hiérarchie sera visible, car c'est l'autorité de certifica	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI

Tâche	Description	Compétences requises
	tion qui génère les certifica ts d'entité finale. Répétez l'opération pour un échantill on des comptes avec lesquels l'autorité de certification est partagée.	
Validez la hiérarchie de l'autorité de certification avec des tests du cycle de vie des certificats	Dans le GitHub référentiel de ce modèle, recherchez les tests du cycle de vie. Exécutez les tests depuis l'AWS CLI pour demander un certificat, exporter un certificat, décrire un certificat et supprimer un certificat.	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI
Importez la chaîne de certifica ts dans des magasins de confiance.	Pour que les navigateurs et autres applications puissent faire confiance à un certifica t, l'émetteur du certificat doit être inclus dans le trust store du navigateur, qui est une liste des certificats fiables CAs. Ajoutez la chaîne de certifica ts de la nouvelle hiérarchi e CA au trust store de votre navigateur et de votre applicati on. Vérifiez que les certificats d'entité finale sont fiables.	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI

Tâche	Description	Compétences requises
Créez un runbook pour documenter la hiérarchie de l'autorité de certification.	Créez un document d'exécuti on pour décrire l'architecture de la hiérarchie de l'autorité de certification, la structure des comptes pouvant demander des certificats d'entité finale, le processus de création et les tâches de gestion de base telles que l'émission de certificats d'entité finale (sauf si vous souhaitez autoriser les comptes enfants en libre-ser vice), l'utilisation et le suivi.	Administrateur cloud, ingénieurs en sécurité, ingénieurs PKI

Ressources connexes

- Conception d'une hiérarchie d'autorités de certification (documentation AWS Private CA)
- Création d'une autorité de certification privée (documentation AWS Private CA)
- Comment utiliser la RAM AWS pour partager vos comptes AWS Private CA entre plusieurs comptes (article de blog AWS)
- Meilleures pratiques d'AWS Private CA (article de blog AWS)
- Activer le partage de ressources au sein d'AWS Organizations (documentation AWS RAM)
- Gestion du cycle de vie de l'autorité de certification privée (documentation AWS Private CA)
- acm-certificate-expiration-check pour AWS Config (documentation AWS Config)
- AWS Certificate Manager assure désormais le suivi de l'expiration des certificats via Amazon CloudWatch (annonce AWS)
- Services intégrés à AWS Certificate Manager (documentation ACM)

Informations supplémentaires

Lorsque vous exportez des certificats, utilisez une phrase secrète sécurisée sur le plan cryptographique et conforme à la stratégie de prévention des pertes de données de votre entreprise.

Désactiver les contrôles standard de sécurité sur tous les comptes membres du Security Hub dans un environnement multi-comptes

Créée par Michael Fuellbier (AWS) et Ahmed Bakry (AWS)

Récapitulatif

> **Important**
>
> AWS Security Hub prend désormais en charge la configuration centralisée pour les normes et les contrôles de sécurité, pour tous les comptes. Cette nouvelle fonctionnalité répond à de nombreux scénarios couverts par la solution dans ce modèle de guide AWS prescriptif. Avant de déployer la solution selon ce modèle, consultez la section Configuration centrale dans Security Hub.

Dans le cloud Amazon Web Services (AWS), les contrôles AWS Security Hub standard, tels que CIS AWS Foundations Benchmark ou AWS Foundational Security Best Practices, ne peuvent être désactivés (désactivés) que manuellement d'un seul Compte AWS coup. Dans un environnement multi-comptes, vous ne pouvez pas désactiver les contrôles sur plusieurs comptes membres du Security Hub en « un seul clic » (c'est-à-dire en un seul appel d'API). Ce modèle montre comment désactiver en un clic les contrôles standard du Security Hub sur tous les comptes membres du Security Hub gérés par votre compte administrateur du Security Hub.

Conditions préalables et limitations

Prérequis

- Un environnement multi-comptes composé d'un compte administrateur Security Hub qui gère plusieurs comptes de membres
- AWS Command Line Interface (AWS CLI) version 2, installée
- AWS Serverless Application Model Interface de ligne de commande (AWS SAM CLI), installée

Limites

- Ce modèle ne fonctionne que dans un environnement multi-comptes où un seul compte administrateur Security Hub gère plusieurs comptes de membres.

- L'initiation de l'événement entraîne de multiples invocations parallèles si vous modifiez un grand nombre de commandes dans un laps de temps très court. Cela peut entraîner un ralentissement de l'API et entraîner l'échec des appels. Par exemple, ce scénario peut se produire si vous modifiez de nombreux contrôles par programmation à l'aide de la CLI Security Hub Controls.

Architecture

Le schéma suivant montre un exemple de AWS Step Functions flux de travail qui désactive les contrôles standard du Security Hub sur plusieurs comptes membres du Security Hub (tel qu'il est affiché depuis le compte administrateur du Security Hub).

Le diagramme inclut le flux de travail suivant :

1. Une EventBridge règle Amazon est initiée selon un calendrier quotidien et appelle la machine à états. Vous pouvez modifier le calendrier de la règle en mettant à jour le `Schedule` paramètre dans votre AWS CloudFormation modèle.
2. Une EventBridge règle est initiée chaque fois qu'un contrôle est activé ou désactivé dans le compte administrateur du Security Hub.
3. Une machine d'état Step Functions propage l'état des contrôles standard de sécurité (c'est-à-dire les contrôles activés ou désactivés) du compte administrateur du Security Hub aux comptes des membres.
4. Un rôle entre comptes AWS Identity and Access Management (IAM) est déployé dans chaque compte membre et assumé par la machine d'état. La machine d'État active ou désactive les commandes de chaque compte membre.
5. Une table Amazon DynamoDB contient des exceptions et des informations sur les contrôles à activer ou à désactiver dans un compte donné. Ces informations remplacent les configurations extraites du compte administrateur Security Hub pour le compte membre spécifié.

> **Note**
>
> L'objectif de la EventBridge règle planifiée est de garantir que les comptes membres du Security Hub récemment ajoutés ont le même statut de contrôle que les comptes existants.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon EventBridge est un service de bus d'événements sans serveur qui vous permet de connecter vos applications à des données en temps réel provenant de diverses sources. Par exemple, AWS Lambda des fonctions, des points de terminaison d'appel HTTP utilisant des destinations d'API ou des bus d'événements dans d'autres. Comptes AWS
- AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir Services AWS par le biais de commandes dans votre interface de ligne de commande.
- AWS Lambda est un service de calcul qui vous aide à exécuter du code sans avoir à allouer ni à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.
- AWS Serverless Application Model (AWS SAM) est un framework open source qui vous aide à créer des applications sans serveur dans le. AWS Cloud
- AWS Security Hubfournit une vue complète de votre état de sécurité dans AWS. Il vous permet également de vérifier que votre AWS environnement est conforme aux normes et aux meilleures pratiques du secteur de la sécurité.
- AWS Step Functionsest un service d'orchestration sans serveur qui vous aide à combiner des AWS Lambda fonctions et d'autres fonctions Services AWS pour créer des applications critiques pour l'entreprise.

Référentiel de code

Le code de ce modèle est disponible dans le référentiel GitHub AWS Security Hub Cross-Account Controls Disabler. Le référentiel de code contient les fichiers et dossiers suivants :

- UpdateMembers/template.yaml — Ce fichier contient les composants déployés dans le compte administrateur du Security Hub, notamment la machine d'état Step Functions et les règles. EventBridge
- member-iam-role/template.yaml — Ce fichier contient le code permettant de déployer le rôle IAM entre comptes dans un compte membre.
- StateMachine.json — Ce fichier définit le flux de travail de la machine à états.

- GetMembers/index.py — Ce fichier contient le code de la machine GetMembersd'état. Un script récupère l'état des contrôles standard de sécurité dans tous les comptes membres du Security Hub existants.
- UpdateMember/index.py — Ce fichier contient un script qui met à jour l'état du contrôle dans chaque compte membre.
- CheckResult/index.py — Ce fichier contient un script qui vérifie l'état de l'appel du flux de travail (accepté ou échec).

Épopées

Déployer un rôle IAM entre comptes dans les comptes membres du Security Hub

Tâche	Description	Compétences requises
Identifiez l'identifiant du compte administrateur du Security Hub.	Configurez un compte administrateur Security Hub, puis notez l'identifiant du compte administrateur.	Architecte du cloud
Déployez le CloudFormation modèle qui inclut le rôle IAM entre comptes dans les comptes des membres.	Pour déployer le modèle member-iam-role/template.yaml dans tous les comptes membres gérés par le compte administrateur du Security Hub, exécutez la commande suivante : `aws cloudformation deploy \ --template-file member-iam-role/template.yaml \ --capabilities CAPABILITY_NAMED_IAM \ --stack-name <your-stack-name> \`	AWS DevOps

Tâche	Description	Compétences requises
	`--parameter-overri des SecurityHubAdminAc countId=<account-ID>` Le `SecurityHubAdminAc countId` paramètre doit correspondre à l'identifiant du compte administrateur Security Hub que vous avez indiqué précédemment.	

Déployer une machine d'état dans le compte administrateur du Security Hub

Tâche	Description	Compétences requises
Package le CloudFormation modèle qui inclut la machine à états avec AWS SAM.	Pour intégrer le UpdateMem bersmodèle /template.yaml dans le compte administrateur du Security Hub, exécutez la commande suivante : `sam package \ --template-file UpdateMembers/temp late.yaml \ --output-template-file UpdateMembers/ template-out.yaml \ --s3-bucket <amzn-s3-demo-bucket>` **Note** Votre compartim ent Amazon Simple Storage Service	AWS DevOps

Tâche	Description	Compétences requises
	(Amazon S3) doit se trouver dans le Région AWS même compartiment que celui où vous déployez CloudFormation le modèle.	

Tâche	Description	Compétences requises
Déployez le CloudFormation modèle intégré dans le compte administrateur du Security Hub.	Pour déployer le CloudFormation modèle dans le compte administrateur du Security Hub, exécutez la commande suivante : `aws cloudformation deploy \ --template-file UpdateMembers/template-out.yaml \ --capabilities CAPABILITY_IAM \ --stack-name <stack-name>` Dans le modèle member-iam-role/template.yaml, le `MemberIAMRolePath` paramètre doit correspondre au paramètre et doit correspondre. `IAMRolePath` `MemberIAMRoleName` `IAMRoleName` **Note** Security Hub étant un service régional, vous devez déployer le modèle individuellement dans chacun d'eux Région AWS. Assurez-vous d'abord de regrouper la solution dans un	AWS DevOps

Tâche	Description	Compétences requises
	compartiment Amazon S3 dans chaque région.	

Ressources connexes

- Désignation d'un compte administrateur Security Hub (documentation Security Hub)
- Gestion des erreurs, des nouvelles tentatives et ajout d'alertes aux exécutions par AWS Step Functions State Machine (AWS article de blog)

Mettez à jour les informations d'identification de l'AWS CLI depuis AWS IAM Identity Center en utilisant PowerShell

Créée par Chad Miles (AWS) et Andy Bowen (AWS)

Récapitulatif

Si vous souhaitez utiliser les informations d'identification AWS IAM Identity Center (successeur d'AWS Single Sign-On) avec AWS Command Line Interface (AWS CLI) SDKs, AWS ou AWS Cloud Development Kit (AWS CDK), vous devez généralement copier-coller les informations d'identification de la console IAM Identity Center dans l'interface de ligne de commande. Ce processus peut prendre un temps considérable et doit être répété pour chaque compte nécessitant un accès.

L'une des solutions les plus courantes consiste à utiliser la `aws sso configure` commande AWS CLI. Cette commande ajoute un profil activé par IAM Identity Center à votre CLI AWS ou à votre kit SDK AWS. Toutefois, l'inconvénient de cette solution est que vous devez exécuter la commande `aws sso login` pour chaque profil ou compte de l'interface de ligne de commande AWS que vous avez configuré de cette manière.

Comme solution alternative, ce modèle décrit comment utiliser les profils nommés de l'interface de ligne de commande AWS et les outils AWS PowerShell pour stocker et actualiser simultanément les informations d'identification de plusieurs comptes à partir d'une seule instance IAM Identity Center. Le script stocke également les données de session IAM Identity Center en mémoire pour actualiser les informations d'identification sans vous reconnecter à IAM Identity Center.

Conditions préalables et limitations

Prérequis

- PowerShell, installé et configuré. Pour plus d'informations, consultez la section Installation PowerShell (documentation Microsoft).
- Outils AWS pour PowerShell, installés et configurés. Pour des raisons de performances, nous vous recommandons vivement d'installer la version modulaire d'AWS Tools for PowerShell, appeléeAWS.Tools. Chaque service AWS est pris en charge par son propre petit module. À l' PowerShell invite, entrez les commandes suivantes pour installer les modules nécessaires à ce modèle : AWS.Tools.InstallerSSO, etSSOIDC.

```
Install-Module AWS.Tools.Installer
```

```
Install-AWSToolsModule SSO, SSOOIDC
```

Pour plus d'informations, voir Installer AWS.tools sous Windows ou Installer AWS.tools sous Linux ou macOS.

- L'AWS CLI ou le SDK AWS doivent être préalablement configurés avec des informations d'identification fonctionnelles en effectuant l'une des opérations suivantes :
  - Utilisez la `aws configure` commande AWS CLI. Pour plus d'informations, consultez la section Configuration rapide (documentation de l'AWS CLI).
  - Configurez l'AWS CLI ou le AWS CDK pour obtenir un accès temporaire via un rôle IAM. Pour plus d'informations, voir Obtenir les informations d'identification du rôle IAM pour l'accès à la CLI (documentation IAM Identity Center).

Limites

- Ce script ne peut pas être utilisé dans un pipeline ou dans une solution entièrement automatisée. Lorsque vous déployez ce script, vous devez autoriser manuellement l'accès depuis IAM Identity Center. Le script continue ensuite automatiquement.

Versions du produit

- Pour tous les systèmes d'exploitation, il est recommandé d'utiliser PowerShell la version 7.0 ou ultérieure.

Architecture

Vous pouvez utiliser le script de ce modèle pour actualiser simultanément plusieurs informations d'identification IAM Identity Center, et vous pouvez créer un fichier d'informations d'identification à utiliser avec l'AWS CLI SDKs, AWS ou AWS CDK.

Outils

Services AWS

- L'interface de ligne de commande AWS (AWS CLI) est un outil open source qui vous permet d'interagir avec les services AWS par le biais de commandes dans votre shell de ligne de commande.

- AWS IAM Identity Center vous aide à gérer de manière centralisée l'accès par authentification unique (SSO) à tous vos comptes AWS et applications cloud.
- Les outils AWS pour PowerShell sont un ensemble de PowerShell modules qui vous aident à créer des scripts pour des opérations sur vos ressources AWS à partir de la ligne de PowerShell commande.

Autres outils

- PowerShellest un programme d'automatisation et de gestion de configuration Microsoft qui s'exécute sous Windows, Linux et macOS.

Bonnes pratiques

Conservez une copie de ce script pour chaque instance d'IAM Identity Center. L'utilisation d'un script pour plusieurs instances n'est pas prise en charge.

Épopées

Exécutez le script SSO

Tâche	Description	Compétences requises
Personnalisez le script SSO.	1. Copiez le script SSO dans la section Informations supplémentaires. 2. Dans la `Param` section, pour votre environnement AWS, définissez les valeurs des variables suivantes : • `DefaultRoleName` — Le rôle ou l'ensemble d'autorisations IAM à utiliser par défaut. • `Region`— La région AWS dans laquelle le centre d'identité IAM est	Administrateur du cloud

Tâche	Description	Compétences requises
	déployé. Pour une liste complète des régions et de leurs codes, consultez la section Points de terminaison régionaux. • `StartUrl`— L'URL utilisée pour accéder à votre page de connexion à IAM Identity Center. Utilisez le même format que celui de la valeur d'exemple dans le script. • `EnvironmentName` — Nom court pour faire référence à cette copie du script, à utiliser lorsque vous exécutez plusieurs copies de script au cours de la même session. 3. Sous la ligne 10, qui se lit comme suit`# Add your Account Informati on` , modifiez les valeurs suivantes dans les tables de hachage pour refléter votre environnement : • `Profile`— Le nom du profil de l'AWS CLI dans lequel stocker les informations d'identif ication temporaires. • `AccountId` — L'ID du compte AWS pour	

Tâche	Description	Compétences requises
	lequel vous récupérez les informations d'identification. • `RoleName`— Le nom du rôle ou de l'ensemble d'autorisations IAM Identity Center que vous souhaitez utiliser. Vous pouvez laisser cela comme `$DefaultRoleName` si vous vouliez utiliser le même rôle que celui que vous avez défini dans la `Param` section. Chaque ligne de la table de hachage doit se terminer par une virgule, sauf la dernière.	

Tâche	Description	Compétences requises

Exécutez le script SSO.	Il est recommandé d'exécuter votre script personnalisé dans le PowerShell shell à l'aide de la commande suivante.
	`./Set-AwsCliSsoCredentials.ps1`
	Vous pouvez également exécuter le script depuis un autre shell en saisissant la commande suivante.
	`pwsh Set-AwsCliSsoCredentials.ps1`
		Administrateur du cloud

Résolution des problèmes

Problème	Solution
`No Access`Erreur	Le rôle IAM que vous utilisez n'est pas autorisé à accéder au rôle ou à l'ensemble d'autorisations que vous avez défini dans un `RoleName` paramètre. Mettez à jour les autorisations pour le rôle que vous utilisez ou définissez un rôle ou un ensemble d'autorisations différent dans le script.

Ressources connexes

- Où sont stockés les paramètres de configuration ? (documentation de la CLI AWS)
- Configuration de l'interface de ligne de commande AWS pour utiliser AWS IAM Identity Center (documentation de l'interface de ligne de commande AWS)

- Utilisation de profils nommés (documentation de l'AWS CLI)

Informations supplémentaires

Script SSO

Dans le script suivant, remplacez les espaces réservés entre crochets (**<>**) par vos propres informations et supprimez les crochets.

```
Set-AwsCliSsoCredentials.ps1
Param(
    $DefaultRoleName = '<AWSAdministratorAccess>',
    $Region          = '<us-west-2>',
    $StartUrl        = "<https://d-12345abcde.awsapps.com/start/>",
    $EnvironmentName = "<CompanyName>"
)
Try {$SsoAwsAccounts = (Get-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Scope
 Global -ErrorAction 'SilentlyContinue').Value.Clone()}
Catch {$SsoAwsAccounts = $False}
if (-not $SsoAwsAccounts) { $SsoAwsAccounts = @(
# Add your account information in the list of hash tables below, expand as necessary,
 and do not forget the commas
    @{Profile = "<Account1>"      ; AccountId = "<012345678901 >"; RoleName =
 $DefaultRoleName },
    @{Profile = "<Account2>"      ; AccountId = "<123456789012>"; RoleName =
 "<AWSReadOnlyAccess>" }
)}
$ErrorActionPreference = "Stop"
if (-not (Test-Path ~\.aws))      { New-Item ~\.aws -type Directory }
if (-not (Test-Path ~\.aws\credentials)) { New-Item ~\.aws\credentials -type File }
$CredentialFile = Resolve-Path ~\.aws\credentials
$PsuedoCreds    = @{AccessKey =
 'AKAEXAMPLE123ACCESS';SecretKey='PsuedoS3cret4cceSSKey123PsuedoS3cretKey'} # Pseudo
 Creds, do not edit.
Try {$SSOTokenExpire = (Get-Variable -Scope Global -Name
 "$($EnvironmentName)SSOTokenExpire" -ErrorAction 'SilentlyContinue').Value} Catch
 {$SSOTokenExpire = $False}
Try {$SSOToken       = (Get-Variable -Scope Global -Name "$($EnvironmentName)SSOToken"
 -ErrorAction 'SilentlyContinue').Value }      Catch {$SSOToken       = $False}
if ( $SSOTokenExpire -lt (Get-Date) ) {
    $SSOToken = $Null
```

```
    $Client   = Register-SSOOIDCClient -ClientName cli-sso-client -ClientType public -
Region $Region @PsuedoCreds
    $Device   = $Client | Start-SSOOIDCDeviceAuthorization -StartUrl $StartUrl -Region
 $Region @PsuedoCreds
    Write-Host "A Browser window should open. Please login there and click ALLOW." -
NoNewline
    Start-Process $Device.VerificationUriComplete
    While (-Not $SSOToken){
        Try {$SSOToken = $Client | New-SSOOIDCToken -DeviceCode $Device.DeviceCode -
GrantType "urn:ietf:params:oauth:grant-type:device_code" -Region $Region @PsuedoCreds}
        Catch {If ($_.Exception.Message -notlike "*AuthorizationPendingException*")
{Write-Error $_.Exception} ; Start-Sleep 1}
    }
    $SSOTokenExpire = (Get-Date).AddSeconds($SSOToken.ExpiresIn)
    Set-Variable -Name "$($EnvironmentName)SSOToken" -Value $SSOToken -Scope Global
    Set-Variable -Name "$($EnvironmentName)SSOTokenExpire" -Value $SSOTokenExpire -
Scope Global
}
$CredsTime     = $SSOTokenExpire - (Get-Date)
$CredsTimeText = ('{0:D2}:{1:D2}:{2:D2} left on SSO Token' -f $CredsTime.Hours,
 $CredsTime.Minutes, $CredsTime.Seconds).TrimStart("0 :")
for ($i = 0; $i -lt $SsoAwsAccounts.Count; $i++) {
    if (([DateTimeOffset]::FromUnixTimeSeconds($SsoAwsAccounts[$i].CredsExpiration /
 1000)).DateTime -lt (Get-Date).ToUniversalTime()) {
        Write-host "`r
    `rRegistering Profile $($SsoAwsAccounts[$i].Profile)" -NoNewline
        $TempCreds = $SSOToken | Get-SSORoleCredential -AccountId
 $SsoAwsAccounts[$i].AccountId -RoleName $SsoAwsAccounts[$i].RoleName -Region $Region
 @PsuedoCreds
        [PSCustomObject]@{AccessKey = $TempCreds.AccessKeyId; SecretKey =
 $TempCreds.SecretAccessKey; SessionToken = $TempCreds.SessionToken
        } | Set-AWSCredential -StoreAs $SsoAwsAccounts[$i].Profile -ProfileLocation
 $CredentialFile
        $SsoAwsAccounts[$i].CredsExpiration = $TempCreds.Expiration
    }
}
Set-Variable -name "$($EnvironmentName)SsoAwsAccounts" -Value $SsoAwsAccounts.Clone() -
Scope Global
Write-Host "`r$($SsoAwsAccounts.Profile) Profiles registered, $CredsTimeText"
```

Utiliser AWS Config pour surveiller les configurations de sécurité d'Amazon Redshift

Créée par Lucas Kauffman (AWS) et abhishek sengar (AWS)

Récapitulatif

À l'aide d'AWS Config, vous pouvez évaluer les configurations de sécurité de vos ressources AWS. AWS Config peut surveiller les ressources, et si les paramètres de configuration enfreignent les règles que vous avez définies, AWS Config signale la ressource comme non conforme.

Vous pouvez utiliser AWS Config pour évaluer et surveiller vos clusters et bases de données Amazon Redshift. Pour plus d'informations sur les recommandations et fonctionnalités de sécurité, consultez la section Sécurité dans Amazon Redshift. Ce modèle inclut des règles AWS Lambda personnalisées pour AWS Config. Vous pouvez déployer ces règles dans votre compte pour surveiller les configurations de sécurité de vos clusters et bases de données Amazon Redshift. Les règles de ce modèle vous aident à utiliser AWS Config pour confirmer que :

- La journalisation des audits est activée pour les bases de données du cluster Amazon Redshift
- Le protocole SSL est requis pour se connecter au cluster Amazon Redshift
- Les chiffrements FIPS (Federal Information Processing Standards) sont utilisés
- Les bases de données du cluster Amazon Redshift sont cryptées
- La surveillance de l'activité des utilisateurs est activée

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- AWS Config doit être activé dans votre compte AWS. Pour plus d'informations, consultez Configuration d'AWS Config avec la console ou Configuration d'AWS Config avec l'AWS CLI.
- La version 3.9 ou ultérieure de Python doit être utilisée pour le gestionnaire AWS Lambda. Pour plus d'informations, consultez Travailler avec Python (documentation AWS Lambda).

Versions du produit

- Python version 3.9 ou ultérieure

Architecture

Pile technologique cible

- AWS Config

Architecture cible

1. AWS Config exécute régulièrement la règle personnalisée.
2. La règle personnalisée invoque la fonction Lambda.
3. La fonction Lambda vérifie la présence de configurations non conformes dans les clusters Amazon Redshift.
4. La fonction Lambda indique l'état de conformité de chaque cluster Amazon Redshift à AWS Config.

Automatisation et mise à l'échelle

Les règles personnalisées d'AWS Config permettent d'évaluer tous les clusters Amazon Redshift de votre compte. Aucune action supplémentaire n'est requise pour faire évoluer cette solution.

Outils

Services AWS

- AWS Config fournit une vue détaillée des ressources de votre compte AWS et de leur configuration. Il vous aide à identifier les liens entre les ressources et l'évolution de leurs configurations au fil du temps.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans avoir à provisionner ou à gérer des serveurs. Il exécute votre code uniquement lorsque cela est nécessaire et évolue automatiquement, de sorte que vous ne payez que pour le temps de calcul que vous utilisez.

- Amazon Redshift est un service d'entrepôt de données géré à l'échelle du pétaoctet dans le cloud AWS.

Référentiel de code

Le code de ce modèle est disponible dans le GitHub aws-config-rulesréférentiel. Les règles personnalisées de ce référentiel sont les règles Lambda du langage de programmation Python. Ce référentiel contient de nombreuses règles personnalisées pour AWS Config. Seules les règles suivantes sont utilisées dans ce modèle :

- `REDSHIFT_AUDIT_ENABLED`— Vérifiez que la journalisation des audits est activée sur le cluster Amazon Redshift. Si vous souhaitez également vérifier que la surveillance de l'activité des utilisateurs est activée, déployez plutôt la `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED` règle.
- `REDSHIFT_SSL_REQUIRED`— Vérifiez que le protocole SSL est requis pour se connecter au cluster Amazon Redshift. Si vous souhaitez également vérifier que les chiffrements FIPS (Federal Information Processing Standards) sont utilisés, déployez plutôt la `REDSHIFT_FIPS_REQUIRED` règle.
- `REDSHIFT_FIPS_REQUIRED`— Vérifiez que le protocole SSL est requis et que les chiffrements FIPS sont utilisés.
- `REDSHIFT_DB_ENCRYPTED`— Vérifiez que les bases de données du cluster Amazon Redshift sont cryptées.
- `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`— Vérifiez que la journalisation des audits et le suivi de l'activité des utilisateurs sont activés.

Épopées

Préparez-vous à déployer les règles

Tâche	Description	Compétences requises
Configurez les politiques IAM.	1. Créez une politique personnalisée basée sur l'identité IAM qui permet au rôle d'exécution Lambda de lire les configurations du	Administrateur AWS

Tâche	Description	Compétences requises
	cluster Amazon Redshift. Pour plus d'informations, consultez Gestion de l'accès aux ressources (documentation Amazon Redshift) et Création de politiques IAM (documentation IAM). `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["redshift:DescribeClusterParameterGroups", "redshift:DescribeClusterParameters", "redshift:DescribeClusters", "redshift:DescribeClusterSecurityGroups", "redshift:DescribeClusterSnapshots", "redshift:DescribeClusterSubnetGroups", "redshift:DescribeEventSubscriptions", "redshift:DescribeLoggingStatus"`	

Tâche	Description	Compétences requises

	<pre>],
	        "Resource":
	"*"
	      }
	    ]
	}</pre>
	2. Assignez les politiques AWSLambdad'exécution et AWSConfigRulesExecutionRolegérées en tant que politique d'autorisation pour le rôle d'exécution Lambda. Pour obtenir des instructions, consultez la section Ajout d'autorisations d'identité IAM (documentation IAM).	

Pour cloner le référentiel.	Dans un shell Bash, exécutez la commande suivante. Cela clone le aws-config-rulesdépôt à partir de. GitHub <pre>git clone https://github.com/awslabs/aws-config-rules.git</pre>	AWS général

Déployez les règles dans AWS Config

Tâche	Description	Compétences requises
Déployez les règles dans AWS Config.	En suivant les instructions de la section Création de règles Lambda personnalisées (documentation AWS Config),	Administrateur AWS

Tâche	Description	Compétences requises
	déployez une ou plusieurs des règles suivantes dans votre compte : • `REDSHIFT_AUDIT_ENABLED` • `REDSHIFT_SSL_REQUIRED` • `REDSHIFT_FIPS_REQUIRED` • `REDSHIFT_DB_ENCRYPTED` • `REDSHIFT_USER_ACTIVITY_MONITORING_ENABLED`	
Vérifiez que les règles sont fonctionnelles.	Après avoir déployé les règles, suivez les instructions de la section Évaluation de vos ressources (documentation AWS Config) pour vérifier qu'AWS Config évalue correctement vos ressources Amazon Redshift.	AWS général

Ressources connexes

Documentation des services AWS

- Sécurité dans Amazon Redshift (documentation Amazon Redshift)
- Gestion de la sécurité des bases de données (documentation Amazon Redshift)
- Règles personnalisées AWS Config (documentation AWS Config)

Recommandations AWS

- Vérifiez que les nouveaux clusters Amazon Redshift ont besoin de points de terminaison SSL
- Assurez-vous qu'un cluster Amazon Redshift est chiffré lors de sa création

Informations supplémentaires

Vous pouvez utiliser les règles gérées par AWS suivantes dans AWS Config pour confirmer les configurations de sécurité suivantes pour Amazon Redshift :

- redshift-cluster-configuration-check— Utilisez cette règle pour confirmer que la journalisation des audits est activée pour les bases de données du cluster Amazon Redshift et pour confirmer que les bases de données sont cryptées.
- redshift-require-tls-ssl— Utilisez cette règle pour confirmer que le protocole SSL est requis pour se connecter au cluster Amazon Redshift.

Utilisez Network Firewall pour capturer les noms de domaine DNS à partir de l'indication du nom du serveur pour le trafic sortant

Créée par Kirankumar Chandrashekar (AWS)

Récapitulatif

Ce modèle vous montre comment utiliser AWS Network Firewall pour collecter les noms de domaine DNS fournis par l'indication du nom du serveur (SNI) dans l'en-tête HTTPS de votre trafic réseau sortant. Network Firewall est un service géré qui facilite le déploiement de protections réseau critiques pour Amazon Virtual Private Cloud (Amazon VPC), notamment la possibilité de sécuriser le trafic sortant à l'aide d'un pare-feu qui bloque les paquets qui ne répondent pas à certaines exigences de sécurité. La sécurisation du trafic sortant vers des noms de domaine DNS spécifiques est appelée filtrage de sortie, qui consiste à surveiller et éventuellement à restreindre le flux d'informations sortantes d'un réseau à un autre.

Après avoir capturé les données SNI qui passent par Network Firewall, vous pouvez utiliser Amazon CloudWatch Logs et AWS Lambda pour publier les données sur une rubrique Amazon Simple Notification Service (Amazon SNS) qui génère des notifications par e-mail. Les notifications par e-mail incluent le nom du serveur et d'autres informations SNI pertinentes. En outre, vous pouvez utiliser le résultat de ce modèle pour autoriser ou restreindre le trafic sortant par nom de domaine dans le SNI en utilisant des règles de pare-feu. Pour plus d'informations, consultez la section Utilisation de groupes de règles dynamiques dans AWS Network Firewall dans la documentation Network Firewall.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Interface de ligne de commande AWS (AWS CLI) version 2, installée et configurée sous Linux, macOS ou Windows.
- Network Firewall, installé et configuré dans Amazon VPC et utilisé pour inspecter le trafic sortant. Vous pouvez configurer Network Firewall pour utiliser l'une des configurations VPC suivantes :
  - Architecture à zone unique simple avec passerelle Internet
  - Architecture multizone avec passerelle Internet

- Architecture avec passerelle Internet et passerelle NAT

Architecture

Le schéma suivant montre comment utiliser Network Firewall pour collecter des données SNI à partir du trafic réseau sortant, puis publier ces données sur une rubrique SNS à l'aide de Logs CloudWatch et Lambda.

Le schéma suivant illustre le flux de travail suivant :

1. Network Firewall collecte les noms de domaine à partir des données SNI contenues dans l'en-tête HTTPS de votre trafic réseau sortant.
2. CloudWatch Logs surveille les données SNI et invoque une fonction Lambda chaque fois que le trafic réseau sortant passe par Network Firewall.
3. La fonction Lambda lit les données SNI capturées par CloudWatch Logs, puis les publie dans une rubrique SNS.
4. La rubrique SNS vous envoie une notification par e-mail qui inclut les données SNI.

Automatisation et mise à l'échelle

- Vous pouvez utiliser AWS CloudFormation pour créer ce modèle en utilisant l'infrastructure comme code.

Pile technologique

- Amazon CloudWatch Logs
- Amazon SNS
- Amazon VPC
- AWS Lambda
- AWS Network Firewall

Outils

Services AWS

- Amazon CloudWatch Logs : vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder à vos fichiers journaux à partir d'instances Amazon Elastic Compute Cloud (Amazon EC2), d'AWS CloudTrail, d'Amazon Route 53 et d'autres sources.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) est un service géré qui permet aux éditeurs de transmettre des messages aux abonnés (également appelés producteurs et consommateurs).
- Amazon VPC — Amazon Virtual Private Cloud (Amazon VPC) fournit une section logiquement isolée du cloud AWS dans laquelle vous pouvez lancer des ressources AWS dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive d'AWS.
- AWS Lambda — AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs.
- AWS Network Firewall — AWS Network Firewall est un service géré qui facilite le déploiement de protections réseau essentielles pour l'ensemble de votre Amazon VPCs.

Épopées

Création d'un groupe de CloudWatch journaux pour Network Firewall

Tâche	Description	Compétences requises
Créez un groupe de CloudWatch journaux.	1. Connectez-vous à AWS Management Console et ouvrez la console CloudWatch . 2. Dans le panneau de navigation, choisissez Groupes de journaux. 3. Choisissez Actions, puis Create Bucket (Créer un compartiment). 4. Tapez un nom pour le groupe de journaux, puis	Administrateur du cloud

Tâche	Description	Compétences requises
	choisissez Créer un groupe de journaux. Pour plus d'informations, consultez la section Utilisation des groupes de journaux et des flux de journaux dans la CloudWatch documentation.	

Création d'un sujet et d'un abonnement SNS

Tâche	Description	Compétences requises
Créez une rubrique SNS.	Pour créer une rubrique SNS, suivez les instructions de la documentation Amazon SNS.	Administrateur du cloud
Abonnez un point de terminaison à la rubrique SNS.	Pour abonner une adresse e-mail en tant que point de terminaison à la rubrique SNS que vous avez créée, suivez les instructions de la documentation Amazon SNS. Pour Protocole, choisissez Email/Email-JSON. **Note** Vous pouvez également choisir un point de terminaison différent en fonction de vos besoins.	Administrateur du cloud

Configurer la connexion dans Network Firewall

Tâche	Description	Compétences requises
Activez la journalisation du pare-feu.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, sous NETWORK FIREWALL, sélectionnez Firewalls. 3. Dans la section Firewalls, choisissez le pare-feu sur lequel vous souhaitez capturer le nom du serveur à partir du SNI pour le trafic sortant. 4. Choisissez l'onglet Détails du pare-feu, puis sélectionnez Modifier dans la section Journalisation. 5. Pour Type de journal, sélectionnez Alerte. Pour Destination du journal pour les alertes, sélectionnez le groupe de CloudWatch journaux. 6. Pour le groupe de CloudWatch journaux, recherchez et choisissez le groupe de journaux que vous avez créé précédemment, puis choisissez Enregistrer.	Administrateur du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations sur l'utilisation CloudWatch des journaux comme destination des journaux pour Network Firewall, consultez Amazon CloudWatch Logs dans la documentation de Network Firewall.	

Configurer une règle dynamique dans Network Firewall

Tâche	Description	Compétences requises
Créez une règle dynamique.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, sous NETWORK FIREWALL, sélectionnez Network Firewall Rule Groups. 3. Choisissez le groupe de règles Create Network Firewall. 4. Sur la page du groupe de règles Create Network Firewall, pour le type de groupe de règles, choisissez Stateful rule group. Remarque : pour plus d'informations, consultez Utilisation de groupes de	Administrateur du cloud

Tâche	Description	Compétences requises
	règles dynamiques dans AWS Network Firewall. 5. Dans la section Groupe de règles dynamique, entrez le nom et la description du groupe de règles. 6. Pour Capacité, définissez la capacité maximale que vous souhaitez autoriser pour le groupe de règles dynamiques (jusqu'à 30 000 maximum). Remarque : vous ne pouvez pas modifier ce paramètre après avoir créé le groupe de règles. Pour plus d'informations sur le calcul de la capacité, consultez la section Configuration de la capacité des groupes de règles dans AWS Network Firewall. Pour plus d'informations sur le paramètre maximal, consultez la section Quotas d'AWS Network Firewall. 7. Pour les options de groupe de règles Stateful, sélectionnez 5 tuples. 8. Dans la section Stateful rule order, sélectionnez Default. 9. Dans la section Variables de règles, conservez les valeurs par défaut.	

Tâche	Description	Compétences requises
	10. Dans la section Ajouter une règle, choisissez TLS pour le protocole. Pour Source, sélectionnez N'importe lequel. Pour Port source, choisissez N'importe quel port. Pour Destination, choisissez N'importe laquelle. Pour Port de destination, choisissez N'importe quel port. Pour Direction du trafic, choisissez Forward. Pour Action, choisissez Alerte. Choisissez Ajouter une règle. 11. Choisissez Créer un groupe de règles dynamiques.	

Tâche	Description	Compétences requises
Associez la règle dynamique à Network Firewall.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Amazon VPC. 2. Dans le volet de navigation, sous NETWORK FIREWALL, sélectionnez Firewalls. 3. Choisissez le pare-feu dans lequel vous souhaitez capturer le nom du serveur à partir du SNI pour le trafic sortant. 4. Dans la section Groupes de règles dynamiques, choisissez Actions, puis choisissez Ajouter des groupes de règles dynamiques non gérés. 5. Sur la page Ajouter des groupes de règles dynamiques non gérés, sélectionnez le groupe de règles dynamiques que vous avez créé précédemment, puis choisissez Ajouter un groupe de règles dynamiques.	Administrateur du cloud

Créez une fonction Lambda pour lire les journaux

Tâche	Description	Compétences requises

Créez le code de la fonction Lambda.	Dans un environnement de développement intégré (IDE) capable de lire l'événement CloudWatch Logs de Network Firewall pour le trafic sortant, collez le code Python 3 suivant et remplacez-le `<SNS-topic-ARN>` par votre valeur :
	`import json`
	`import gzip`
	`import base64`
	`import boto3`
	`sns_client = boto3.client('sns')`
	`def lambda_handler(event, context):`
	`  decoded_event = json.loads(gzip.decompress(base64.b64decode(event['awslogs']['data'])))`
	`  body = '''`
	`  {filtermatch}`
	`  '''.format(`
	`  loggroup=decoded_event['logGroup'],`
	`  logstream=decoded_event['logStream'],`
	`  filtermatch=decoded_event['logEvents'][0]['message'],`
	`  )`
		Développeur d'applications

Tâche	Description	Compétences requises

	<pre>print(body)
	filterMatch = json.loads(body)
	data = []
	if 'http' in filterMatch['event']:
	data.append(filterMatch['event']['http']['hostname'])
	elif 'tls' in filterMatch['event']:
	data.append(filterMatch['event']['tls']['sni'])
	result = 'Domain accessed ' + 1*' ' + (data[0]) + 1*' ' 'via AWS Network Firewall ' + 1*' ' + (filterMatch['firewall_name'])
	print(result)
	message = {'ServerName': result}
	send_to_sns = sns_client.publish(
	TargetArn=<SNS-topic-ARN>,
	#Replace with the SNS topic ARN
	Message=json.dumps({'default': json.dumps(message),
	
	'sms': json.dumps(message),
	
	'email': json.dumps(message)}),
	Subject='Server Name passed through the Network Firewall',</pre>	

Tâche	Description	Compétences requises

	<pre>MessageSt
	ructure='json'
	)</pre>
	Cet exemple de code analyse le contenu CloudWatch des journaux et capture le nom du serveur fourni par le SNI dans l'en-tête HTTPS.	

Créez la fonction Lambda.	Pour créer la fonction Lambda, suivez les instructions de la documentation Lambda et choisissez Python 3.9 for Runtime.	Administrateur du cloud
Ajoutez le code à la fonction Lambda.	Pour ajouter votre code Python à la fonction Lambda que vous avez créée précédemment, suivez les instructions de la documentation Lambda.	Administrateur du cloud

Tâche	Description	Compétences requises
Ajoutez CloudWatch des journaux comme déclencheur à la fonction Lambda.	1. Connectez-vous à l'AWS Management Console et ouvrez la console Lambda. 2. Dans le volet de navigation, choisissez Functions, puis choisissez la fonction que vous avez créée précédemment. 3. Dans la section Présentation de la fonction, choisissez Ajouter un déclencheur. 4. Sur la page Ajouter un déclencheur, dans la section Configuration du déclencheur, choisissez CloudWatch Logs, puis Ajouter. 5. Pour Groupe de journaux, choisissez le groupe de CloudWatch journaux que vous avez créé précédemment. 6. Dans Nom du filtre, entrez le nom de votre filtre. 7. Choisissez Ajouter. 8. Dans l'onglet Configuration de la page de votre fonction, dans la section Déclencheurs, sélectionnez le déclencheur que vous venez d'ajouter, puis sélectionnez Activer.	Administrateur du cloud

Tâche	Description	Compétences requises
	Pour plus d'informations, consultez la section Utilisation de Lambda avec des CloudWatch journaux dans la documentation Lambda.	

Tâche	Description	Compétences requises
Ajoutez des autorisations de publication sur SNS.	Ajoutez l'autorisation SNS:Publish au rôle d'exécution Lambda, afin que Lambda puisse effectuer des appels d'API pour publier des messages sur SNS. 1. Trouvez le rôle d'exécution de la fonction Lambda que vous avez créée précédemment. 2. Ajoutez la politique suivante à votre rôle AWS Identity and Access Management (IAM) : `{ "Version": "2012-10-17", "Statement": [ { "Sid": "AllowSNSPublish", "Effect": "Allow", "Action": [ "sns:GetTopicAttributes", "sns:Subscribe", "sns:Unsubscribe", "sns:Publish" ],`	Administrateur du cloud

Tâche	Description	Compétences requises

	<pre>"Resource": "*"
	}
	]
	}</pre>	

Testez la fonctionnalité de votre notification SNS

Tâche	Description	Compétences requises

Envoyez du trafic via Network Firewall.	1. Envoyez ou attendez que le trafic HTTPS passe par Network Firewall.
	2. Consultez l'e-mail de notification SNS que vous recevez d'AWS lorsque le trafic passe par Network Firewall. L'e-mail inclut les détails du SNI pour le trafic sortant. Par exemple, l'e-mail généré à partir du code Lambda ci-dessus aura le contenu suivant si le nom de domaine consulté est EMAIL-JSON https://aws.amazon.comet si le protocole d'abonnement est EMAIL-JSON :
	<pre>{
	"Type": "Notification",
	"MessageId": "<messageID>",</pre>
		Ingénieur de test

Tâche	Description	Compétences requises
	"TopicArn": "arn:aws:sns:us-west-2:123456789:testSNSTopic", "Subject": "Server Name passed through the Network Firewall", "Message": "{\"ServerName\": \"Domain 'aws.amazon.com' accessed via AWS Network Firewall 'AWS-Network-Firewall-Multi-AZ-firewall\"}", "Timestamp": "2022-03-22T04:10:04.217Z", "SignatureVersion": "1", "Signature": "<Signature>", "SigningCertURL": "<SigningCertUrl>", "UnsubscribeURL": "<UnsubscribeURL>" } Consultez ensuite le journal des alertes Network Firewall sur Amazon CloudWatch en suivant les instructions de la CloudWatch documentation Amazon. Le journal des alertes affiche le résultat suivant : { "firewall_name": "AWS-Network-Firew	

Tâche	Description	Compétences requises
	`all-Multi-AZ-firew all", "availability_zone ": "us-east-2b", "event_timestamp": "<event timestamp>", "event": { "timestamp": "2021-03-22T04:10: 04.214222+0000", "flow_id": <flow ID>, "event_type": "alert", "src_ip": "10.1.3.76", "src_port": 22761, "dest_ip": "99.86.59.73", "dest_port": 443, "proto": "TCP", "alert": { "action": "allowed", "signatur e_id": 2, "rev": 0, "signatur e": "", "category": "", "severity": 3 }, "tls": { "subject": "CN=aws.amazon.com", "issuerdn ": "C=US, O=Amazon,`	

Tâche	Description	Compétences requises
	OU=Server CA 1B, CN=Amazon", "serial": "<serial number>", "fingerprint": "<fingerprint ID>", "sni": "aws.amazon.com", "version": "TLS 1.2", "notbefore": "2020-09-30T00:00:00", "notafter": "2021-09-23T12:00:00", "ja3": {}, "ja3s": {} }, "app_proto": "tls" } }	

Utilisez Terraform pour activer automatiquement Amazon GuardDuty pour une organisation

Créée par Aarthi Kannan (AWS)

Récapitulatif

Amazon surveille GuardDuty en permanence vos comptes Amazon Web Services (AWS) et utilise les informations sur les menaces pour identifier les activités inattendues et potentiellement malveillantes au sein de votre environnement AWS. L'activation manuelle GuardDuty pour plusieurs comptes ou organisations, dans plusieurs régions AWS ou via l'AWS Management Console peut s'avérer fastidieuse. Vous pouvez automatiser le processus en utilisant un outil d'infrastructure en tant que code (IaC), tel que Terraform, qui peut fournir et gérer des services et des ressources multicomptes et multirégionaux dans le cloud.

AWS recommande d'utiliser AWS Organizations pour configurer et gérer plusieurs comptes dans GuardDuty. Ce modèle est conforme à cette recommandation. L'un des avantages de cette approche est que, lorsque de nouveaux comptes sont créés ou ajoutés à l'organisation, GuardDuty ils sont automatiquement activés dans ces comptes pour toutes les régions prises en charge, sans intervention manuelle.

Ce modèle montre comment utiliser HashiCorp Terraform pour activer Amazon GuardDuty pour trois comptes Amazon Web Services (AWS) ou plus dans une organisation. L'exemple de code fourni avec ce modèle effectue les opérations suivantes :

- GuardDuty Activé pour tous les comptes AWS actuellement membres de l'organisation cible dans AWS Organizations
- Active la fonctionnalité d'activation automatique GuardDuty, qui active automatiquement tous GuardDuty les comptes ajoutés à l'organisation cible à l'avenir
- Vous permet de sélectionner les régions dans lesquelles vous souhaitez activer GuardDuty
- Utilise le compte de sécurité de l'organisation en tant qu'administrateur GuardDuty délégué
- Crée un compartiment Amazon Simple Storage Service (Amazon S3) dans le compte de journalisation et le GuardDuty configure pour publier les résultats agrégés de tous les comptes de ce compartiment
- Attribue une politique de cycle de vie qui transfère les résultats du compartiment S3 vers le stockage flexible de récupération Amazon S3 Glacier après 365 jours, par défaut

Vous pouvez exécuter manuellement cet exemple de code ou l'intégrer dans votre pipeline d'intégration continue et de livraison continue (CI/CD).

Public cible

Ce modèle est recommandé aux utilisateurs expérimentés avec Terraform GuardDuty, Python et AWS Organizations.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- Une organisation est configurée dans AWS Organizations et contient au moins les trois comptes suivants :
  - Un compte de gestion — Il s'agit du compte à partir duquel vous déployez le code Terraform, soit de manière autonome, soit dans le cadre du pipeline CI/CD. L'état Terraform est également stocké dans ce compte.
  - Un compte de sécurité — Ce compte est utilisé en tant qu'administrateur GuardDuty délégué. Pour plus d'informations, consultez Considérations importantes pour les administrateurs GuardDuty délégués (GuardDuty documentation).
  - Un compte de journalisation — Ce compte contient le compartiment S3 où sont GuardDuty publiés les résultats agrégés de tous les comptes membres.

  Pour plus d'informations sur la façon de configurer l'organisation avec la configuration requise, consultez Créer une structure de compte (AWS Well-Architected Labs).
- Un compartiment Amazon S3 et une table Amazon DynamoDB qui servent de backend distant pour stocker l'état de Terraform dans le compte de gestion. Pour plus d'informations sur l'utilisation de backends distants pour l'état Terraform, consultez S3 Backends (documentation Terraform). Pour un exemple de code qui configure la gestion de l'état à distance avec un backend S3, voir remote-state-s3-backend (Terraform Registry). Notez les critères suivants :
  - Le compartiment S3 et la table DynamoDB doivent se trouver dans la même région.
  - Lors de la création de la table DynamoDB, la clé de partition doit **`LockID`** être (distinguer majuscules et minuscules) et le type de clé de partition doit être String. Tous les autres paramètres du tableau doivent être à leurs valeurs par défaut. Pour plus d'informations, consultez À propos des clés primaires et Création d'une table (documentation DynamoDB).

- Un compartiment S3 qui sera utilisé pour stocker les journaux d'accès pour le compartiment S3 dans lequel les résultats GuardDuty seront publiés. Pour plus d'informations, consultez Activer la journalisation des accès au serveur Amazon S3 (documentation Amazon S3). Si vous effectuez un déploiement dans une zone de landing zone d'AWS Control Tower, vous pouvez réutiliser le compartiment S3 dans le compte d'archive du journal à cette fin.
- La version 0.14.6 ou ultérieure de Terraform est installée et configurée. Pour plus d'informations, consultez Get Started — AWS (documentation Terraform).
- La version 3.9.6 ou ultérieure de Python est installée et configurée. Pour plus d'informations, consultez la section Sources (site Web de Python).
- Le SDK AWS pour Python (Boto3) est installé. Pour plus d'informations, voir Installation (documentation Boto3).
- jq est installé et configuré. Pour plus d'informations, consultez Télécharger jq (documentation jq).

Limites

- Ce modèle est compatible avec les systèmes d'exploitation macOS et Amazon Linux 2. Ce modèle n'a pas été testé pour être utilisé dans les systèmes d'exploitation Windows.

> **Note**
>
> Le support d'Amazon Linux 2 touche à sa fin. Pour plus d'informations, consultez Amazon Linux 2 FAQs.

- GuardDuty ne doit pas déjà être activé dans aucun des comptes, dans aucune des régions cibles.
- Dans ce modèle, la solution IaC ne déploie pas les prérequis.
- Ce modèle est conçu pour une zone de landing zone AWS qui respecte les meilleures pratiques suivantes :
  - La zone d'atterrissage a été créée à l'aide d'AWS Control Tower.
  - Des comptes AWS distincts sont utilisés pour la sécurité et la journalisation.

Versions du produit

- Terraform version 0.14.6 ou ultérieure. L'exemple de code a été testé pour la version 1.2.8.
- Python version 3.9.6 ou ultérieure.

Architecture

Cette section donne un aperçu général de cette solution et de l'architecture établie par l'exemple de code. Le schéma suivant montre les ressources déployées sur les différents comptes de l'organisation, au sein d'une même région AWS.

1. Terraform crée le rôle GuardDutyTerraformOrgRoleAWS Identity and Access Management (IAM) dans le compte de sécurité et le compte de connexion.
2. Terraform crée un compartiment S3 dans la région AWS par défaut dans le compte de journalisation. Ce compartiment est utilisé comme destination de publication pour agréger tous les GuardDuty résultats provenant de toutes les régions et de tous les comptes de l'organisation. Terraform crée également une clé AWS Key Management Service (AWS KMS) dans le compte de sécurité qui est utilisée pour chiffrer les résultats du compartiment S3 et configure l'archivage automatique des résultats du compartiment S3 dans le stockage S3 Glacier Flexible Retrieval.
3. À partir du compte de gestion, Terraform désigne le compte de sécurité comme administrateur délégué pour. GuardDuty Cela signifie que le compte de sécurité gère désormais le GuardDuty service pour tous les comptes des membres, y compris le compte de gestion. Les comptes de membres individuels ne peuvent pas être suspendus ou GuardDuty désactivés par eux-mêmes.
4. Terraform crée le GuardDuty détecteur dans le compte de sécurité, pour l'administrateur GuardDuty délégué.
5. S'il n'est pas déjà activé, Terraform active la protection S3 dans. GuardDuty Pour plus d'informations, consultez la section Protection d'Amazon S3 sur Amazon GuardDuty (GuardDuty documentation).
6. Terraform inscrit tous les comptes de membres actifs actuels de l'organisation en tant que membres. GuardDuty
7. Terraform configure l'administrateur GuardDuty délégué pour publier les résultats agrégés de tous les comptes membres dans le compartiment S3 du compte de journalisation.
8. Terraform répète les étapes 3 à 7 pour chaque région AWS que vous choisissez.

Automatisation et mise à l'échelle

L'exemple de code fourni est modularisé afin que vous puissiez l'intégrer dans votre pipeline CI/CD pour un déploiement automatisé.

Outils

Services AWS

- Amazon DynamoDB est un service de base de données NoSQL entièrement géré, offrant des performances rapides, prévisibles et évolutives.
- Amazon GuardDuty est un service de surveillance continue de la sécurité qui analyse et traite les journaux afin d'identifier les activités inattendues et potentiellement non autorisées dans votre environnement AWS.
- AWS Identity and Access Management (IAM) vous aide à gérer en toute sécurité l'accès à vos ressources AWS en contrôlant qui est authentifié et autorisé à les utiliser.
- AWS Key Management Service (AWS KMS) vous aide à créer et à contrôler des clés cryptographiques pour protéger vos données.
- AWS Organizations est un service de gestion de comptes qui vous aide à consolider plusieurs comptes AWS au sein d'une organisation que vous créez et gérez de manière centralisée.
- Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets basé sur le cloud qui vous permet de stocker, de protéger et de récupérer n'importe quel volume de données.
- Le SDK AWS pour Python (Boto3) est un kit de développement logiciel qui vous aide à intégrer votre application, bibliothèque ou script Python aux services AWS.

Autres outils et services

- HashiCorp Terraform est une application d'interface en ligne de commande qui vous aide à utiliser du code pour provisionner et gérer l'infrastructure et les ressources du cloud.
- Python est un langage de programmation polyvalent.
- jq est un processeur de ligne de commande qui vous permet de travailler avec des fichiers JSON.

Référentiel de code

Le code de ce modèle est disponible sur GitHub, dans le organizations-with-terraform référentiel amazon-guardduty-for-aws-.

Épopées

Activer GuardDuty au sein de l'organisation

Tâche	Description	Compétences requises
Pour cloner le référentiel.	Dans un shell Bash, exécutez la commande suivante. Dans Cloner le référentiel, dans la section Informations supplémentaires, vous pouvez copier la commande complète contenant l'URL du GitHub référentiel. Cela clone le organizations-with-terraform référentiel amazon-guardduty-for-aws- à partir de GitHub. `git clone <github-repository-url>`	DevOps ingénieur
Modifiez le fichier de configuration Terraform.	1. Dans le `root` dossier du référentiel cloné, répliquez le fichier configuration.json .sample en exécutant la commande suivante. `cp configuration.json .sample configuration.json` 2. Modifiez le nouveau fichier configuration.json et définissez les valeurs pour chacune des variables suivantes : • `management_acc_id` — Numéro	DevOps ingénieur, AWS général, Terraform, Python

Tâche	Description	Compétences requises
	de compte du compte de gestion. • `delegated_admin_acc_id` — Numéro de compte du compte de sécurité. • `logging_acc_id` — ID de compte du compte de connexion. • `target_regions` — Liste séparée par des virgules des régions AWS que vous souhaitez activer. GuardDuty • `organization_id` — ID AWS Organizations de l'organisation dans laquelle vous effectuez l'activation GuardDuty. • `default_region` — La région où votre état Terraform est stocké dans le compte de gestion. Il s'agit de la même région où vous avez déployé le compartiment S3 et la table DynamoDB pour le backend Terraform. • `role_to_assume_for_role_creation` — Nom que vous souhaitez attribuer à un nouveau	

Tâche	Description	Compétences requises
	rôle IAM dans les comptes de sécurité et de journalisation. Vous créerez ce nouveau rôle dans l'histoire suivante. Terraform assume ce rôle pour créer le rôle `GuardDutyTerraformOrgRole` IAM dans les comptes de sécurité et de journalisation. • `finding_publishing_frequency` — Fréquence à laquelle les GuardDuty résultats sont publiés dans le compartiment S3. • `guardduty_findings_bucket_region` — Région préférée dans laquelle vous souhaitez créer le compartiment S3 pour les résultats publiés. • `logging_acc_s3_bucket_name` — Nom préféré pour le compartiment S3 pour les résultats publiés. • `security_acc_kms_key_alias` — Alias AWS KMS pour la clé utilisée pour chiffrer GuardDuty les résultats.	

Tâche	Description	Compétences requises
	• `s3_access_log_bucket_name` — Nom d'un compartiment S3 préexistant dans lequel vous souhaitez collecter les journaux d'accès pour le compartiment S3 utilisé pour les GuardDuty résultats. Ce compartiment doit se trouver dans la même région AWS que le compartiment de GuardDuty résultats. • `tfm_state_backend_s3_bucket` — Nom du compartiment S3 préexistant pour stocker l'état du backend distant Terraform. • `tfm_state_backend_dynamodb_table` — Nom de la table DynamoDB préexistante permettant de verrouiller l'état Terraform. 3. Enregistrez et fermez le fichier de configuration .	

Tâche	Description	Compétences requises
Générez des CloudFormation modèles pour les nouveaux rôles IAM.	Ce modèle inclut une solution IaC permettant de créer deux CloudFormation modèles. Ces modèles créent deux rôles IAM que Terraform utilise lors du processus de configuration. Ces modèles respectent les meilleures pratiques de sécurité relatives aux autorisations du moindre privilège. 1. Dans un shell Bash, dans le `root` dossier du référentiel, accédez à `cfn-templates/` . Ce dossier contient des fichiers CloudFormation modèles avec des stubs. 2. Exécutez la commande suivante. Cela remplace les stubs par les valeurs que vous avez fournies dans le fichier configuration.json. `bash scripts/replace_config_stubs.sh` 3. Vérifiez que les CloudFormation modèles suivants ont été créés dans le `cfn-templates/` dossier : • management-account-role.yaml — Ce fichier contient la définition du	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
	rôle et les autorisations associées pour le rôle IAM dans le compte de gestion, qui dispose des autorisations minimales requises pour exécuter ce modèle. • role-to-assume-for-role-creation.yaml — Ce fichier contient la définition du rôle et les autorisations associées pour le rôle IAM dans les comptes de sécurité et de journalisation. Terraform assume ce rôle afin de créer le GuardDuty TerraformOrgRolerôle dans ces comptes.	

Tâche	Description	Compétences requises
Créez les rôles IAM.	En suivant les instructions de la section Création d'une pile (CloudFormation documentation), procédez comme suit : 1. Déployez la pile role-to-assume-for-role-creation.yaml dans les comptes de sécurité et de journalisation. 2. Déployez la pile management-account-role.yaml dans le compte de gestion. Lorsque vous créez la pile avec succès et que vous voyez l'état de la `CREATE_COMPLETE` pile, notez l'Amazon Resource Name (ARN) de ce nouveau rôle dans le résultat.	DevOps ingénieur, AWS général
Assumez le rôle IAM dans le compte de gestion.	Pour des raisons de sécurité, nous vous recommandons d'assumer le nouveau rôle management-account-roleIAM avant de continuer. Dans l'interface de ligne de commande AWS (AWS CLI), entrez la commande dans Assumer le rôle IAM du compte de gestion dans la section Informations supplémentaires.	DevOps ingénieur, AWS général

Tâche	Description	Compétences requises
Exécutez le script de configuration.	Dans le `root` dossier du référentiel, exécutez la commande suivante pour démarrer le script de configuration. `bash scripts/full-setup.sh` Le script full-setup.sh exécute les actions suivantes : • Exporte toutes les valeurs de configuration sous forme de variables d'environnement • Génère les fichiers de code backend.tf et terraform .tfvars pour chaque module Terraform • Permet un accès fiable au GuardDuty sein de l'organisation via l'interface de ligne de commande AWS. • Importe l'état de l'organisation dans l'état Terraform • Crée le compartiment S3 pour publier les résultats dans le compte de journalisation • Crée la clé AWS KMS pour chiffrer les résultats dans le compte de sécurité	DevOps ingénieur, Python

Tâche	Description	Compétences requises
	• Activé GuardDuty dans l'ensemble de l'organisation, dans toutes les régions sélectionnées, comme décrit dans la section Architecture	

(Facultatif) Désactiver GuardDuty dans l'organisation

Tâche	Description	Compétences requises
Exécutez le script de nettoyage.	Si vous avez utilisé ce modèle pour l'activer GuardDuty pour l'organisation et que vous souhaitez le désactiver GuardDuty, dans le `root` dossier du référentiel, exécutez la commande suivante pour démarrer le script cleanup-gd.sh. `bash scripts/cleanup-gd.sh` Ce script est désactivé GuardDuty dans l'organisation cible, supprime toutes les ressources déployées et restaure l'organisation à son état antérieur avant d'utiliser Terraform pour l'activer. GuardDuty	DevOps ingénieur, AWS général, Terraform, Python

Tâche	Description	Compétences requises
	Note Ce script ne supprime pas les fichiers d'état Terraform ni ne verrouille les fichiers des backends locaux et distants. Si cela est nécessaire, vous devez effectuer ces actions manuellement. En outre, ce script ne supprime pas l'organisation importée ni les comptes qu'elle gère. L'accès sécurisé pour GuardDuty n'est pas désactivé dans le cadre du script de nettoyage.	
Supprimez les rôles IAM.	Supprimez les piles créées avec les modèles role-to-assume-for-role-creation.yaml et .yaml. management-account-role CloudFormation Pour plus d'informations, consultez Supprimer une pile (CloudFormation documentation).	DevOps ingénieur, AWS général

Ressources connexes

Documentation AWS

- Gestion de plusieurs comptes (GuardDuty documentation)
- Octroi du moindre privilège (documentation IAM)

Marketing sur AWS

- Amazon GuardDuty
- AWS Organizations

Autres ressources

- Terraforme
- Documentation de la CLI Terraform

Informations supplémentaires

Cloner le référentiel

Exécutez la commande suivante pour cloner le GitHub référentiel.

```
git clone https://github.com/aws-samples/amazon-guardduty-for-aws-organizations-with-terraform
```

Assumez le rôle IAM du compte de gestion

Pour assumer le rôle IAM dans le compte de gestion, exécutez la commande suivante. Remplacez `<IAM role ARN>` par l'ARN du rôle IAM.

```
export ROLE_CREDENTIALS=$(aws sts assume-role --role-arn <IAM role ARN> --role-session-name AWSCLI-Session --output json)
export AWS_ACCESS_KEY_ID=$(echo $ROLE_CREDENTIALS | jq .Credentials.AccessKeyId | sed 's/"//g')
export AWS_SECRET_ACCESS_KEY=$(echo $ROLE_CREDENTIALS | jq .Credentials.SecretAccessKey | sed 's/"//g')
export AWS_SESSION_TOKEN=$(echo $ROLE_CREDENTIALS | jq .Credentials.SessionToken | sed 's/"//g')
```

Vérifiez les meilleures pratiques opérationnelles pour la norme PCI DSS 4.0 en utilisant AWS Config

Créée par Tala Qraitem (AWS) et Alex Goff (AWS)

Récapitulatif

La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) décrit les protocoles techniques et opérationnels essentiels pour protéger les données de paiement. La norme PCI DSS a été développée pour encourager et améliorer la sécurité des données pour les comptes de cartes de paiement. Il facilite également l'adoption globale de mesures de sécurité cohérentes. Bien qu'il soit spécifiquement conçu pour les environnements contenant des données de comptes de cartes de paiement, vous pouvez utiliser la norme PCI DSS pour vous protéger contre les menaces et sécuriser d'autres éléments de l'écosystème de paiement.

La version 4.0 de la norme PCI DSS a été publiée pour répondre à l'évolution des exigences, fournir des éclaircissements ou des directives supplémentaires et améliorer la structure et le format de la norme. Pour plus d'informations sur les modifications, voir Résumé des modifications entre les versions PCI DSS 3.2.1 à 4.0.

Un pack de AWS Config conformité est un ensemble de AWS Config règles et d'actions correctives qui vous aident à créer des contrôles de gouvernance en matière de sécurité, d'exploitation ou d'optimisation des coûts. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans un Compte AWS et Région AWS, ou vous pouvez le déployer au sein d'une organisation dans AWS Organizations.

Les packs de conformité pour la version 4.0 de la norme PCI DSS complètent et s'appuient sur le pack de conformité de la version 3.2.1. Les règles du pack de conformité correspondent aux règles de la norme. Pour plus d'informations, consultez le mappage fourni dans la section Pièces jointes. Vous pouvez choisir entre deux versions de ce pack de conformité : l'une qui inclut les types de ressources globaux et l'autre qui les exclut.

> **Important**
>
> Les packs de conformité ne sont pas conçus pour garantir pleinement la conformité à une norme de gouvernance ou de conformité spécifique. Il vous incombe de déterminer vous-même si l'utilisation est conforme aux exigences légales et réglementaires applicables.

Conditions préalables et limitations

Prérequis

- Ayez un actif Compte AWS.
- Configurez AWS Config.
- Répondez aux conditions requises pour les packs de conformité.
- Déployez le pack de conformité PCI DSS version 3.2.1.
- Disposez des autorisations nécessaires pour accéder aux packs de conformité AWS Config et les gérer. Pour un exemple de politique, consultez la section Informations supplémentaires de ce modèle.

Limites

- Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, mais tous les quotas ne peuvent pas être augmentés. Assurez-vous de connaître les limites du AWS Config service, y compris les limites applicables aux packs de conformité à compte unique et aux packs de conformité pour les organisations.
- La version de ce pack de conformité qui inclut les types de ressources globaux est destinée au déploiement uniquement dans la `us-east-1` région.
- La version de ce pack de conformité qui exclut les types de ressources globaux est destinée au déploiement uniquement dans les régions suivantes :
  - `ap-east-1`
  - `ap-south-1`
  - `ap-northeast-2`
  - `ap-southeast-1`
  - `ap-southeast-2`
  - `ap-northeast-1`
  - `ca-central-1`
  - `eu-central-1`
  - `eu-west-1`
  - `eu-west-2`

- eu-west-3
- eu-north-1
- sa-east-1
- us-east-2
- us-west-1
- us-west-2

Outils

Services AWS

- AWS Configfournit une vue détaillée des ressources de votre ordinateur Compte AWS et de la façon dont elles sont configurées. Il vous aide à identifier la façon dont les ressources sont liées les unes aux autres et comment leurs configurations ont évolué au fil du temps.
- AWS Systems Managervous aide à gérer vos applications et votre infrastructure exécutées dans le AWS Cloud. Il simplifie la gestion des applications et des ressources, réduit le délai de détection et de résolution des problèmes opérationnels et vous aide à gérer vos AWS ressources en toute sécurité à grande échelle.

Référentiel de code

Les packs de conformité se trouvent dans le référentiel des packs GitHub de AWS Config conformité. Ce référentiel contient les modèles suivants relatifs à la version 4.0 de la norme PCI DSS :

- Meilleures pratiques opérationnelles pour PCI-DSS-v4.0- .yaml including-global-resourcetypes
- Meilleures pratiques opérationnelles pour PCI-DSS-v4.0- .yaml excluding-global-resourcetypes

Épopées

Déployer et gérer le pack de conformité

Tâche	Description	Compétences requises
Téléchargez le pack de conformité.	Si vous déployez le pack de conformité dans la us-	DevOps ingénieur

Tâche	Description	Compétences requises
	`east-1` région, télécharg ez le modèle Operational-Best-Practices-for-PCI-DSS-v4.0 - .yaml. including-global-r esourcetypes Si vous déployez le pack de conformité dans une autre région, téléchargez le modèle Operational-Best-Practices-for-PCI-DSS-v4.0 - .yaml. excluding-global-resourcety pes	
(Facultatif) Modifiez le pack de conformité.	Vous pouvez modifier le modèle de pack de conformit é en fonction des besoins uniques de votre organisat ion. Par exemple, vous pouvez créer des actions de correctio n personnalisées. Pour plus d'informations sur la création et la modification de modèles, consultez la section Création de modèles pour des packs de conformité personnalisés dans la AWS Config documentation.	AWS général

Tâche	Description	Compétences requises
Déployez le pack de conformité.	Si vous effectuez un déploiement dans une cible Compte AWS ou Région AWS, suivez les instructions de la section Déploiement de packs de conformité dans la AWS Config documentation. Vous pouvez utiliser le AWS Management Console ou le AWS Command Line Interface (AWS CLI). Si vous déployez le pack de conformité au sein d'une organisation en AWS Organizations, suivez les instructions de la section Déployer le pack de AWS Config conformité à l'aide de la configuration rapide dans la AWS Systems Manager documentation.	AWS général
(Facultatif) Modifiez le pack de conformité.	Si vous souhaitez modifier le pack de conformité, suivez les instructions de la section Modification des packs de conformité de la AWS Config documentation. Vous pouvez utiliser le AWS Management Console ou le AWS CLI.	AWS général

Tâche	Description	Compétences requises
(Facultatif) Supprimez le pack de conformité.	Si vous souhaitez supprimer le pack de conformité, suivez les instructions de la section Suppression des packs de conformité de la AWS Config documentation. Vous pouvez utiliser le AWS Management Console ou le AWS CLI.	AWS général

Ressources connexes

AWS resources

- Packs de conformité pour AWS Config (AWS Config documentation)
- Déployez le pack de AWS Config conformité à l'aide de Quick Setup (documentation Systems Manager)
- Conformité à la norme PCI DSS sur AWS(site Web)AWS
- PCI DSS version 4.0 activée AWS(guide de conformité)

Ressources PCI DSS

- Hub de ressources PCI DSS version 4.0
- Bibliothèque de documents du Conseil des normes de sécurité PCI
- Résumé des modifications entre les versions 3.2.1 et 4.0 de la norme PCI DSS

Informations supplémentaires

Voici un exemple de politique AWS Identity and Access Management (IAM) qui permet à l'utilisateur d'accéder aux packs de conformité AWS Config et de les gérer :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "config:PutConfigRule",
                "config:PutConformancePack",
                "config:DeleteConfigRule",
                "config:DeleteRemediationConfiguration",
                "config:DeleteConformancePack",
                "config:PutRemediationConfigurations",
                "config:BatchGetAggregateResourceConfig",
                "config:BatchGetResourceConfig",
                "config:Get*",
                "config:Describe*",
                "config:Deliver*",
                "config:List*",
                "config:Select*"
            ],
            "Resource": "*"
        }
    ]
}
```

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Vérifiez que les nouveaux clusters Amazon Redshift ont besoin de points de terminaison SSL

Créée par Priyanka Chaudhary (AWS)

Récapitulatif

Ce modèle fournit un CloudFormation modèle Amazon Web Services (AWS) qui vous avertit automatiquement lorsqu'un nouveau cluster Amazon Redshift est lancé sans points de terminaison SSL (Secure Sockets Layer).

Amazon Redshift est un service d'entrepôt de données basé sur le cloud entièrement géré à l'échelle du pétaoctet. Il est conçu pour le stockage et l'analyse de jeux de données à grande échelle. Il est également utilisé pour effectuer des migrations de bases de données à grande échelle. Pour des raisons de sécurité, Amazon Redshift prend en charge le protocole SSL pour chiffrer la connexion entre l'application cliente SQL Server de l'utilisateur et le cluster Amazon Redshift. Pour configurer votre cluster afin qu'il nécessite une connexion SSL, vous définissez le `require_SSL` paramètre sur `true` dans le groupe de paramètres associé au cluster lors du lancement.

Le contrôle de sécurité fourni avec ce modèle surveille les appels d'API Amazon Redshift dans CloudTrail les journaux AWS et lance un événement Amazon CloudWatch Events pour les CreateCluster,, ModifyClusterRestoreFromClusterSnapshot, CreateClusterParameterGroupet. ModifyClusterParameterGroup APIs Lorsque l'événement détecte l'un d'entre eux APIs, il appelle AWS Lambda, qui exécute un script Python. La fonction Python analyse l' CloudWatch événement à la recherche des CloudTrail événements répertoriés. Lorsqu'un cluster Amazon Redshift est créé, modifié ou restauré à partir d'un instantané existant, qu'un nouveau groupe de paramètres est créé pour le cluster ou qu'un groupe de paramètres existant est modifié, la fonction vérifie le `require_SSL` paramètre du cluster. Si la valeur du paramètre est `false` égale à cette valeur, la fonction envoie une notification Amazon Simple Notification Service (Amazon SNS) à l'utilisateur avec les informations pertinentes : le nom du cluster Amazon Redshift, la région AWS, le compte AWS et le nom de ressource Amazon (ARN) pour Lambda d'où provient cette notification.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.

- Un cloud privé virtuel (VPC) avec un groupe de sous-réseaux de clusters et un groupe de sécurité associé.

Limites

- Ce contrôle de sécurité est régional. Vous devez le déployer dans chaque région AWS que vous souhaitez surveiller.

Architecture

Architecture cible

Automatisation et mise à l'échelle

- Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs.
- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données entièrement géré de plusieurs pétaoctets dans le cloud.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets. Vous pouvez utiliser Amazon S3 pour stocker et récupérer n'importe quelle quantité de données, n'importe quand et depuis n'importe quel emplacement sur le Web.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail. Les abonnés reçoivent tous les messages publiés dans les rubriques auxquelles ils sont abonnés, et tous les abonnés à une rubrique reçoivent les mêmes messages.

Code

Ce modèle inclut les pièces jointes suivantes :

- `RedshiftSSLEndpointsRequired.zip`— Le code Lambda pour le contrôle de sécurité.
- `RedshiftSSLEndpointsRequired.yml`— Le CloudFormation modèle qui définit l'événement et la fonction Lambda.

Épopées

Configuration du compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 pour héberger le fichier .zip de code Lambda. Ce compartiment S3 doit se trouver dans la même région AWS que le cluster Amazon Redshift que vous souhaitez surveiller. Le nom d'un compartiment S3 est unique au monde et l'espace de noms est partagé par tous les comptes AWS. Le nom du compartiment S3 ne peut pas	Architecte du cloud

Tâche	Description	Compétences requises
	inclure de barres obliques en tête.	
Téléchargez le code Lambda.	Téléchargez le fichier .zip de code Lambda fourni dans la section Pièces jointes dans le compartiment S3.	Architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle AWS.	Ouvrez la CloudFormation console AWS dans la même région AWS que votre compartiment S3 et déployez le modèle joint`RedshiftSSLEndpointsRequired.yml` . Pour plus d'informations sur le déploiement de CloudFormation modèles AWS, consultez la section Création d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation.	Architecte du cloud
Complétez les paramètres du modèle.	Lorsque vous lancez le modèle, les informations suivantes vous sont demandées : • Compartiment S3 : Spécifiez le compartiment que vous avez créé ou sélectionné	Architecte du cloud

Tâche	Description	Compétences requises
	dans le premier épisode épique. C'est ici que vous avez chargé le code Lambda joint (fichier .zip). • Clé S3 : Spécifiez l'emplacement du fichier Lambda .zip dans votre compartiment S3 (par exemple, nom de fichier .zip ou controls/ nom de fichier .zip). N'incluez pas de barres obliques en tête. • E-mail de notification : indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications Amazon SNS. • Niveau de journalisation Lamba : Spécifiez le niveau et la fréquence de journalisation pour la fonction Lambda. Utilisez Info pour consigner des messages d'information détaillés sur la progression, Erreur pour les événements d'erreur susceptibles de permettre la poursuite du déploiement et Avertissement pour les situations potentiellement dangereuses.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Vous devez confirmer cet abonnement par e-mail pour commencer à recevoir des notifications de violation.	Architecte du cloud

Ressources connexes

- Création d'un compartiment S3 (documentation Amazon S3)
- Téléchargement de fichiers dans un compartiment S3 (documentation Amazon S3)
- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail (CloudTrail documentation AWS)
- Création d'un cluster Amazon Redshift (documentation Amazon Redshift)
- Configuration des options de sécurité pour les connexions (documentation Amazon Redshift)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Vérifiez que les nouveaux clusters Amazon Redshift sont lancés dans un VPC

Créée par Priyanka Chaudhary (AWS)

Récapitulatif

Ce modèle fournit un CloudFormation modèle Amazon Web Services (AWS) qui vous avertit automatiquement lorsqu'un cluster Amazon Redshift est lancé en dehors d'un cloud privé virtuel (VPC).

Amazon Redshift est un produit d'entrepôt de données basé sur le cloud entièrement géré à l'échelle du pétaoctet. Il est conçu pour le stockage et l'analyse de jeux de données à grande échelle. Il est également utilisé pour effectuer des migrations de bases de données à grande échelle. Amazon Virtual Private Cloud (Amazon VPC) vous permet de mettre en place une section logiquement isolée du cloud AWS où vous pouvez lancer des ressources AWS telles que des clusters Amazon Redshift dans un réseau virtuel que vous définissez.

Le contrôle de sécurité fourni avec ce modèle surveille les appels d'API Amazon Redshift dans CloudTrail les journaux AWS et déclenche un événement Amazon CloudWatch Events pour le et. CreateClusterRestoreFromClusterSnapshot APIs Lorsque l'événement détecte l'un d'entre eux APIs, il appelle AWS Lambda, qui exécute un script Python. La fonction Python analyse l' CloudWatch événement. Si un cluster Amazon Redshift est créé ou restauré à partir d'un instantané et apparaît en dehors du réseau Amazon VPC, la fonction envoie une notification Amazon Simple Notification Service (Amazon SNS) à l'utilisateur avec les informations pertinentes : nom du cluster Amazon Redshift, région AWS, compte AWS et nom de ressource Amazon (ARN) pour Lambda indiquant que cette notification est provenant de.

Conditions préalables et limitations

Prérequis

- Un compte AWS actif.
- VPC avec un groupe de sous-réseaux de clusters et un groupe de sécurité associé.

Limites

- Le CloudFormation modèle AWS prend uniquement en charge RestoreFromClusterSnapshotles actions CreateClusteret (nouveaux clusters). Il ne détecte pas les clusters Amazon Redshift existants créés en dehors d'un VPC.
- Ce contrôle de sécurité est régional. Vous devez le déployer dans chaque région AWS que vous souhaitez surveiller.

Architecture

Architecture cible

Automatisation et mise à l'échelle

Si vous utilisez AWS Organizations, vous pouvez utiliser AWS Cloudformation StackSets pour déployer ce modèle sur plusieurs comptes que vous souhaitez surveiller.

Outils

Services AWS

- AWS CloudFormation — AWS vous CloudFormation aide à modéliser et à configurer vos ressources AWS, à les approvisionner rapidement et de manière cohérente, et à les gérer tout au long de leur cycle de vie. Vous pouvez utiliser un modèle pour décrire vos ressources et leurs dépendances, puis les lancer et les configurer ensemble sous forme de pile, au lieu de gérer les ressources individuellement.
- AWS CloudTrail — AWS vous CloudTrail aide à mettre en œuvre la gouvernance, la conformité et l'audit opérationnel et des risques de votre compte AWS. Les actions entreprises par un utilisateur, un rôle ou un service AWS sont enregistrées sous forme d'événements dans CloudTrail.
- Amazon CloudWatch Events — Amazon CloudWatch Events fournit un flux quasi en temps réel d'événements système décrivant les modifications apportées aux ressources AWS.
- AWS Lambda — AWS Lambda est un service de calcul qui prend en charge l'exécution de code sans provisionner ni gérer de serveurs. AWS Lambda exécute le code uniquement lorsque cela est nécessaire et se met à l'échelle automatiquement, qu'il s'agisse de quelques requêtes par jour ou de milliers de requêtes par seconde.
- Amazon Redshift — Amazon Redshift est un service d'entrepôt de données entièrement géré de plusieurs pétaoctets dans le cloud. Amazon Redshift est intégré à votre lac de données, ce qui

vous permet d'utiliser vos données pour acquérir de nouvelles informations pour votre entreprise et vos clients.

- Amazon S3 — Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets hautement évolutif que vous pouvez utiliser pour un large éventail de solutions de stockage, notamment les sites Web, les applications mobiles, les sauvegardes et les lacs de données.
- Amazon SNS — Amazon Simple Notification Service (Amazon SNS) coordonne et gère la distribution ou l'envoi de messages entre les éditeurs et les clients, y compris les serveurs Web et les adresses e-mail.

Code

Ce modèle inclut les pièces jointes suivantes :

- `RedshiftMustBeInVPC.zip`— Le code Lambda pour le contrôle de sécurité.
- `RedshiftMustBeInVPC.yml`— Le CloudFormation modèle qui définit l'événement et la fonction Lambda.

Pour utiliser ces fichiers, suivez les instructions de la section suivante.

Épopées

Configuration du compartiment S3

Tâche	Description	Compétences requises
Définissez le compartiment S3.	Sur la console Amazon S3, choisissez ou créez un compartiment S3 pour héberger le fichier .zip de code Lambda. Ce compartiment S3 doit se trouver dans la même région AWS que le cluster Amazon Redshift que vous souhaitez surveiller. Le nom d'un compartiment S3 est unique au monde et l'espace	Architecte du cloud

Tâche	Description	Compétences requises
	de noms est partagé par tous les comptes AWS. Le nom du compartiment S3 ne peut pas inclure de barres obliques en tête.	
Téléchargez le code Lambda.	Téléchargez le code Lambda (`RedshiftMustBeInVPC.zip` fichier) fourni dans la section Pièces jointes dans le compartiment S3.	Architecte du cloud

Déployer le CloudFormation modèle

Tâche	Description	Compétences requises
Lancez le CloudFormation modèle.	Ouvrez la CloudFormation console AWS dans la même région AWS que votre compartiment S3 et déployez le modèle joint (`RedshiftMustBeInVPC.yml`). Pour plus d'informations sur le déploiement de CloudFormation modèles AWS, consultez la section Création d'une pile sur la CloudFormation console AWS dans la CloudFormation documentation.	Architecte du cloud
Complétez les paramètres du modèle.	Lorsque vous lancez le modèle, les informations suivantes vous sont demandées :	Architecte du cloud

Tâche	Description	Compétences requises
	• Compartiment S3 : Spécifiez le compartiment que vous avez créé ou sélectionné dans le premier épisode épique. C'est ici que vous avez chargé le code Lambda joint (fichier .zip). • Clé S3 : Spécifiez l'emplacement du fichier Lambda .zip dans votre compartiment S3 (par exemple, nom de fichier .zip ou controls/ nom de fichier .zip). N'incluez pas de barres obliques en tête. • E-mail de notification : indiquez une adresse e-mail active à laquelle vous souhaitez recevoir des notifications Amazon SNS. • Niveau de journalisation Lamba : Spécifiez le niveau et la fréquence de journalisation pour la fonction Lambda. Utilisez Info pour consigner des messages d'information détaillés sur la progression, Erreur pour les événements d'erreur susceptibles de permettre la poursuite du déploiement et Avertissement pour les situations potentiellement dangereuses.	

Confirmer l'abonnement.

Tâche	Description	Compétences requises
Confirmez votre abonnement.	Lorsque le CloudFormation modèle est déployé avec succès, il envoie un e-mail d'abonnement à l'adresse e-mail que vous avez fournie. Vous devez confirmer cet abonnement par e-mail pour commencer à recevoir des notifications de violation.	Architecte du cloud

Ressources connexes

- Création d'un compartiment S3 (documentation Amazon S3)
- Chargement de fichiers dans un compartiment S3 (documentation Amazon S3)
- Création d'une pile sur la CloudFormation console AWS (CloudFormation documentation AWS)
- Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d'API AWS à l'aide d'AWS CloudTrail (CloudTrail documentation AWS)
- Création d'un cluster Amazon Redshift (documentation Amazon Redshift)

Pièces jointes

Pour accéder au contenu supplémentaire associé à ce document, décompressez le fichier suivant : attachment.zip

Plus de modèles

- Accédez à un hôte bastion à l'aide du gestionnaire de session et d'Amazon EC2 Instance Connect
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS Fargate, d' PrivateLinkAWS et d'un Network Load Balancer
- Accédez à des applications de conteneur en privé sur Amazon ECS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Accédez à des applications de conteneur en privé sur Amazon EKS à l'aide d'AWS PrivateLink et d'un Network Load Balancer
- Autoriser EC2 les instances à accéder en écriture aux compartiments S3 dans les comptes AMS
- Associer un AWS CodeCommit référentiel dans un compte Compte AWS à Amazon SageMaker AI Studio Classic dans un autre compte
- Authentifiez les utilisateurs existants de l'application React à l'aide d'Amazon Cognito et de l'interface utilisateur AWS Amplify
- Automatisez l'ajout ou la mise à jour d'entrées de registre Windows à l'aide d'AWS Systems Manager
- Automatisez l'application du chiffrement dans AWS Glue à l'aide d'un CloudFormation modèle AWS
- Associez automatiquement une politique gérée par AWS pour Systems Manager aux profils d' EC2 instance à l'aide de Cloud Custodian et d'AWS CDK
- Chiffrez automatiquement les volumes Amazon EBS existants et nouveaux
- Bloquez l'accès public à Amazon RDS à l'aide de Cloud Custodian
- Centralisation de la résolution DNS à l'aide AWS Managed Microsoft AD et sur site de Microsoft Active Directory
- Mettez en œuvre une analyse Checkov personnalisée et centralisée pour appliquer la politique avant de déployer AWS l'infrastructure
- Consultez les applications ou les CloudFormation modèles AWS CDK pour connaître les meilleures pratiques à l'aide des packs de règles cdk-nag
- Vérifiez la présence de balises obligatoires dans les EC2 instances au lancement
- Configuration de l'accès intercompte à Amazon DynamoDB
- Configurer le chiffrement HTTPS pour Oracle JD Edwards EnterpriseOne sur Oracle à l'aide WebLogic d'un Application Load Balancer

- Configuration de la journalisation et de la surveillance des événements de sécurité dans votre AWS IoT environnement
- Configurer l'authentification TLS mutuelle pour les applications exécutées sur Amazon EKS
- Connectez-vous en utilisant un tunnel SSH dans pgAdmin
- Créez une application React à l'aide d'AWS Amplify et ajoutez l'authentification avec Amazon Cognito
- Créez un rapport sur les résultats de l'analyseur d'accès réseau pour l'accès Internet entrant en plusieurs Comptes AWS
- Personnalisez les CloudWatch alertes Amazon pour AWS Network Firewall
- Déployez un pare-feu à l'aide d'AWS Network Firewall et d'AWS Transit Gateway
- Déployez une ChatOps solution pour gérer les résultats du scan SAST en utilisant Amazon Q Developer dans les applications de chat, les actions personnalisées et AWS CloudFormation
- Documentez la conception de votre zone de landing zone AWS
- Activer les connexions chiffrées pour les instances de base de données PostgreSQL dans Amazon RDS
- Chiffrer une instance de base de données Amazon RDS pour PostgreSQL existante
- Appliquer le balisage automatique des bases de données Amazon RDS au lancement
- Appliquer le balisage des clusters Amazon EMR au lancement
- Assurez-vous que la journalisation d'Amazon EMR sur Amazon S3 est activée au lancement
- Générez un CloudFormation modèle AWS contenant les règles gérées par AWS Config à l'aide de Troposphere
- Recevez des notifications Amazon SNS lorsque l'état clé d'une clé AWS KMS change
- Aidez à appliquer le balisage DynamoDB
- Identifiez et alertez lorsque les ressources Amazon Data Firehose ne sont pas chiffrées à l'aide d'une clé AWS KMS
- SHA1 Implémenter le hachage des données personnelles lors de la migration de SQL Server vers PostgreSQL
- Améliorez les performances opérationnelles en activant Amazon DevOps Guru dans plusieurs régions AWS, sur plusieurs comptes et OUs avec le kit AWS CDK
- Ingérez et migrez des instances EC2 Windows vers un compte AWS Managed Services
- Migrez Amazon RDS for Oracle vers Amazon RDS for PostgreSQL en mode SSL à l'aide d'AWS DMS

- Migrer une pile ELK vers Elastic Cloud sur AWS
- Migrer une charge de travail F5 BIG-IP vers F5 BIG-IP VE sur le cloud AWS
- Surveillez Amazon Aurora pour détecter les instances sans chiffrement
- Fournissez des rôles IAM avec le moindre privilège en déployant une solution de distribution automatique de rôles
- Rotation des informations d'identification de base de données sans redémarrer les conteneurs
- Sécurisez et rationalisez l'accès des utilisateurs dans une base de données de fédération DB2 sur AWS en utilisant des contextes fiables
- Envoyez AWS WAF des logs à Splunk à l'aide AWS Firewall Manager d'Amazon Data Firehose
- Diffusez du contenu statique dans un compartiment Amazon S3 via un VPC en utilisant Amazon CloudFront
- Configurer le end-to-end chiffrement des applications sur Amazon EKS à l'aide du gestionnaire de certificats et de Let's Encrypt
- Utiliser l'utilisateur IDs dans les politiques IAM pour le contrôle d'accès et l'automatisation
- Vérifiez que les équilibreurs de charge ELB nécessitent une terminaison TLS
- Consultez les journaux et les statistiques d'AWS Network Firewall à l'aide de Splunk
- Visualisez les rapports d'identification IAM pour tous les comptes AWS à l'aide d'Amazon QuickSight

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.